Intelligent Transportation Systems Security Control Set Template and Instructions

www.its.dot.gov/index.htm

Final Report – July 31, 2023
Publication Number FHWA-JPO-23-122

U.S. Department of Transportation

Produced by (Name of Contract)
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
(List all USDOT agencies sponsoring this report; only list one agency on the report cover)

Notice

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-23-122		

4. Title and Subtitle	5. Report Date
Intelligent Transportation Systems Security Control Set Template and Instructions	July 31, 2023
	6. Performing Organization Code V-337

7. Author(s)	8. Performing Organization Report No.
Randy Gabel, Christina Sames, Hector Martinez, Pam Miller, Julie Nethery Snyder, Dr. Michaela Vanderveen	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
U.S. DOT Volpe National Transportation Systems Center 220 Binney Street Cambridge MA 02142	**11. Contract or Grant No.** IAA 693JJ320N300058

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
ITS-Joint Program Office 1200 New Jersey Avenue, S.E. Washington, DC 20590	Final Report August 28, 2020 – August 27, 2023
	14. Sponsoring Agency Code HOIT-1

15. Supplementary Notes

This work was performed in collaboration with the National Institute of Standards and Technology and MITRE Corp.

16. Abstract

This document is a template and instructions for developing control sets for ITS physical objects (systems and devices) as defined in Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT). The control sets can be provided to developers and can be used to identify requirements for developing and assessing physical objects.

The intent is for authors of control set documents to maintain the format provided in this template to ensure consistent development and use across the ITS community. The content within the prescribed sections may vary based on the types of systems and their physical objects which are the subjects of each instantiation of this document.

17. Keywords	18. Distribution Statement
Intelligent Transportation Systems, Cybersecurity, Control Sets, NIST SP 800-53	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
unclassified	unclassified	63	

Table of Contents

List of Tables

INSTRUCTIONS: This document is a template and instructions for developing control sets for ITS physical objects (systems and devices) as defined in Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT). The control sets can be provided to developers and can be used to identify requirements for developing and assessing physical objects.

The intent is for authors[1] of control set documents to maintain the format provided in this template to ensure consistent development and use across the ITS community. The content within the prescribed sections may vary based on the types of systems and their physical objects which are the subjects of each instantiation of this document.

More than one physical object may be the subject of this control set. This would typically happen if the physical objects were similar in technology and use and, therefore, have similar vulnerabilities that may be exploited by similar threat sources, creating similar risk. That is, the controls selected to mitigate the risks are similar enough to justify combining the physical objects in a single control set document.

Italicized orange text in this document prompts authors to enter the content specific to the physical object. Once content specific to the physical object has been entered, change the italicized orange text to black font color. Also delete the italicized instructions and examples in the blue boxes (such as in this instruction box) as this document is being developed for a given ITS and its physical object(s).

To aid users of this document in navigating references, create bookmarks for all cited publications and link each occurrence of that publication in the final control set document to the bookmark.[2]

[1] The *ITS Operating Procedures for Developing Control Sets* explain who these authors may be.

[2] To bookmark text, such as publications listed in the Standards element of this document, highlight the text, go to the Insert menu, select Bookmark, and provide a unique bookmark name with no spaces; underscores may be used to separate text for clarity. To link text in the body to the bookmark created, highlight the body text, right-click and select Link, select Place in this Document in the left pane, and scroll to select the appropriate bookmark from the list in the right pane.

Chapter 1. Identification

INSTRUCTIONS: In this Identification chapter, identify the control set document by providing the following information regarding this document: a unique name, a version number and date, the version of NIST Special Publication (SP) 800-53 used, any other documentation used, and the events that can cause the document to be modified or updated.

1.1 Purpose, Scope, and Applicability

The subject of this control set[3] document is ITS – *enter a short title or name for the physical object(s) that are the focus of this document. Also change the title on the title page to match this text.* This document identifies security and privacy control specifications required to address security and privacy risks specific to ITS *name of physical object(s)*. This control set document is created from controls in NIST SP 800-53.

This control set document identifies security controls typically needed to mitigate security risks to *name for the physical object(s)*. The objective of this control set is to provide a means to better protect the *name for the physical object(s)* and the information flows supported by its interfaces as more advanced features are added.

The controls (primarily technical controls) relevant to *name for the physical object(s)* 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.

[3] A control set is a predefined set of controls and specifications that addresses an agreed upon topic (i.e., a physical object) and is assembled to address the protection needs of that physical object (reference *ITS Operating Procedures for Developing Control Sets*). Control sets are similar in construct to overlays as defined and described in NIST SP 800-53 and NIST SP 800-53B but differ in development and implementation from overlays as there is no baseline to which an ITS control set is applied. ITS control sets are complete on their own, whereas an overlay is a means to modify a selected baseline. The NIST baseline approach is not used in this document.

This control set is intended to be used by system and service managers/owners, system integrators, system engineers, and system component manufacturers to derive security requirements for the *name for the physical object(s)*.

The risk mitigation and protection provided by other controls implemented in larger systems, operations, or data centers, or by the Infrastructure Owner/Operators (IOOs) operating ITS provide benefit to physical objects that are part of these larger systems, centers, or IOOs. Owners, operators, and users of *name for the physical object(s)* may examine the security assessment of the larger system to determine which risks might not be mitigated and/or might be passed on to a *name for the physical object(s)* itself and then select controls that mitigate that risk. Some controls tagged in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*, as organizational controls are included in this control set because there are aspects of the control that need to be conveyed to the manufacturer/vendor for design and implementation. In some cases, the organizational control is purely non-technical but is so important to successfully securing the *name for the physical object(s)* that the control cannot be ignored and must be addressed by the IOO before, during, or after a *name for the physical object(s)* is delivered and installed.

1.2 Revisions

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

- NIST issues new revisions[4] of SP 800-53.
- ARC-IT is significantly revised.
- Relevant standards are developed or updated.
- Significant changes to technologies are made.
- New threats and/or vulnerabilities are discovered that impact the subject of this document.

1.3 Sources

INSTRUCTIONS: List, describe, and explain how key sources influence or inform the selection of controls for the physical devices that are the subject of this control set document. Sources that are typically relevant are provided below, but other sources may need to be added.

[4] NIST publishes two types of updates to NIST SP 800-53 – revisions and errata changes. Full revisions typically include substantive changes to controls. Errata changes do not usually include substantive changes to controls. For the latest Revision 4 to Revision 5 update, NIST published an analysis of the updates between the two revisions of NIST SP 800-53. This analysis is available on NIST's SP 800-53 site at: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final. Authors of control set documents must examine the analysis of revisions and should examine errata changes to identify any impacts to control selections in the control set document.

- ARC-IT 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 for typical threat sources and vulnerabilities that may be relevant or tailored to apply to ITS.
- NIST SP 800-82 for industrial control system (ICS)[5] threats and vulnerabilities that may be relevant or tailored to apply to ITS.
- MITRE ATT&CK® for ICS for threat sources' tactics techniques and procedures and mitigations that may also be relevant or tailor to apply to ITS.
- ITS Cybersecurity Framework Profile (ITS Profile) for prioritization of Subcategories mapped to security controls, which can be used to guide control specifications in this control set.

1.4 Relationship Between Control Sets and ARC-IT

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[6] 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 that plan, develop, operate, maintain, and use ITS. It defines stakeholder roles and the relationships between stakeholders. This is also the view where needs are defined since ARC-IT, and more broadly ITS, is driven by the needs of stakeholder organizations, their constituents, and customers.
- **Functional View** looks at ITS from a functional perspective. Functional requirements are defined that support ITS user needs. Processes and data flows provide a structured presentation of functions and interactions that support the requirements.

[5] NIST SP 800-82 Rev 2 is in revision and the scope is expanding to operational technology (OT).

[6] https://www.arc-it.net/html/security/deviceclasses.html.

- **Physical View** defines the physical objects (the systems and devices) that provide ITS functionality. Information flows define the flow of information between physical objects. Functional Objects organize the functionality that is required to support ITS within each physical object.
- **Communications View** defines how physical objects communicate. It defines communications standards and profiles that are combined into communications solutions that specify how information can be reliably and securely shared between physical objects.

Within ARC-IT, these views are presented in "service packages," which include the subset of ARC-IT that meets one or more user needs. A service package will include some number of physical objects. Each physical object may contain one or more functional objects defining ITS-specific functionality necessary to address those user needs. The physical objects are connected by information flows that can be implemented by the defined communications solutions. ARC-IT v9.1 has 152 service packages organized into 12 functional areas.[7]

Cybersecurity in ARC-IT[8] is addressed through the analysis of the confidentiality, integrity, and availability (C-I-A) required for information flows within each service package. Each information flow was scored using a Low-Moderate-High (L-M-H) rating. These ratings are then applied to the physical object where the information flow originates or ends, and a device security class is assigned to those objects. Because there could be 27 possible (and potentially untenable) combinations of L-M-H ratings over the C-I-A dimensions, ARC-IT groups the ratings into more manageable five device security classes.[9] Planners and engineers should select devices that are certified to meet the requirements for a class but could avoid the unnecessary expense of using devices that meet higher classes than necessary for an application.

Only the controls (primarily technical controls[10]) relevant to the *name of physical objects* are specified in this control set document. This approach is necessary to simplify and decrease the size of the document and to make the document more manageable and usable. The risk mitigation and protection provided by other controls implemented in larger systems, operations or data centers, or by the organizations operating ITS provide benefit to physical objects that are part of these larger systems, centers, or organizations. Control assessments of physical objects will be limited in scope, but owners, operators, and users of *name of physical objects* 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]

[7] https://www.arc-it.net/html/servicepackages/servicepackages-areaspsort.html.

[8] https://www.arc-it.net/html/security/security.html.

[9] https://www.arc-it.net/html/security/deviceclasses.html.

[10] The technical controls are typically implemented by systems rather than by people.

[11] Risk management processes are identified in the NIST Risk Management Framework (RMF); see NIST SP 800-39 and NIST SP 800-37.

Chapter 2. Physical Object Characteristics

INSTRUCTIONS: In this chapter, use the subsections to define/describe the physical object; identify the device security class by service package the physical object may support; identify the assumptions about or the characteristics of the physical object; and identify the threats, vulnerabilities, and predisposing conditions that justify the control specifications and the applicability of this control set document.

2.1 Definition/Description

INSTRUCTIONS: Provide as much detail as needed to describe the physical object, distinguish it from other physical objects, and clarify the scope of this document. Explain how the physical object is unique and, therefore, warrants this document and the control specifications. Any descriptive text should be consistent with the ARC-IT description of the physical object.

Describe the environment in which the physical object will be used (e.g., inside a locked cabinet in the field with a common and easily obtainable key, exposed to the environment near the roadside, in a mobile vehicle). Also include a description of the type of information that will be processed by the physical object. Describe the functionality of the physical object (e.g., type of technology, stand-alone, connected).

For example, a control set document based on the environment in which the physical object will operate should include details about the type and quality of connectivity, type of interface used, communications protocols, storage capacity, characteristics of the physical environment such as the power source and availability of other utilities, types of hazards in the environment, inventory of spare parts, and a description of any additional operating requirements.

A given physical object might be included in the implementation of many different systems; the definition/description of the physical object must be clear which implementations it covers. For instance, a single instance of "ITS Roadway Equipment" includes a traffic signal controller, its associated detector controllers as well as detectors, signal heads, conflict monitors, power supplies and some communications gear. Another implementation might be a dynamic message sign controller, and yet another might be an over-height detection system.

ARC-IT defines *name of physical object* as *description of the physical object*. The scope of this control set relevant to the physical object is *describe the scope*. The functions of this physical object include *describe the functional objects associated with this physical object*. The physical object operates in *describe the environment*. The types and quality of connectivity and interfaces required by this physical object include *describe the types and quality of connectivity and interfaces*. The information flows for this physical object include *describe the information flows*. The physical object may be included in the implementation of *describe the different systems*.

2.2 Physical Object Device Security Class by Service Package

Table 1 conveys that the *name of physical object* appears in *number of* service packages. This table also indicates the device security class (1-5) for each physical object based on its application within a specific service package. Users of this control set document should examine this table to identify the device security class for the physical object, then go to **Table 6** to determine which controls are necessary to protect that physical object as part of the service package.

Given a physical object may be used within multiple service packages, it is necessary to consider the impact of the physical object on the mission/functions the service package supports, which is addressed by aligning control specifications under the appropriate device security class in **Table 6**.

*INSTRUCTIONS: **Table 1** contains examples of two physical objects that appear in multiple service packages. They are Connected Vehicle Roadside Equipment (CVRSE) and ITS Roadway Equipment (ITSRE). Use this example only to understand how this table could be completed for the physical objects that are the subject of this document. Delete this data and replace it with data from ARC-IT that is specific to the subject physical objects.*

CAUTION: ARC-IT evolves with technology, standards, and changing concerns, so any information included in this document will age. The control set must be developed with an understanding of the services, and it is prudent to note the services so analyzed and the date. Matching the device security class to the physical object is most important, as a physical object's device security class might change in the future.

Table 1: Physical Object Device Security Class by Service Package

Service package	Device Security Class	
	CVRSE	ITSRE
Advanced Railroad Grade Crossing	5	5
Asset Tracking	2	
Automated Vehicle Operations	3	3
Border Management Systems	1	
Broadcast Traveler Information	2	
Commercial Vehicle Parking		2
Connected Eco-Driving	2	
Connected Vehicle System Monitoring and Management	5	
Connected Vehicle Traffic Signal System	3	3
Curve Speed Warning	2	2

Service package	Device Security Class	
	CVRSE	ITSRE
Data Distribution	4	3
Drawbridge Management		3
Dynamic Lane Management and Shoulder Use	2	3
Dynamic Roadway Warning		2
Eco-Approach and Departure at Signalized Intersections	3	3
Eco-Lanes Management	3	2
Eco-Traffic Metering	2	2
Eco-Traffic Signal Timing	2	3
Emergency Vehicle Preemption	3	3
Emissions Monitoring	2	2
Freight Signal Priority	3	3
HOV/HOT Lane Management	3	2
Incident Scene Safety Monitoring	3	2
Infrastructure Enhanced Cooperative Adaptive Cruise Control	3	3
Infrastructure Monitoring	5	4
Infrastructure-Based Traffic Surveillance		2
Integrated Multi-Modal Electronic Payment		
Intermittent Bus Lanes	3	2
Intersection Safety Warning and Collision Avoidance	3	3
In-Vehicle Signage	2	2
ITS Data Warehouse	1	2
Location and Time	5	5
Low Emissions Zone Management	2	2
Maintenance and Construction Signal Priority		3
Map Management	3	
Oversize Vehicle Warning	1	2
Parking Space Management	2	
Pedestrian and Cyclist Safety	3	3
Queue Warning	2	2

Service package	Device Security Class	
	CVRSE	ITSRE
Railroad Operations Coordination		2
Reduced Speed Zone Warning / Lane Closure	2	2
Regional Parking Management		2
Restricted Lane Warnings	2	2
Reversible Lane Management	1	4
Road Use Charging		
Road Weather Information for Freight Carriers	3	2
Road Weather Motorist Alert and Warning	3	2
Roadside Lighting	2	2
Roadway Automated Treatment		3
Roadway Closure Management	3	4
Roadway Maintenance and Construction		5
Roadway Micro-Prediction		3
Route ID for the Visually Impaired	2	
Signal Enforcement		2
Situational Awareness	1	
Smart Park and Ride System	2	
Speed Harmonization	2	2
Speed Warning and Enforcement	1	2
Spot Weather Impact Warning	3	2
Standard Railroad Grade Crossing		2
Stop Sign Gap Assist	5	5
Traffic Incident Management System		2
Traffic Information Dissemination		2
Traffic Metering		2
Traffic Signal Control		3
Transit Signal Priority	3	3
Transit Stop Request	4	
Transit Vehicle at Station/Stop Warnings	2	2

Service package	Device Security Class	
	CVRSE	ITSRE
Transportation Infrastructure Protection	3	5
Tunnel Management	2	5
Variable Speed Limits		2
Vehicle-Based Traffic Surveillance	2	
Weather Data Collection	2	3
Wide-Area Alert		2
Work Zone Management	2	2
Work Zone Safety Monitoring	3	2
Wrong Way Vehicle Detection and Warning	1	2

2.3 Assumptions and Characteristics

INSTRUCTIONS: Identify the assumptions and characteristics about physical objects that justify the control specifications and the applicability of this control set document. The assumptions relate to the environments in which physical objects operate; the nature of operations conducted by organizations; the functionality employed within systems; the types of assets to be protected, the types of threats facing organizations, missions/business processes, and systems; and the type of information processed, stored, or transmitted by systems.

If the examples in the bulleted list below are relevant to the physical objects which are the subject of this control set, use them as is or edit them to be more relevant.

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

- Systems are not always located in physical facilities.
- User data/information in organizational systems is not relatively persistent.
- Systems are not multi-user in operation or have no users.

- Systems exist in networked environments, but many ITS jurisdictions maintain their own communications infrastructure.[12]
- Systems are special purpose in nature.
- Organizations have the necessary structure, resources, and infrastructure to implement the controls.

INSTRUCTIONS: The following paragraphs discuss the examples of assumptions and characteristics listed above that are relevant to many ITS physical objects. If these examples are relevant to the physical objects which are the subject of this document, use them as is or edit them to be more relevant. Add any other assumptions and characteristics as necessary to fully explain how the physical objects are different from other technologies and, most importantly, to establish the essential foundation for selection of security controls. The justification for selecting a control later in this document can be traced back to this list of assumptions and characteristics.

Name of physical objects are not located in physical facilities; rather, they are deployed in remote and exposed environments, and this presents a set of risks not experienced in typical IT systems in physical facilities (e.g., Traffic Management Centers). From a risk management perspective, these physical objects are more akin to operational technology (OT) than to IT. For example, Physical and Environmental (PE) controls (e.g., gates, guards, humidity/temperature controls, fire detection and suppression, lighting) associated with a fixed facility cannot be implemented for *name of physical objects*. However, other PE controls that provide anti-tamper measures or tamper evidence and/or notification would be more appropriate, such as control enhancements addressing physical access (e.g., PE-3(4), Lockable Casings, and PE-3(5), Tamper Protection) or monitoring the environment (e.g., PE-14, Environmental Controls).

The data created or processed by *name of physical objects* are more perishable than persistent in nature and, therefore, may not require the same protections as persistent data. Also, the set of users of that data is far different for the physical objects. Most immediately there are non-human users of the data (e.g., other physical objects or vehicles), but that data may also be collected, correlated, analyzed, or otherwise processed for human consumption and decisions. However, it is possible the data is collected and used in a way not originally intended or for which ITS physical objects were designed; therefore, additional security protections may be necessary.

Name of physical objects exist in networked environments, but not necessarily in the same manner as typical information systems, and the physical objects may use different communications protocols. Secure communications are required to and from the equipment, especially considering the media may be wireless in many cases. Robust means of authentication and access control are required to ensure the

[12] This means there might not be a gateway to the Internet, or it might be behind many devices. The infrastructure is typically managed in-house or contracted to dedicated staff.

integrity and availability of signals and commands. The semi-autonomous operations of the *name of physical objects* may require increased levels of assurance of functionality.

Name of physical objects are not general purpose in nature; rather, they are highly specialized equipment that perform a limited set of functions. As such, many of the controls appropriate for typical IT systems are not required for physical objects to ensure confidentiality, integrity, and availability of the physical objects, the information they process, and the service packages and functions supported by the physical objects. These other controls are implemented by the larger system or organization that controls the physical objects, but some protections provided by the larger system or organization may be inherited by the *name of physical object*.

Larger organizations typically have the necessary structure, resources, and infrastructure to implement the required controls. However, the assumption can become an issue for nonfederal or smaller entities, such as municipalities and first responders. Such entities may not be large enough or sufficiently resourced to have elements dedicated to providing the range of security capabilities that are assumed by the controls. Organizations must consider such factors in their risk-based decisions, specifically in the selection of controls to mitigate risk.

2.4 Resources for Identifying Threats, Vulnerabilities, and Predisposing Conditions

INSTRUCTIONS: The content of this chapter is presented here because it flows logically with the process. But the tables in this chapter can be rather large; therefore, it may be more appropriate to provide the tables of threats, vulnerabilities, and predisposing conditions in an appendix rather than in the main body of the document. The main body can still be used to introduce the concepts at the appropriate point in the process flow but then point to the detailed content in the appendix.

A threat event is an event or situation that could potentially cause an undesirable consequence or impact to the physical objects resulting from some threat source, which exhibits a certain level of capability, intent, and targeting (adversarial) or range of effects (non-adversarial). An adversarial threat event is an event that is caused intentionally (by an adversary or other malicious entity) and could have negative impacts. A non-adversarial threat event is a threat associated with accident or human error, structural failure, or environmental causes[13].

ARC-IT explains that security threats are events or circumstances that adversely impact a surface transportation system or communication between systems. Threats cover a broad spectrum and include errors, fraud, disgruntled employees, fire, water damage, hackers, terrorist acts, viruses, and natural

[13] For more information regarding the types of threat sources and threat events as well as their relationship to the other risk factors (likelihood, vulnerabilities, impact) in the risk assessment process, refer to NIST SP 800-30.

disasters. For the ITS architecture, general threat categories are identified that encompass all these specific threats but allow threats to be categorized in a general way. The four general threat categories are as follows:

- *Deception: a circumstance or event that may result in an authorized entity receiving false data and believing it to be true.*
- *Disruption: a circumstance or event that interrupts or prevents the correct operation of system services and functions.*
- *Usurpation: a circumstance or event that results in control of system services or functions by an unauthorized entity.*
- *(Unauthorized) Disclosure: a circumstance or event whereby an entity gains access to data for which the entity is not authorized.*

The system implementer and system manager must ultimately identify and analyze specific threats to determine the likelihood of their occurrence and their potential to harm a specific ITS system. Security threats, along with security objectives (i.e., the need for confidentiality, integrity, and availability), provide the basis for evaluating appropriate security services.

*The threats most relevant to the physical objects are provided in **Table 2**, **Table 3**, and **Table 4**. The vulnerabilities and predisposing conditions in **Table 5** are grouped according to where they exist, such as in the organization's policy and procedures, or the inadequacy of security mechanisms implemented in hardware, firmware, and software. Policies and procedures (the first bullet below) are referred to as being in the organization while security mechanisms (in all the other bullets) are in or about the system. Understanding the source of vulnerabilities and predisposing conditions can assist in determining optimal mitigation strategies—it helps control set developers select the controls appropriate to mitigate risk to the physical objects. The groups of vulnerabilities are:*

- *Policy and Procedures*
- *System*
  - *Architecture and Design*
  - *Configuration and Maintenance*
- *Physical*
- *Software Development*
- *Communication and Network Configuration*

A broad set of adversarial and non-adversarial threat events that could potentially impact *name of physical objects* is provided in **Table 2** (adversarial) and **Table 3** (non-adversarial) below. The properties of *name of physical object* may also present unique opportunities to a threat source, specifically addressing how the threat source can manipulate the process of the *name of physical object* or the supported service package to cause physical damage. **Table 4** provides an overview of potential threat events more specific to the *name of physical object*.

Threat events listed below focus on the *name of physical objects*, not the larger system comprised of various types of physical objects and other components. Various threat events may ultimately impact a *name of physical object* or its mission/operations, either by compromise of the *name of physical object*

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 *name of physical object* can implement a protection measure to mitigate the risk will the threat be considered relevant to the *name of physical object* itself and, therefore, controls will be selected in this document to mitigate only those risks.

*INSTRUCTIONS: The information in **Table 2**, **Table 3**, **Table 4**, and **Table 5** leverages concepts from multiple NIST risk management resources. The tables use NIST SP 800-30 Appendix E, Threat Events, Appendix F, Vulnerabilities and Predisposing Conditions, to identify threats, vulnerabilities, and predisposing conditions relevant to physical objects that are the subject of the control set documents. For example, the threat events of "craft phishing attacks" and "create counterfeit/spoof websites" are not included as examples because they are not usually relevant to the ITS physical objects in question, as those physical objects don't usually provide email or web services.*

NIST SP 800-82 Appendix C, Threat Sources, Vulnerabilities, and Incidents, was also used to identify vulnerabilities specific to ITS physical objects, because ITS are similar to industrial control systems (ICS) and have similar risks. NIST SP 800-82 characterizes threat events in the categories of denial of control, manipulation of control, spoofed reporting message, theft of operational information, loss of safety, and loss of availability, many of which are a concern for ITS physical objects and, therefore, should be mitigated. Authors of control set documents should examine the construct and content of NIST SP 800-82 Appendix C to understand the context in which threats and vulnerabilities are discussed and, more importantly, to determine what content is relevant or not and what relevant content may need to be adapted to ITS physical objects. To the extent feasible, this template maintains the construct in NIST SP 800-82 to make it easier for authors to find the example content below in the tables and to organize the list of relevant threats and vulnerabilities. Not all the threats or vulnerabilities may be relevant to the subject physical objects; for example, higher level organizations or systems might more efficiently address policy and procedure or configuration and maintenance vulnerabilities. Note also that NIST SP 800-82 provides a control overlay that lists controls that mitigate risk to ICS. That overlay may be examined to identify controls that are relevant to ITS.

Because ITS are similar to ICS, the MITRE ATT&CK® for ICS is one risk-based resource that may be used to help identify controls necessary to mitigate some ITS risks. ATT&CK® for ICS is a knowledge base for observed cyber adversary behavior in the ICS technology domain. It reflects the various phases of an adversary's attack life cycle and the assets and systems they are known to target. The ATT&CK® for ICS Matrix provides an overview of the tactics[14] (the why) and techniques[15] (the how) described in the knowledge base and visually aligns individual techniques under the tactics in which they can be applied. A

[14] The tactics are: Initial Access, Execution, Persistence, Privilege Execution, Evasion, Discovery, Lateral Movement, Collection, Command and Control, Inhibit Response Function, Impair Process Control, Impact.

[15] Examples of techniques are Replication through Removable Media, Scripting, Project File Infection, Hooking, Masquerading, Wireless Sniffing, Exploitation of Remote Services, Man in the Middle, Connection Proxy, Data Destruction, Spoof Reporting Message, Loss of Safety.

catalog of attack techniques is provided which also maps the tactics to the techniques and provides a technical description of the techniques. Each technique is mapped to relevant mitigations which are mapped to security controls from NIST SP 800-53[16]. Not all ICS techniques will apply to ITS, but many can be leveraged to aid in the selection of controls that mitigate the techniques. Note also that ATT&CK[17] does not map mitigations to all control families or all controls within a given family, as the scope of ATT&CK is limited to the more technical controls (as opposed to management or operational controls) that are relevant to identified attack techniques. Developers of control sets must ultimately examine all the controls in the controls catalog in NIST SP 800-53 to select the complete set of controls that can mitigate the assessed risk then specify those controls in the Summary of Control Specifications *and the* Detailed Control Specifications *sections of the control set.*

***Table 2**, **Table 3**, **Table 4**, and **Table 5** list threats, vulnerabilities, or predisposing conditions from NIST SP 800-30 for general IT systems and from NIST SP 800-82 for OT that may also be relevant to ITS systems. Use the information in these tables only as an example. Be sure to adapt the information. For example, change "OT" to "ITS" or add or delete entries as appropriate to document the adversarial and non-adversarial threats and the vulnerabilities or predisposing conditions specific to the physical objects that are the subject of this control set document. Adjust the wording as necessary to be more relevant to ITS physical objects (e.g., change "primary facility" and "backup facility" to "primary location" and "backup location," because physical objects in the field are not necessarily housed in a facility). Retain the formatting and organization of the tables to ensure each type of threat or vulnerability is considered (may enter "None" where appropriate), and to promote consistency across control set documents.*

Table 2: Adversarial Threat Events

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	**Description**
Perform perimeter network reconnaissance/scanning.	Adversary uses commercial or free software to scan organizational perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks.
Perform network sniffing of exposed networks.	Adversary with access to exposed wired or wireless data channels used to transmit information, uses network sniffing to identify components, resources, and protections.
Gather information using open-	Adversary mines publicly accessible information to gather

[16] The relevant controls are identified in the information box in the top right-hand corner of each mitigation page. From the ATT&CK for ICS main page, navigate to the mitigation pages by selecting "Mitigations" from the left pane, or click on this link: https://collaborate.mitre.org/attackics/index.php/Mitigations. Then select a mitigation Name from the displayed table.

[17] MITRE ATT&CK® for ICS currently identifies 51 mitigations developed to lessen or eliminate the impact of attackers' techniques; there can be a many-to-many relationship between mitigations and techniques. Those mitigations are mapped to security controls, but that is only a subset of controls necessary to mitigate all risks to ITS, as ATT&CK® for ICS's scope does not include all control families.

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	Description
source discovery of organizational information.	information about organizational systems, business processes, users or personnel, or external relationships that the adversary can subsequently employ in support of an attack.
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.
Perform malware-directed internal reconnaissance.	Adversary uses malware installed inside the organizational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.
Craft phishing attacks.	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.
Craft spear phishing attacks.	Adversary employs phishing attacks targeted at high value targets (e.g., senior leaders/executives).
Craft attacks specifically based on deployed information technology environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organizational information technology environment.
Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.
Create and operate false front organizations to inject malicious components into the supply chain.	Adversary creates false front organizations with the appearance of legitimate suppliers in the critical life-cycle path that then inject corrupted/malicious system components into the organizational supply chain.
Deliver known malware to internal organizational information systems (e.g., virus via email).	Adversary uses common delivery mechanisms (e.g., email) to install/insert known malware (e. g., malware whose existence is known) into organizational information systems.
Deliver modified malware to internal organizational information systems.	Adversary uses common delivery mechanisms (e.g., email) to install/insert known malware (e. g., malware whose existence is known) into organizational information systems.
Deliver targeted malware for control of internal systems and exfiltration of data.	Adversary uses more sophisticated delivery mechanisms than email (e.g., web traffic, instant messaging, FTP) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems.
Deliver malware by providing removable media.	Adversary installs malware that is specifically designed to take control of internal organizational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions.
Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware or commercial information technology products. Adversary is not targeting specific organizations, simply looking for entry points into internal organizational information systems. Note

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	Description
	that this is particularly a concern for mobile applications.
Insert targeted malware into organizational information systems and information system components.	Adversary inserts malware into organizational information systems and information system components (e.g., commercial information technology products), specifically targeted to the hardware, software, and firmware used by organizations (based on knowledge gained via reconnaissance).
Insert specialized malware into organizational information systems based on system configurations.	Adversary inserts specialized, non-detectable, malware into organizational information systems based on system configurations, specifically targeting critical information system components based on reconnaissance and placement within organizational information systems.
Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.
Insert tampered critical components into organizational systems.	Adversary replaces, though supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.
Install general-purpose sniffers on organization-controlled systems or networks.	Adversary installs sniffing software onto internal organizational information systems or networks.
Install persistent and targeted sniffers on organizational information systems and networks.	Adversary places within internal organizational systems or networks software designed to (over a continuous period) collect (sniff) network traffic.
Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Adversary uses postal service or other commercial delivery services to deliver to organizational mailrooms a device that is able to scan wireless communications accessible from within the mailrooms and then wirelessly transmit information back to adversary.
Insert subverted individuals into organizations.	Adversary places individuals within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions.
Insert subverted individuals into privileged positions in organizations.	Adversary places individuals in privileged positions within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions. Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files) and may leverage access to one privileged capability to get to another capability.
Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware or commercial information technology products. Adversary is not targeting specific organizations, simply looking for entry points into internal organizational information systems. Note that this is particularly a concern for mobile applications.
Exploit physical access of authorized staff to gain access to organizational facilities.	Adversary follows (“tailgates”) authorized individuals into secure/controlled locations with the goal of gaining access to facilities, circumventing physical security checks.
Exploit poorly configured or	Adversary gains access through the Internet to systems that are not

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	Description
unauthorized systems exposed to the Internet.	authorized for Internet connectivity or that do not meet organizational configuration requirements.
Exploit split tunneling.	Adversary takes advantage of external organizational or personal information systems (e.g., laptop computers at remote locations) that are simultaneously connected securely to organizational information systems or networks and to nonsecure remote connections.
Exploit multi-tenancy in a cloud environment.	Adversary, with processes running in an organizationally-used cloud environment, takes advantage of multi-tenancy to observe behavior of organizational processes, acquire organizational information, or interfere with the timely or correct functioning of organizational processes.
Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones).	Adversary takes advantage of fact that transportable information systems are outside physical protection of organizations and logical protection of corporate firewalls, and compromises the systems based on known vulnerabilities to gather information from those systems.
Exploit recently discovered vulnerabilities.	Adversary exploits recently discovered vulnerabilities in organizational information systems in an attempt to compromise the systems before mitigation measures are available or in place.
Exploit vulnerabilities using zero-day attacks.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Zero-day attacks are based on adversary insight into the information systems and applications used by organizations as well as adversary reconnaissance of organizations.
Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	Adversary launches attacks on organizations in a time and manner consistent with organizational needs to conduct mission/business operations.
Exploit insecure or incomplete data deletion in multi-tenant environment.	Adversary circumvents or defeats isolation mechanisms in a multi-tenant environment (e.g., in a cloud computing environment) to observe, corrupt, or deny service to hosted services and information/data.
Compromise critical systems via physical access.	Adversary obtains physical access to organizational information systems and makes modifications.
Compromise systems or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organizations for purposes of subsequently infecting organizations when reconnected.
Compromise software of organizational critical information systems.	Adversary inserts malware or otherwise corrupts critical internal organizational information systems.
Compromise organizational information systems to facilitate exfiltration of data/information.	Adversary implants malware into internal organizational information systems, where the malware over time can identify and then exfiltrate valuable information.
Compromise mission-critical information.	Adversary compromises the integrity of mission-critical information, thus preventing or impeding ability of organizations to which information is supplied, from carrying out operations.

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	**Description**
Compromise design, manufacture, and/or distribution of system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.
Conduct communications interception attacks.	Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing publicly known flaws), targets those communications, and gains access to transmitted information and channels.
Conduct wireless jamming attacks.	Adversary takes measures to interfere with wireless communications 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 attacks leveraging traffic/data movement allowed across perimeter.	Adversary makes use of permitted information flows (e.g., email communication, removable storage) to compromise internal information systems, which allows adversary to obtain and exfiltrate sensitive information through perimeters.
Conduct simple Denial of Service (DoS) attack.	Adversary attempts to make an Internet-accessible resource unavailable to intended users or prevent the resource from functioning efficiently or at all, temporarily or indefinitely.
Conduct Distributed Denial of Service (DDoS) attacks.	Adversary uses multiple compromised information systems to attack a single target, thereby causing denial of service for users of the targeted information systems.
Conduct targeted DoS attacks.	Adversary targets DoS attacks to critical information systems, components, or supporting infrastructures, based on adversary knowledge of dependencies.
Conduct physical attacks on organizational facilities.	Adversary conducts a physical attack on organizational facilities (e.g., sets a fire).
Conduct physical attacks on infrastructures supporting organizational facilities.	Adversary conducts a physical attack on one or more infrastructures supporting organizational facilities (e.g., breaks a water main, cuts a power line).
Conduct cyber-physical attacks on organizational facilities.	Adversary conducts a cyber-physical attack on organizational facilities (e.g., remotely changes HVAC settings).
Conduct data scavenging attacks in a cloud environment.	Adversary obtains data used and then deleted by organizational processes running in a cloud environment.
Conduct brute force login attempts/password guessing attacks.	Adversary attempts to gain access to organizational information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.
Conduct nontargeted zero-day attacks.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Attacks are not based on any adversary insights into specific vulnerabilities of organizations.
Conduct externally based session hijacking.	Adversary takes control of (hijacks) already established, legitimate information system sessions between organizations and external entities (e.g., users connecting from off-site locations).
Conduct internally based session	Adversary places an entity within organizations in order to gain

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	Description
hijacking.	access to organizational information systems or networks for the express purpose of taking control (hijacking) an already established, legitimate session either between organizations and external entities (e.g., users connecting from remote locations) or between two locations within internal networks.
Conduct externally based network traffic modification (man in the middle) attacks.	Adversary, operating outside organizational systems, intercepts/eavesdrops on sessions between organizational and external systems. Adversary then relays messages between organizational and external systems, making them believe that they are talking directly to each other over a private connection, when in fact the entire communication is controlled by the adversary. Such attacks are of particular concern for organizational use of community, hybrid, and public clouds.
Conduct internally based network traffic modification (man in the middle) attacks.	Adversary operating within the organizational infrastructure intercepts and corrupts data sessions.
Conduct outsider-based social engineering to obtain information.	Externally placed adversary takes actions (e.g., using email, phone) with the intent of persuading or otherwise tricking individuals within organizations into revealing critical/sensitive information (e.g., personally identifiable information).
Conduct insider-based social engineering to obtain information.	Internally placed adversary takes actions (e.g., using email, phone) so that individuals within organizations reveal critical/sensitive information (e.g., mission information).
Conduct attacks targeting and compromising personal devices of critical employees.	Adversary targets key organizational employees by placing malware on their personally owned information systems and devices (e.g., laptop/notebook computers, personal digital assistants, smart phones). The intent is to take advantage of any instances where employees use personal information systems or devices to handle critical/sensitive information.
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom systems and components.
Obtain sensitive information through network sniffing of external networks.	Adversary with access to exposed wired or wireless data channels that organizations (or organizational personnel) use to transmit information (e.g., kiosks, public wireless networks) intercepts communications.
Obtain sensitive information via exfiltration.	Adversary directs malware on organizational systems to locate and surreptitiously transmit sensitive information or insider manually exfiltrates data.
Cause degradation or denial of attacker-selected services or capabilities.	Adversary directs malware on organizational systems to impair the correct and timely support of organizational mission/business functions.
Cause deterioration/destruction of critical system components and functions.	Adversary destroys or causes deterioration of critical system components to impede or eliminate organizational ability to carry out missions or business functions. Detection of this action is not a

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	**Description**
	concern.
Cause integrity loss by polluting or corrupting critical data.	Adversary implants corrupted and incorrect data in critical data, resulting in suboptimal actions or loss of confidence in organizational data/services.
Obtain sensitive information through network sniffing of external networks.	Adversary with access to exposed wired or wireless data channels that organizations (or organizational personnel) use to transmit information (e.g., kiosks, public wireless networks) intercepts communications.
Cause integrity loss by injecting false but believable data into organizational information systems.	Adversary injects false but believable data into organizational information systems, resulting in suboptimal actions or loss of confidence in organizational data/services.
Obtain information by externally located interception of wireless network traffic.	Adversary intercepts organizational communications over wireless networks. Examples include targeting public wireless access or hotel networking connections, and drive-by subversion of home or organizational wireless routers.
Cause disclosure of critical and/or sensitive information by authorized users.	Adversary induces (e.g., via social engineering) authorized users to inadvertently expose, disclose, or mishandle critical/sensitive information.
Cause unauthorized disclosure and/or unavailability by spilling sensitive information.	Adversary contaminates organizational information systems (including devices and networks) by causing them to handle information of a classification/sensitivity for which they have not been authorized. The information is exposed to individuals who are not authorized access to such information, and the information system, device, or network is unavailable while the spill is investigated and mitigated.
Obtain information by externally located interception of wireless network traffic.	Adversary intercepts organizational communications over wireless networks. Examples include targeting public wireless access or hotel networking connections, and drive-by subversion of home or organizational wireless routers.
Obtain unauthorized access.	Adversary with authorized access to organizational systems, gains access to resources that exceeds authorization.
Obtain sensitive data/information from publicly accessible information systems.	Adversary scans or mines information on publicly accessible servers and web pages of organizations with the intent of finding 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.
Obfuscate adversary actions.	Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations.
Adapt cyber attacks based on detailed surveillance.	Adversary adapts behavior in response to surveillance and organizational security measures.
Coordinate a campaign of multi-staged attacks (e.g., hopping).	Adversary moves the source of malicious commands or actions from one compromised information system to another, making analysis difficult.
Coordinate a campaign that	Adversary combines attacks that require both physical presence

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	Description
combines internal and external attacks across multiple information systems and information technologies.	within organizational facilities and cyber methods to achieve success. Physical attack steps may be as simple as convincing maintenance personnel to leave doors or cabinets open.
Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome.	Adversary does not limit planning to the targeting of one organization. Adversary observes multiple organizations to acquire necessary information on targets of interest.
Coordinate a campaign that spreads attacks across organizational systems from existing presence.	Adversary uses existing presence within organizational systems to extend the adversary's span of control to other organizational systems including organizational infrastructure. Adversary thus is in position to further undermine organizational ability to carry out missions/business functions.
Coordinate a campaign of continuous, adaptive, and changing cyber attacks based on detailed surveillance.	Adversary attacks continually change in response to surveillance and organizational security measures.
Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organizational operations.

Table 3 provides a high-level characterization of non-adversarial threat events as adapted from NIST SP 800-30. 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.

*INSTRUCTIONS: Adjust the wording in **Table 3** as necessary to be more relevant. Most importantly, add or subtract entries as appropriate to document the non-adversarial threat events specific to the physical objects that are the subject of this control set document.*

Table 3: Non-Adversarial Threat Events

Threat Event	Description
Spill sensitive information	Authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
Mishandling of critical and/or sensitive information by authorized users	Authorized privileged user inadvertently exposes critical/sensitive information.
Incorrect privilege settings	Authorized privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too

	low.
Communications contention	Degraded communications performance due to contention.
Unreadable display	Display unreadable due to aging equipment.
Earthquake at primary facility[18]	Earthquake of organization-defined magnitude at primary facility makes facility inoperable.
Fire at primary facility	Fire (not due to adversarial activity) at primary facility makes facility inoperable.
Fire at backup facility	Fire (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Flood at primary facility	Flood (not due to adversarial activity) at primary facility makes facility inoperable.
Flood at backup facility	Flood (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Hurricane at primary facility	Hurricane of organization-defined strength at primary facility makes facility inoperable.
Hurricane at backup facility	Hurricane of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Resource depletion	Degraded processing performance due to resource depletion.
Introduction of vulnerabilities into software products	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.
Disk error	Corrupted storage due to a disk error.
Pervasive disk error	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.
Windstorm/tornado at primary facility	Windstorm/tornado of organization-defined strength at primary facility makes facility inoperable.
Windstorm/tornado at backup facility	Windstorm/tornado of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.

Table 4 provides an overview of potential threat events that are specific to and even more relevant to the *name of physical object* than the general threats listed in **Table 2** and **Table 3** above. These physical object threat events are adapted from NIST SP 800-82 which addresses ICS, as ICS are similar in nature and operations to ITS physical objects.

*INSTRUCTIONS: The threat events from NIST SP 800-82 in **Table 4** are examples only. Adjust the wording in **Table 4** to be more relevant to the control set topic. Most importantly, add or subtract entries*

[18] In the context of ITS, this is the primary location of the physical objects in the field, not necessarily a facility that houses typical IT.

as appropriate to document the threat events specific to the physical objects that are the subject of this control set document.

Table 4: 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 5 includes or adapts vulnerabilities and predisposing conditions from NIST SP 800-82. 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.

*INSTRUCTIONS: Adjust the wording from NIST SP 800-82 in **Table 5** as necessary to be more relevant. Most importantly, add or subtract entries as appropriate to document the vulnerabilities and predisposing conditions specific to the physical objects that are the subject of this control set document.*

Table 5: Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Inadequate organizational	Risk assessments should be performed with acknowledgement from

Vulnerability	Description
ownership of risk assessments	appropriate levels within the organization. Lack of understanding of risk could lead to under-mitigated scenarios or inadequate funding and selection of controls.
Inadequate security policy for ITS	Vulnerabilities are often introduced into the ITS environment due to inadequate policies or the lack of policies specifically for ITS security. Controls and countermeasures should be derived from a risk assessment or policy. This ensures uniformity and accountability.
Inadequate ITS security training and awareness program	A documented formal ITS security training and awareness program is designed to keep staff up to date on organizational security policies and procedures as well as 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.
Lack of inventory management policy	Inventory policy and procedures should include installation, removal, and changes made to hardware, firmware, and software. An incomplete inventory could lead to unmanaged and unprotected devices within the ITS environment.
Lack of configuration management policy	Lack of policy and procedures for ITS configuration management can lead to an unmanageable and highly vulnerable inventory of hardware, firmware, and software.
Inadequate organizational ownership of risk assessments	Risk assessments should be performed with acknowledgement from appropriate levels within the organization. Lack of understanding of risk could lead to under-mitigated scenarios or inadequate funding and selection of controls.
Inadequate incident detection & response plan and procedures	Incident detection and response plans, procedures, and methods are necessary for rapidly detecting incidents, minimizing loss and destruction, preserving evidence for later forensic examination, mitigating the weaknesses that were exploited, and restoring services. Establishing a successful incident response capability includes continually monitoring for anomalies, prioritizing the handling of incidents, and implementing effective methods of collecting, analyzing, and reporting data.
Lack of redundancy for critical components	Lack of redundancy in critical components could provide single point of failure possibilities.
Inadequate incorporation of security into architecture and design.	Incorporating security into the physical object architecture, design must start with budget, and schedule of the physical object. The security architecture is part of the Enterprise Architecture. The architectures must address the identification and authorization of users, access control mechanism, network topologies, and system configuration and integrity mechanisms.
Inadequate management of change allowing insecure architecture to evolve	The network infrastructure within the ITS environment has often been developed and modified based on business and operational requirements, with little consideration for the potential security impacts of the changes. Over time, security gaps may have been inadvertently introduced within the infrastructure. Without remediation, these gaps may represent backdoors into the ITS. Sensors and controllers that were historically simple devices are now often manufactured as intelligent devices. In some cases, sensors and controllers may be replaced with IIoT devices which allow direct internet connections. Security should be incorporated into change management for all ITS devices, not just traditional IT components.

Vulnerability	Description
No security perimeter defined	If the ITS or physical object does not have a security perimeter clearly defined, then it is not possible to ensure that the necessary controls are deployed and configured properly. This can lead to unauthorized access to systems and data, as well as other problems.
Control networks used for non-control traffic	Control and non-control traffic have different requirements, such as determinism and reliability, so having both types of traffic on a single network makes it more difficult to correctly configure the network so that it meets the requirements of the control traffic, and that complexity can create undue risk. For example, non-control traffic could inadvertently consume resources that control traffic needs, causing disruptions in physical object functions. There may also be the potential for lateral movement from the non-control traffic to the control traffic, which could lead to hijacking or other types of attacks.
Control network services dependent on a non-control network	When IT services such as Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) are used by control networks, they are often implemented in the IT network. This causes the ITS network to become dependent on the IT network, which may not have the reliability and availability requirements needed by ITS.
Inadequate collection of event data history	Forensic analysis depends on collection and retention of enough data. Without proper and accurate data collection, it might be impossible to determine what caused a security incident to occur. Incidents might go unnoticed, leading to additional damage and/or disruption. Regular monitoring is also needed to identify problems with controls, such as misconfigurations and failures.
Hardware, firmware, and software not under asset 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 not under configuration management	The organization doesn't 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 (OS) and vendor software patches may not be developed until significantly after security vulnerabilities are found.	Because of the tight coupling between ITS software and the underlying ITS, changes must undergo expensive and time-consuming comprehensive regression testing. The elapsed time for such testing and subsequent distribution of updated software provides a long window of vulnerability. Vulnerability management procedures should include flexibility for interim alternative mitigations.
Vendor declines to develop patches for vulnerability	Out-of-date OSs and applications may contain newly discovered vulnerabilities that could be exploited. Security patch support may not be available for legacy ITS, so vulnerability management procedures should include contingency plans for mitigating vulnerabilities where patches

Vulnerability	Description
	may never be available or replacement plans.
Lack of a vulnerability management program	Vulnerabilities not considered by the organization could result in exploitation. Vulnerability management procedures should be in place to determine a plan of action or inaction upon discovery of a vulnerability. Some ITS considerations are: availability concerns may push patching until the next planned operational downtime; security patch support may not be available for ITS systems that use outdated OSs; isolated systems may not require immediate patching; and ITS exposed to the internet may need prioritized for patching.
Inadequate testing of security changes	Modifications to hardware, firmware, and software deployed without testing could compromise normal operation of the ITS. Documented procedures should be developed for testing all changes for security impact. The live operational systems should never be used for testing. The testing of system modifications may need to be coordinated with system vendors and integrators.
Poor remote access controls	There are many reasons why an ITS may need to be remotely accessed, including vendors and system integrators performing system maintenance functions, and also ITS engineers accessing geographically remote system components. The concept of least privilege should be applied to remote access controls. Remote access capabilities must be adequately controlled to prevent unauthorized individuals from gaining access, or authorized individuals from gaining excessive access, to the ITS.
Poor configurations are used	Improperly configured systems may leave unnecessary ports and protocols open. These unnecessary functions may contain vulnerabilities that increase the overall risk to the system. Using default configurations often exposes vulnerabilities and exploitable services. All settings should be examined.
Critical configurations are not stored or backed up	Procedures should be available for restoring ITS configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent loss of data. Documented procedures should be developed for maintaining configuration settings.
Data unprotected on portable device	If sensitive data (e.g., passwords, dial-up numbers) are stored cleartext on portable devices such as laptops and mobile devices and these devices are lost or stolen, system security could be compromised. Policy, procedures, and mechanisms are required for protection.
Vendor default passwords are used	Most vendor default passwords are easy to discover within vendor product manuals, which are also available to adversaries. Using the default password can drastically increase ITS vulnerability.
Passwords generation, use, and protection not in accord with policy	Password policy and procedure must be followed to be effective. Violations of password policy and procedures can increase physical object vulnerability.
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 situation

Vulnerability	Description
Improper data linking	ITS data storage systems may be linked with non-ITS data sources. An example of this is database links, which allow data from one database (e.g., data historian) to be automatically replicated to others. Data linkage may create a vulnerability if it is not properly configured and may allow unauthorized data access or manipulation.
Malware protection 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.
Malware protection implemented without sufficient testing	Malware protection software deployed without sufficient testing could impact normal operation of the ITS and block the system from performing necessary control actions.
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.
Intrusion detection/prevention software not installed	Incidents can result in loss of system availability and integrity; the capture, modification, and deletion of data; and incorrect execution of control commands. Intrusion Detection System / Intrusion Protection System (IDS/IPS) software may stop or prevent various types of attacks, including DoS attacks, and identify attacked internal hosts, such as those infected with worms. IDS/IPS software must be tested prior to deployment to determine that it does not compromise normal operation of the physical object.
Logs not maintained	Without proper and accurate logs, it might be impossible to determine what caused a security event to occur and perform adequate forensics.
Unauthorized personnel have physical access to equipment	Physical access to physical object equipment should be restricted to only the necessary personnel, considering safety requirements, such as emergency shutdown or restarts. Unauthorized access to physical object equipment can lead to any of the following: • Physical theft of data and hardware • Physical damage or destruction of data and hardware • Modification of the operational process • Unauthorized changes to or uses of the functional environment (e.g., data connections use of removable media, adding/removing resources) • Disconnection of physical data links • Undetectable interception of data (keystroke and other input logging)
Radio frequency, electromagnetic pulse (EMP), static discharge, brownouts, and voltage spikes	Without proper shielding, grounding, power conditioning, and/or surge suppression, some hardware used for control systems is vulnerable to radio frequency and EMP, static discharge, brownouts, and voltage spikes. The impact can range from temporary disruption of command and control to permanent damage to circuit boards.
Lack of backup power	Without backup power to critical assets, a general loss of power will shut down the physical object 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	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; some may continue to operate but in a minimal capacity and may produce intermittent errors, continually reboot, or become permanently inoperable.
Unsecured physical ports	Unsecured universal serial bus and IBM personal system 2 ports could allow unauthorized connection of thumb drives, keystroke loggers, etc.
Improper Data Validation	Physical object software may not properly validate received data to ensure validity. Invalid data may result in numerous vulnerabilities including buffer overflows, command injections, cross-site scripting, and path traversals.
Installed security capabilities not enabled by default	Security capabilities that were installed with the product are useless if they are not enabled or at least identified as being disabled.
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 not employed	Data flow controls, based on data characteristics, are needed to restrict which information is permitted between systems. These controls can prevent illegal operations.
Firewalls nonexistent or improperly configured	A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and corporate networks, allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping, and providing individuals with unauthorized access to systems.
Inadequate firewall and router logs	Without proper and accurate logs, it might be impossible to determine what caused a security incident to occur.
Standard, well-documented communication protocols are used in plain text	Adversaries that can monitor the physical object network activity, can use a protocol analyzer or other utilities to decode the data transferred by protocols such as telnet, File Transfer Protocol, Hypertext Transfer Protocol, and Network File System. The use of such protocols also makes it easier for adversaries to perform attacks against the physical object and manipulate physical object network activity.
Authentication of users, data or devices is substandard or nonexistent	Without authentication, there is the potential to replay, modify, or spoof data; or to spoof device identities or user identities; or masquerade devices.
Use of unsecure ITS protocols	ITS protocols often have few or no security capabilities, such as authentication and encryption, to protect data from unauthorized access or tampering. Also, incorrect implementation of the protocols can lead to additional vulnerabilities.
Lack of integrity checking for communications	Adversaries could manipulate communications undetected. To ensure integrity, the physical object can use lower-layer protocols (e.g., IPsec) that offer data integrity protection when traversing untrusted physical media.
Inadequate authentication between clients and servers over wireless connection	Strong mutual authentication between clients and servers is needed to ensure legitimate clients do not connect to a rogue access point deployed by an adversary, and to ensure adversary clients do not connect to any of the ITS's wireless networks.
Inadequate data protection between clients and	Sensitive data between clients and servers should be protected using strong encryption to ensure that adversaries cannot gain unauthorized

Vulnerability	Description
servers over wireless connection	access to the unencrypted data.
Unauthorized physical access to sensors or final elements	Physical access to sensors and final elements allows for direct manipulation of the physical process. Many smart devices are configured on a fieldbus such that electronic access to the sensor network allows for manipulation of controlling parameters. Physical access to the whole of the loop should be managed to prevent incidents.
Unauthorized wireless access to sensors or final elements[19]	Wireless access to sensors and final elements allows for direct manipulation of the physical process. Many smart devices allow for wireless configuration (e.g., Bluetooth, Wi-Fi, WirelessHART). Wireless access should be securely configured or disabled using hardware write-protect where possible to protect unauthorized modification of the sensors and final elements which are connected both to the physical process and to the physical object environment.
Inappropriate segmentation of asset management system	Most architectures are designed for PLCs, RTUs, DCS, and SCADA controllers to manipulate the process, and for asset management systems to monitor the assets connected to the controllers. Many asset management systems also have the technical ability to modify the configuration of sensors and final elements, although modification may not be their primary function. The asset management system should be controlled appropriately based on its ability (or lack of ability) to manipulate the process.

[19] Examples of sensors are cameras, induction loops, or anything that can be used to detect the presence of people or vehicles, vehicle motion, speed, direction, weight, etc. Examples of final elements are the things that are being controlled, such as red-yellow-green (R-Y-G) lights, pedestrian crossing signals, gates, scales, red light/stop sign/speed cameras, overhead message signs, variable speed or lane direction signs, etc.

Chapter 3. Summary of Control Specifications

This control set specifies the base controls and enhancements for *name of physical object*, per device security class with consideration for the impact a compromise of the security objectives (i.e., confidentiality, integrity, and availability) would have on a service package. The controls are specified primarily if the physical object or the physical object developer can implement the controls to mitigate the risk specific to the physical object. That is, primarily technical controls are selected. The presumption is that the organization that owns the larger system, of which the physical object is a part, will implement the non-technical controls to further protect the physical objects.

Table 6 below contains a summary of the control specifications as they apply in this control set document. The symbols used in the table are as follows:

*INSTRUCTIONS: Not all the symbols below must be used in each control set document. Leave this chapter as is until **Table 6** is completed, then determine which symbols were not used and delete those lines immediately below.*

*For a more detailed explanation of each of the symbols listed immediately below, see the set of instructions at the beginning of **Chapter 4, Detailed Control Specifications**.*

- "NS" indicates the control is not selected. This would be used only if multiple columns are used to convey the disparate control specifications for more than one physical object in the same table.
- "G" indicates there is guidance for the control, including specific applicability guidance or possibly implementation tailoring guidance.
- "V" indicates this control set document defines a value for an ITS-specific parameter for the control[20], 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 best practices.
- "R" indicates there is at least one risk reference or resource that informs the control selection
- "S" indicates there is a standard or best practice that the control helps to meet.

[20] 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.

- "M" indicates the control is implemented by the manufacturer of the physical object.
- "I" indicates the control is implemented by the IOO organization.
- "M/I" indicates the control is implemented by the manufacturer and the IOO organization.

INSTRUCTIONS: This template contains a limited control selection as a notional example. Only a sampling of control families is included. Base controls are in bold text and the control enhancements are not bold to help identify the parent-child relationships.

NIST SP 800-53 uses the construct of base controls and enhancements to the base controls. Enhancements are statements of security capability to build in additional, but related, functionality to a base control and/or increase the strength of a base control. For example, SC-8, Transmission Confidentiality and Integrity, requires basic protection of the confidentiality and/or integrity of transmitted information but doesn't necessarily specify the physical or logical means to achieve that protection; the discussion that accompanies the control text simply provides examples of how to provide the protection. However, SC-8(1), Transmission Confidentiality and Integrity | Cryptographic Protection, is more robust and specific, in that it specifies encryption as the means to achieve the desired level of protection.

The ellipsis on a line indicates not all controls in each family are listed nor are all families represented in this example, but all families and controls should be examined for selection. This is only an example to illustrate the construct for listing relevant controls for a given physical device.

*Use the information in **Chapter 2.3, Assumptions and Characteristics**, above to understand the unique characteristics of the subject physical device and, therefore, the unique risks (i.e., the pairings of threats against vulnerabilities and/or predisposing conditions) that must be mitigated by or for the physical object, either by the manufacturer of the physical object or by the IOO organization that ultimately owns or operates the physical object (enter the appropriate values of "M", "I", or "M/I" in the last column).*

Compare the risks against the controls and control enhancements in NIST SP 800-53 to determine which controls and enhancements individually or in combination will mitigate the risks. Also indicate which of those controls and enhancements are appropriate for each of the five device security classes. The more robust security controls are typically selected for the higher device security classes, based on risk tolerance and cost/benefit analyses.

The ITS Profile informs control selection decisions by linking ITS-related Mission Objectives to cybersecurity activities and outcomes (Cybersecurity Framework Subcategories) and controls in NIST SP 800-53 that help organizations achieve those activities and outcomes. Reference the ITS Profile to determine which Subcategories and, therefore, Informative References (e.g., security controls[21]) have been prioritized by the organization that owns the physical objects. For example, if the Subcategory of

[21] Informative References map to NIST SP 800-53 Rev 5 controls; see: https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/csf-pf-to-sp800-53r5-mappings.xlsx

DE.CM-4 "Malicious code is detected" has a high priority in the ITS Profile, it is necessary to understand which security controls (i.e., SC-18, SC-44, and SI-4) under Informative References support that Subcategory so the controls can be appropriately weighed for applicability to a physical object in each device security class.

ARC-IT may be used to inform control selections but should not be viewed as a constraining factor (https://www.arc-it.net/html/security/deviceclasses.htm, and click on each Device Class to examine a list of controls). Within ARC-IT click on the Device Class to understand which control families may be relevant at each Device Class levels 1-5. ARC-IT does not provide control-level recommendations for every physical object. ARC-IT provides control-level recommendations for only three physical objects: CVRSE, ITSRE, and Vehicle On-board Equipment (OBE).

Due to the nature of physical objects and the operational environment, implementation of selected controls may need to deviate from implementations for typical information systems, as is described in the Discussion element[22] for each control in NIST SP 800-53. Unique implementations are described in the guidance provided in **Chapter 4, Detailed Control Specifications**, of this control set document. The last column of **Table 6** below indicates if the control should be implemented by the manufacturer within or for the physical object and by the IOO organization. Allocation of responsibility for the controls may be different than what is implied in the control text in NIST SP 800-53, in that the device itself may need to implement controls typically implemented by the organization, or vice versa.

Table 6: Control Specifications by Device Security Class *Name of Physical Object*[23]

ID	TITLE	Device Security Class					Responsibility: Manufacturer (M) IOO (I)
		1	2	3	4	5	
AC-1	**(Access Control) Policy and Procedures**	G	G	G	G	G	I
AC-2	**Account Management**	GR	GR	GR	GR	GR	I
AC-2(1)	Automated System Account Management	NS	GR	GR	GR	GR	I
AC-2(2)	Removal of Temporary and Emergency Accounts	NS	VRS	VRS	VRS	VRS	M

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

[23] The contents of this table are notional and must be adapted to suit the needs of the authors of the control set documents.

ID	TITLE	Device Security Class					Responsibility: Manufacturer (M) IOO (I)
		1	2	3	4	5	
AC-2(3)	Disable Accounts	NS	VR	VR	VR	VR	M
AC-2(4)	Automated Audit Actions	G	G	G	G	G	M
AC-2(5)	Inactivity Logout	GV	GV	GV	GV	GV	I
AC-2(7)	Role-Based Schemes	GVR	GVR	GVR	GVR	GVR	I
AC-2(9)	Restrictions on Use of Shared and Group Accounts	G	G	G	G	G	I
AC-2(10)	Shared and Group Account Credential Change	GR	GR	GR	GR	GR	M
AC-2(11)	Usage Conditions	NS	NS	NS	GV	GV	M/I
…							
PE-1	**(Physical and Environmental Protection) Policy and Procedures**	G	G	G	G	G	I
PE-2	**Physical Access Authorizations**	GR	GR	GR	GR	GR	I
PE-3	**Physical Access Control**	GVR	GVR	GVR	GVR	GVR	I
PE-3(1)	System Access	G	G	G	G	G	M/I
PE-3(4)	Lockable Casings	GV	GV	GV	GV	GV	M/I
PE-3(5)	Tamper Protection	NS	NS	V	V	V	M/I
PE-3(7)	Physical Barriers	NS	NS	GR	GR	GR	I
…							

ID	TITLE	Device Security Class					Responsibility: Manufacturer (M) IOO (I)
		1	2	3	4	5	
SA-1	**(System and Services Acquisition) Policy and Procedures**	G	G	G	G	G	I
SA-2	**Allocation of Resources**	G	G	G	G	G	I
SA-3	**System Development Life Cycle**	G	G	G	G	G	I
SA-3(1)	Manage Development Environment	G	G	G	G	G	M/I
SA-3(2)	Use of Live Data	G	G	G	G	G	M/I
SA-3(3)	Technology Refresh	G	G	G	G	G	M/I
…							
SC-1	**(System and Communications Protection) Policy and Procedures**	G	G	G	G	G	I
SC-2	**Application Partitioning**	NS	G	G	G	G	M/I
SC-3	**Security Function Isolation**	NS	NS	NS	G	G	M/I
SC-4	**Information in Shared System Resources**	NS	GR	GR	GR	GR	M/I
SC-5	**Denial of Service Protection**	GV	GV	GV	GV	GV	M/I
SC-8	**Transmission Confidentiality and Integrity**	NS	VR	VR	VR	VR	M
SC-8(1)	Cryptographic Protection	NS	VR	VR	VR	VR	M
SC-10	**Network Disconnect**	GR	GR	GR	GR	GR	M

ID	TITLE	Device Security Class					Responsibility: Manufacturer (M) IOO (I)
		1	2	3	4	5	
SC-13	**Cryptographic Protection**	NS	GR	GR	GR	GR	M
…							

Chapter 4. Detailed Control Specifications

*INSTRUCTIONS: This chapter is a comprehensive view of controls shown in **Table 6**.*

Elaborate on guidance given in NIST SP 800-53 to provide ITS-specific details. The examples provided below are a subset of the examples provided in Table 6, and some content is notional/fictitious for demonstration purposes only; delete any irrelevant or fictitious information and replace it with real information. Follow the prescribed format in the examples below, but omit portions that are not relevant (e.g., not every control will have a risk reference or resource associated with them.

*For controls selected in **Chapter 3, Summary of Control Specifications**, indicate the part responsible for implementing the control. The options are the manufacturer (M), the IOO (I), or both (M/I).*

*Provide a Justification to Select based on physical object characteristics, risks (i.e., threat sources/events that may exploit vulnerabilities or predisposing conditions), ITS Profile priorities, etc. described in **Chapter 1, Identification**. These justifications are usually required, but on occasion a control may only have guidance as its applicability is not absolute. That guidance must be designed to help users of the control set document understand under what circumstances the control is applicable.*

In addition to the Justification to Select specification, a control may have other specifications that include Guidance (including specific tailoring guidance); Parameter Values; and Risk References and Resources, and Standards). These specifications are not mandatory but should be listed to help explain the need for the control, its unique implementation in the ITS environment, parameter values unique to ITS physical objects, or required ITS standards or best practices. If one or more of these specifications (, Guidance, Parameter Values, Risk References or Resources, or Standards) is not relevant to a given control, do not include that specification heading after the Justification to Select heading. Examples below illustrate this construct where some controls have more or fewer types of specifications.

In some cases, the Discussion from NIST SP 800-53 for selected controls and enhancements should be modified to address the characteristics of the subject physical objects and the environments in which they operate. The Guidance element herein can also provide tailoring guidance as to why a particular control or control enhancement may not be applicable in some environments and offer suggestions for compensating controls, as appropriate.

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 to fully understand the meaning.

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

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

If a control has a parameter value in paragraph a. and paragraph c. for which values are being provided, but no parameter value to define for paragraph b., then the notation will identify only paragraph a. and c. and will not contain a reference to paragraph b.

Where multiple values may be defined within a paragraph or subparagraph, their position will be noted using 1st PV or 2nd PV as appropriate. If the parameter value contains no annotation regarding its placement, then this indicates there is only one value to define for the control and annotation of its placement within the control is not needed. It should be noted that sometimes a parameter value begins with the word “a” which should not be confused with a paragraph annotation of “a.”

Example parameter values set below are placed in italics. The actual values must be set by the group developing the control set document. Leave the values in italics so users of the control set document know that the text is a parameter value provisionally set by the authors of the control set document, but that the value might be further adjusted based on policy or local risk. Review NIST SP 800-53 to understand the range or options for the parameter values.

The term "standard" is used within the context of information security policies to distinguish between written policies, standards, and procedures. Organizations should maintain all three types of documentation to help secure their environment. Information security policies are high-level statements or rules about protecting people or systems (e.g., "the organization will maintain secure passwords” or “systems must be interoperable"). A "standard" provides a detailed description of required product features or functionality (e.g., password length/complexity, interoperability with other products in that ecosystem regardless of manufacturers). A "procedure" can describe a step-by-step method to implement various standards (e.g., "the organization will enable password length controls on all production systems").

If a control is selected to help comply with a standard; align with a best practice, guidance, or recommendations; etc., list the standard, ideally including the paragraph to aid in identifying and evaluating the relevance to physical objects that are the subject of this control set document. The examples below indicate to which types of ITS the reference applies, such as Traffic Management Centers (TMC), ITSRE, or Roadside Equipment (RSE), but those parenthetical annotations need not be included in the final control set document. Examples of potentially relevant standards, best practices, etc., might include:

- *National Electrical Manufacturers Association (NEMA) Technical Standard (TS) 8-2018 (NEMA TS 8-2018) (for TMC, ITSRE, RSE)*
- *Advanced Transportation Controller 5201 v06 (ATC 5201) (for ITSRE)*
- *National Transportation Communications for Intelligent Transportation System (ITS) Protocol (NTCIP) 9014, v01.20 (NTCIP 9104) (for TMC, ITSRE, RSE)*

- *Connected Transportation Interoperability (CTI) 4001 v01.00 (CTI 4001) (for RSE)*
- *Connected Transportation Interoperability (CTI) 4501 v01.00 (CTI 4501) (for TMC, ITSRE, RSE)*
- *Implementation Guide for Industrial Control Systems, version 7 (IG ICS) (for ITSRE, RSE)*
- *Institute of Electrical and Electronics Engineers (IEEE) 1609.2-2016 (IEEE 1609.2) (for RSE)*
- *Institute of Electrical and Electronics Engineers (IEEE) 1609.2.1-2020 (IEEE 1609.2.1) (for RSE)*
- *National Transportation Communications for ITS Protocol (NTCIP 1202) (for ITSRE)*
- *International Organization for Standards (ISO)/TS 21177:2019, Intelligent Transport Systems—ITS Station Security Services for Secure Session Establishment and Authentication Between Trusted Devices (ISO TS 2177) (for ITSRE)*

Note: standards relating to vehicles and vehicle communications are out of scope for the example physical objects presented in this template, but the communications between infrastructure and vehicles is in scope.

SC-8, Transmission Confidentiality and Integrity

Responsible Party (M/I): M

Justification to Select: Threat event, “Perform network sniffing of exposed networks” in **Table 2**, Section *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. S.

Guidance: The ATC transmits and receives information to/from TMC and RSU. The ATC should implement the control either in a typical manner if resources permit or in a customized manner to provide equivalent protections. Integrity protection is more important than confidentiality since the impact of information disclosure is low compared to the impact of data spoofing.

Parameter Value(s):

“confidentiality and integrity” (Note: using NIST-approved algorithms and protocols).

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

ARC-IT Mechanisms:

- Role-based access control as specified in the Access Control family with cryptographically enforced integrity checking:

- VPN using TLS 1.2 or 1.3 with a minimum of 128-bit (256 bit recommended) security symmetric cryptography for two-way information flows using strong password or preferably X.509 certificates for integrity protection.
- VPN using TLS 1.2 and 1.3 with a minimum of 128-bit (256 bit recommended) security symmetric cryptography for two-way information flows using strong password or preferably X.509 certificates for confidentiality protection.

Standards: RFC 8446[24], NTCIP 9014 v01.20, section B.2[25]

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 2**, Section *Perform reconnaissance and gather information,* and "Obtain sensitive information through network sniffing of external networks" in **Table 2**, Section Achieve results (i.e., cause adverse impacts, obtain information).

Guidance: Cryptographic protection is the only feasible means to protect the information in transit, as physical protection is not possible in most ITS environments. Ensure the strength of the confidentiality or the integrity mechanism is sufficient to protect the sensitivity of the information.

Parameter Value(s):

"prevent unauthorized disclosure of information and detect changes to information"

Risk References and Resources:

NIST SP 800-82: 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

SC-10, Network Disconnect

Responsible Party (M/I): M

Justification to Select: 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

[24] Internet Engineering Task Force (IETF) Request for Comment 8446, The Transport Layer Security (TLS) Protocol Version 1.3, August 2018.
[25] National Transportation Communications for ITS Protocol (NTCIP) 9014 v01.20, Infrastructure Standards Security Assessment (ISSA), Aug 2021.

the scope of this control set transmit or receive information; therefore, the control applies and is implemented on the physical object or possibly the distant end, either in a typical manner if resources permit or in an atypical manner to provide equivalent protections.

Guidance: Applicable for local connections by an operational user who accesses the signal program, or a User Developer who makes changes to the API. Not applicable for connections to the TMC, to allow for TLS, heartbeat, etc. Ensure the time period for disconnect is sufficiently short given the sensitivity of the information (e.g., shorter timeout periods for communications paths where information with higher sensitivity is exchanged).

Parameter Value(s):

"no more than 15 minutes"

Risk References and Resources:

NIST SP 800-82: NOTE: The intent of this control is effectively covered by AC-17 (9) for ITS systems.

ARC-IT Mechanisms:

- For Transmission Control Protocol/Internet Protocol (TCP/IP) ports in any state other than 'LISTENING,' the device shall de-allocate that TCP/IP port once 15 minutes have passed with no activity on that port.
- For UDP/IP ports in any state other than 'LISTENING,' the device shall de-allocate that User Datagram Protocol/Internet Protocol (UDP/IP) port once 15 minutes have passed with no activity on that port.

SC-13, Cryptographic Protection

Responsible Party (M/I): M

Justification to Select: Threat events, "Perform network sniffing of exposed networks" in **Table 2**, Section *Perform reconnaissance and gather information,* and "Obtain sensitive information through network sniffing of external networks" in **Table 2**, Section Achieve results (i.e., cause adverse impacts, obtain information).

Guidance: The ATC device should support the cryptographic algorithms necessary to set up TLS tunnels with device certificates. This includes a secure random number generator (see ARC-IT guidance below). This also includes securely procuring, storing, updating, and using its own certificate for TLS use, and being able to verify the TLS certificate of the communication endpoint (e.g., TMC).

Risk References and Resources:

ARC-IT Mechanisms:

- Devices may support additional cryptographic algorithms.

- Devices shall provide a FIPS 140-2[26] compliant random number generator, i.e., compliant to NIST SP 800-90A Revision 1[27].

Standards: FIPS 140-3[28], NIST SP 800-90A Rev. 1[29]

[26] Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 25, 2001.

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

[28] Federal Information Processing Standard (FIPS) 140-3, Security Requirements for Cryptographic Modules, March 22, 2019

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

Chapter 5. Implementation Considerations

*INSTRUCTIONS: This chapter provides considerations when selecting and implementing the controls specified in **Chapter 4, Detailed Control Specifications**.*

***Chapter 4** identifies a set of controls typically required to protect name of physical objects. There are controls that are usually not mandatory and do not warrant inclusion in the set of controls in **Chapter 4**. However, based on different technologies used, such controls may need to be selected. These controls require consideration to ensure that if selected and implemented, the controls will support achieving desired capabilities while adequately protecting ITS information. Situationally applicable additional controls for name of physical objects are included in this chapter, their justification for situational inclusion is documented, and any ITS-specific considerations for selection and implementation are documented. Examples are provided below.*

Organizations should consider the following control guidance when implementing specific system capabilities when a system is used to store, process, or transmit ITS information.

AC-18, Wireless Access

Guidance: This control discusses use of wireless access, but it is not typically mandatory for systems storing, processing, or transmitting ITS information, unless that information is transmitted wirelessly. If wireless technologies are used for systems that process ITS information, they may impact the risk posture; therefore, this control should be selected and implemented in a way that achieves desired capabilities but adequately protects ITS information. For the *name of physical objects* ensure *describe the implementation considerations for this control.*

AC-19, Access Control for Mobile Devices

Guidance: This control discusses access control for mobile devices, but is not typically mandatory for systems storing, processing, or transmitting ITS information, unless that information is processed on a mobile device. If mobile devices are used for systems that process ITS information, they may impact the risk posture; therefore, this control should be selected and implemented in a way that achieves desired capabilities but adequately protects ITS information. For the *name of physical objects* ensure *describe the implementation considerations for this control.*

CM-7(8), Least Functionality | Binary or Machine Executable Code

Guidance: This control enhancement discusses how binary or machine executable code applies to all sources of that code, including commercial software and firmware and open-source software. ITS physical objects may not require executable code, but if they do that code may impact the risk posture;

therefore, this control enhancement should be selected and implemented in a way that achieves desired capabilities but adequately protects ITS information. For the *name of physical objects* ensure *describe the implementation considerations for this enhancement.*

Chapter 6. References

INSTRUCTIONS: List all references cited in this document. If available, provide a link to the referenced publication.

The references are included in a word table so they can be sorted and formatted. After the references are complete, remove the borders[30] but keep the table (i.e., retain the table structure).

ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation https://www.arc-it.net/html/architecture/architecture.html
ATC 5201	Institute of Transportation Engineers (ITE) / American Association of State Highway and Transportation Officials (AASHTO) / National Electrical Manufactures Association (NEMA) *Advanced Transportation Controller (ATC) Standard* 5201 v06 https://www.ite.org/pub/?id=074A20C1-A415-533F-02B9-B0D185D40FA1
ATT&CK	MITRE ATT&CK® for Industrial Control Systems https://collaborate.mitre.org/attackics/index.php/Main_Page
CTI 4001	Institute of Transportation Engineers (ITE) / American Association of State Highway and Transportation Officials (AASHTO) / National Electrical Manufactures Association (NEMA) NEMA, Connected Transportation Interoperability (CTI) 4001 v01.00, *Roadside Unit (RSU) Standard,* September 2021 https://www.ite.org/pub/?id=764FB228-0F6C-BA02-6D7B-16A86B1F8108
CTI 4501	Institute of Transportation Engineers (ITE) / American Association of State Highway and Transportation Officials (AASHTO) / National Electrical Manufactures Association (NEMA) NEMA, Connected Transportation Interoperability (CTI) 4501, v01.00, *Connected Intersections Implementation Guide – Guidance to Setting Up and Operating a Connected Intersection (CI),* September 2021 https://www.ite.org/pub/?id=76270782-B7E4-7F75-BC72-D5E318B14C9A
Cybersecurity Framework	*Framework for Improving Critical Infrastructure Cybersecurity* (also known as the *Cybersecurity Framework*) https://www.nist.gov/cyberframework

[30] Right-click anywhere in the table; on the "Table" tab select "Table Properties"; select "Borders and Shading" near the bottom; deselect the internal and external borders in the diagram at the right; click "OK"; and click "OK" again.

FIPS 140-3	Federal Information Processing Standard (FIPS) 140-3, *Security Requirements for Cryptographic Modules*, March 22, 2019 https://csrc.nist.gov/publications/detail/fips/140/3/final
IEEE 1609.2	Institute of Electrical and Electronics Engineers (IEEE) 1609.2-2016, IEEE *Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages* https://standards.ieee.org/standard/1609_2-2016.html
IEEE 1609.2.1	Institute of Electrical and Electronics Engineers (IEEE) 1609.2.1-2020 - IEEE *Standard for Wireless Access in Vehicular Environments (WAVE)--Certificate Management Interfaces for End Entities*. https://standards.ieee.org/standard/1609_2_1-2020.html
IG ICS	Center for Internet Security (CIS) Controls™, *Implementation Guide for Industrial Control Systems*, version 7 https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/
ISA IEC 62443	International Society of Automation / International Electrotechnical Commission (ISA/IEC) 62443-4-2, *Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components* https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c
ISO TS 2177	*International Organization for Standards (ISO)/TS 21177:2019, Intelligent Transport Systems — ITS Station Security Services for Secure Session Establishment and Authentication Between Trusted Devices* https://www.iso.org/standard/70056.html
ITS Control Set Procedures	*Intelligent Transportation Systems (ITS) Operating Procedures for Developing Control Sets* https://placeholder
ITS Profile	*Intelligent Transportation Systems (ITS) Cybersecurity Framework Profile* https://placeholder
NEMA TS 8	National Electrical Manufacturers Association Technical Standard (NEMA TS) 8-2018, *Cyber and Physical Security for Intelligent Transportation Systems (ITS)* https://www.nema.org/standards/view/cyber-and-physical-security-for-intelligent-transportation-systems-its
NEMA TS 10	National Electrical Manufacturers Association Technical Standard (NEMA TS) 10-2019, *Connected Vehicle Infrastructure – Roadside Equipment* https://www.nema.org/standards/view/connected-vehicle-infrastructure-roadside-equipment
NIST Glossary	National Institute of Standards and Technology, Gaithersburg, MD, NIST Internal Report (NISTIR) 7298, Rev. 3, *Glossary of Key Information Security Terms* https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf https://csrc.nist.gov/glossary
NTCIP 1202	National Transportation Communications for ITS Protocol 1202, v03A, *Object Definitions for Actuated Signal Controllers (ASC) Interface,* May 2019

https://www.ntcip.org/file/2019/07/NTCIP-1202v0328A.pdf

NTCIP 1218 National Transportation Communications for ITS Protocol, *Object Definitions for Roadside Units (RSUs),* Sept 2020. https://www.ntcip.org/file/2021/01/NTCIP-1218v0138-RSU-toUSDOT-20200905.pdf

NTCIP 9014 National Transportation Communications for ITS Protocol, *Infrastructure Standards Security Assessment (ISSA)*, Aug 2021 https://www.ntcip.org/file/2021/08/NTCIP9014v0120.pdf

RFC 8446 Internet Engineering Task Force (IETF) Request for Comment 8446, *The Transport Layer Security (TLS) Protocol Version 1.3,* August 2018 https://datatracker.ietf.org/doc/html/rfc8446

NIST SP 800-30 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-30, *Joint Task Force (2012) Guide for Conducting Risk Assessments*. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

NIST SP 800-37 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-37, Rev. 2, *Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy*. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

NIST SP 800-39 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-39, *Joint Task Force (2011) Managing Information Security Risk - Organization, Mission, and Information System View*. https://csrc.nist.gov/publications/detail/sp/800-39/final

NIST SP 800-53 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-53, Rev. 5, *Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations*. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST SP 800-53B National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-53B, *Control Baselines for Information Systems and Organizations*, September 2020 (includes updates as of December 10, 2020) https://csrc.nist.gov/publications/detail/sp/800-53b/final

NIST SP 800-56A National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-56A, Rev 3, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*, April 16, 2018 https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final

NIST SP 800-56B National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-56B, Rev 2, *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography*, March 21, 2019 https://csrc.nist.gov/publications/detail/sp/800-56b/rev-2/final

NIST SP 800-56C	National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-56C, Rev 2, *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*, August 18, 2020 https://csrc.nist.gov/publications/detail/sp/800-56c/rev-2/final
NIST SP 800-57-1	National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-57 Part 1, Rev 5, *Recommendation for Key Management: Part 1 – General*, May 4, 2020 https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final
NIST SP 800-57-2	National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-57, Part 2, Rev 1, *Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations*, May 23, 2019 https://csrc.nist.gov/publications/detail/sp/800-57-part-2/rev-1/final
NIST SP 800-57-3	National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-57, Part 3, Rev 1, *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*, January 22, 2015 https://csrc.nist.gov/publications/detail/sp/800-57-part-3/rev-1/final
NIST SP 800-82	National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-82 Rev. 2, *Guide to Industrial Control Systems (ICS) Security*. https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
NIST SP 800-160 V1	National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-160 Volume 1, Rev. 1, *Engineering Trustworthy Secure Systems* https://csrc.nist.gov/publications/detail/sp/800-160/vol-1-rev-1/draft
NIST SP 800-160 V2	National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-160 Volume 2, Rev. 1, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final

INSTRUCTIONS: There are other resources that may help practitioners but cannot at this time be cited as a current reference above, because they are "works in progress" (WIP). Those resources are listed here for consideration along with the resource link wherever available:

IEEE 1609.2-20XX: Security Services. This is a new version of IEEE 1609.2 that includes the .2a and .2b amendments.

SAE J2945/4 (WIP), Road Safety Applications

SAE J2945/A (WIP), Standard for Lane-Level and Road Furniture Mapping for Infrastructure-based V2X Applications

SAE J2945/B (WIP), Recommended Practices for Signalized Intersection Applications

SAE J2945/C (WIP), Traffic Probe Use and Operation

Institute of Transportation Engineers (ITE) / American Association of State Highway and Transportation Officials (AASHTO) / National Electrical Manufactures Association (NEMA): Cybersecurity for the Advanced Transportation Controller (ATC) Standard (WIP).

SAE J3161/1 (WIP) On-Board System Requirements for LTE V2X V2V Safety Communications, https://www.sae.org/standards/content/j3161/1).

Appendix A. Acronyms and Abbreviations

INSTRUCTIONS: Include all acronyms and abbreviations used in this document. It is not necessary to create an acronym from a term that is used only once, unless that acronym is commonly used to identify a body, well-known concept, etc. Abbreviations for control families (e.g., AC, AT, AU) are included in Appendix B *to provide an easier reference to NIST SP 800-53 control families. The acronyms are included in a word table so they can be sorted and formatted.*

ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
AASHTO	American Association of State Highway and Transportation Officials
ASC	Actuated Signal Controller
ATC	Advanced Transportation Controller
CI	Connected Intersection
C-I-A	Confidentiality, Integrity, and Availability
CIS	Center for Internet Security
CTI	Connected Transportation Interoperability
CV	Connected Vehicle
CVO	Commercial Vehicle Operations
CVRSE	Connected Vehicle Roadside Equipment
DoS	Denial of Service
DDoS	Distributed Denial of Service
EMP	Electromagnetic Pulse
FIPS	Federal Information Processing Standard

FOIA	Freedom of Information Act
IBM	International Business Machines
ICS	Industrial Control Systems
ID	Identification
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IPS	Intrusion Protection System
IPSec	Internet Protocol Security
ISSA	Infrastructure Standards Security Assessment
IT	Information Technology
ITE	Institute of Transportation Engineers
ITSRE	Intelligent Transportation System Roadside Equipment
ITS	Intelligent Transportation Systems
L-M-H	Low, Moderate, and High
NEMA	National Electrical Manufacturers Association
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Internal Report
NTCIP	National Transportation Communications for Intelligent Transportation System (ITS) Protocol
OBE	On-board Equipment
OS	Operating System
OT	Operational Technology
RFC	Request for Comment
RSE	Roadside Equipment
RSU	Roadside Unit (see also Roadside Equipment)
SP	Special Publication

TMC	Traffic Management Center
TS	Technical Standard
TTPs	Tactics, Techniques, and Procedures
U.S.	United States
WIM	Weigh In Motion

Appendix B. Control Family Abbreviations

INSTRUCTIONS: List here only the NIST SP 800-53 control families that are included in the control specifications in Chapter 3, Summary of Control Specifications*, or in Chapter 5, Implementation Considerations.*

The abbreviations are included in a word table so they can be sorted and formatted. After the acronyms are complete, remove the borders[31] but keep the table (i.e., retain the table structure).

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

[31] Right-click anywhere in the table; on the “Table” tab select “Table Properties”; select “Borders and Shading” near the bottom; deselect the internal and external borders in the diagram at the right; click “OK”; and click “OK” again.

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 C. Glossary

INSTRUCTIONS: The physical objects that are the subject of control set documents may be unique and require the use of special terms. As such, it may be necessary to define those special terms in this document. More widely used terms may also be found in the NIST Glossary or other authoritative publications. In the table below, insert definitions in alphabetical order. Examples are provided in the table below; add or delete terms and definitions as needed. If a term and definition are being used from a different publication, include the reference tag (e.g., "(SP 800-37)") below the term. The definitions are included in a word table with borders so the terms and definitions can be sorted and formatted more easily. After the definitions are complete, remove the borders[1] but keep the table (i.e., retain the table structure).

Connected Vehicle (ARC-IT)	A vehicle connected device that is equipped with onboard equipment (OBE) that is active and operational and includes the means to send and receive data to and from other connected devices.
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 (ARC-IT)	A statement of the security requirements for a device in terms of its requirements for Confidentiality, Integrity, and Availability, expressed as Low, Moderate, or High ratings for each of the three
Enterprise Object	An organization or individual that interacts with other Enterprise Objects and/or Physical Objects. An Enterprise Object may be a component of another larger Enterprise Object, which may in turn be a component of a third, even larger, Enterprise Object (e.g., a Traffic Management Center Manager is a component of State Department of Transportation is a component of State Government). Enterprise Objects may participate wholly or in part in other Enterprise Objects (e.g., a Device Developer is a component of Auto Manufacturer but also participates in Standards Body).
Information Flow (ARC-IT)	Information that is exchanged between Physical Objects (subsystems and terminators) in the Physical View of ARC-IT. The terms "information flow" and

	"architecture flow" are used interchangeably. Information flows are the primary tool that is used to define the ITS architecture interfaces. These information flows and their communication requirements define the interfaces which form the basis for much of the ongoing standards work in the national ITS program.
Intelligent Transportation System (ARC-IT)	The system defined as the electronics, communications, or information processing in transportation infrastructure and in vehicles used singly or integrated to improve transportation safety and mobility and enhance productivity. Intelligent transportation systems (ITS) encompass a broad range of wireless and wire line communications-based information and electronics technologies.
On-board Equipment (ARC-IT)	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 (ARC-IT)	Systems or devices that provide ITS functionality that makes up the ITS and the surrounding environment. They are defined in terms of the services they support, the processing they include, and their interfaces with other Physical Objects. They are grouped into six classes: Centers, Field, ITS, Support, Travelers, and Vehicles. Example Physical Objects are the Traffic Management Center, 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 (NIST Glossary)	The organization’s or stakeholder’s readiness to bear the risk after risk treatment in order to achieve its objectives. Note: Risk tolerance can be influenced by legal or regulatory requirements.
Roadside Unit (ARC-IT)	A fixed-position cooperative device. This may be a permanent installation or temporary equipment brought on-site for a period of time associated with an incident, road construction, or other event.
Service Package (ARC-IT)	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 directly related to ITS strategies used to meet regional goals and objectives.

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 Document Number]

U.S. Department of Transportation