Operating Procedures for Developing Security Control Sets for Intelligent Transportation Systems (ITS)

www.its.dot.gov/index.htm

Final Report – July 31, 2023
Publication Number FHWA-JPO-23-123

U.S. Department of Transportation

Produced by U.S. DOT Volpe National Transportation Systems Center
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
ITS Joint Program Office

Notice

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

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

Technical Report Documentation Page

1. Report No. **FHWA-JPO-23-123**	**2. Government Accession No.**	**3. Recipient's Catalog No.**

4. Title and Subtitle Operating Procedures for Developing Security Control Sets for Intelligent Transportation Systems (ITS)	**5. Report Date** July 31, 2023
	6. Performing Organization Code V-337
7. Author(s) Randy Gabel, Christina Sames, Hector Martinez, Pam Miller, Julie Nethery Snyder, Hillary Tran, Dr. Michaela Vanderveen	**8. Performing Organization Report No.**
9. Performing Organization Name and Address U.S. DOT Volpe National Transportation Systems Center 220 Binney Street Cambridge MA 02142	**10. Work Unit No. (TRAIS)**
	11. Contract or Grant No. IAA 693JJ320N300058
12. Sponsoring Agency Name and Address ITS-Joint Program Office 1200 New Jersey Avenue, S.E. Washington, DC 20590	**13. Type of Report and Period Covered** 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 provides guidance to community organizations that propose to create, develop, approve, and maintain control sets for various physical objects, such as Connected Vehicle Roadside Equipment (CVRSE), ITS Roadway Equipment (ITSRE), and Vehicle Onboard Equipment (OBE) used within the Intelligent Transportation System (ITS) community. These operating procedures provide a detailed description of the process, roles and responsibilities, definitions related to control sets, and references to additional information and material available to support the control set development process.

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

19. Security Classif. (of this report) unclassified	**20. Security Classif. (of this page)** unclassified	**21. No. of Pages** 39	**22. Price**

Table of Contents

List of Tables

List of Figures

Chapter 1. Purpose

This document provides guidance to community organizations that propose to create, develop, approve, and maintain control sets for various physical objects, such as Connected Vehicle Roadside Equipment (CVRSE), ITS Roadway Equipment (ITSRE), and Vehicle Onboard Equipment (OBE) used within the Intelligent Transportation System (ITS) community. These operating procedures provide a detailed description of the process, roles and responsibilities, definitions related to control sets, and references to additional information and material available to support the control set development process.

The information provided within is current as of July 31, 2023, and is subject to change as work continues to develop ITS control sets.

ITS control sets are specifications of controls needed to mitigate the risk of operating ITS physical objects. ITS control sets are developed by selecting the controls from the NIST SP 800-53 controls catalog and providing other specifications based on the risk (i.e., combination of threats, vulnerabilities, and impact) associated with the physical objects. A companion document to this set of operating procedures is the *Intelligent Transportation Systems (ITS) Control Set Template and Instructions* (hereafter referred to as the ITS Control Set Template) that fully explains how to develop the control sets. The ITS control sets are intended to be provided to system and device developers or manufactures, ITS project managers and engineers, and ITS system integrators to help identify security requirements when acquiring or developing physical objects. ITS control sets can also be used by standards bodies to to create, update, or improve security requirements in ITS standards.

ITS 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 control baseline to which an overlay is applied. ITS control sets are complete on their own, whereas an overlay is a means to modify a selected control baseline. The NIST control baseline approach is not used in this document.

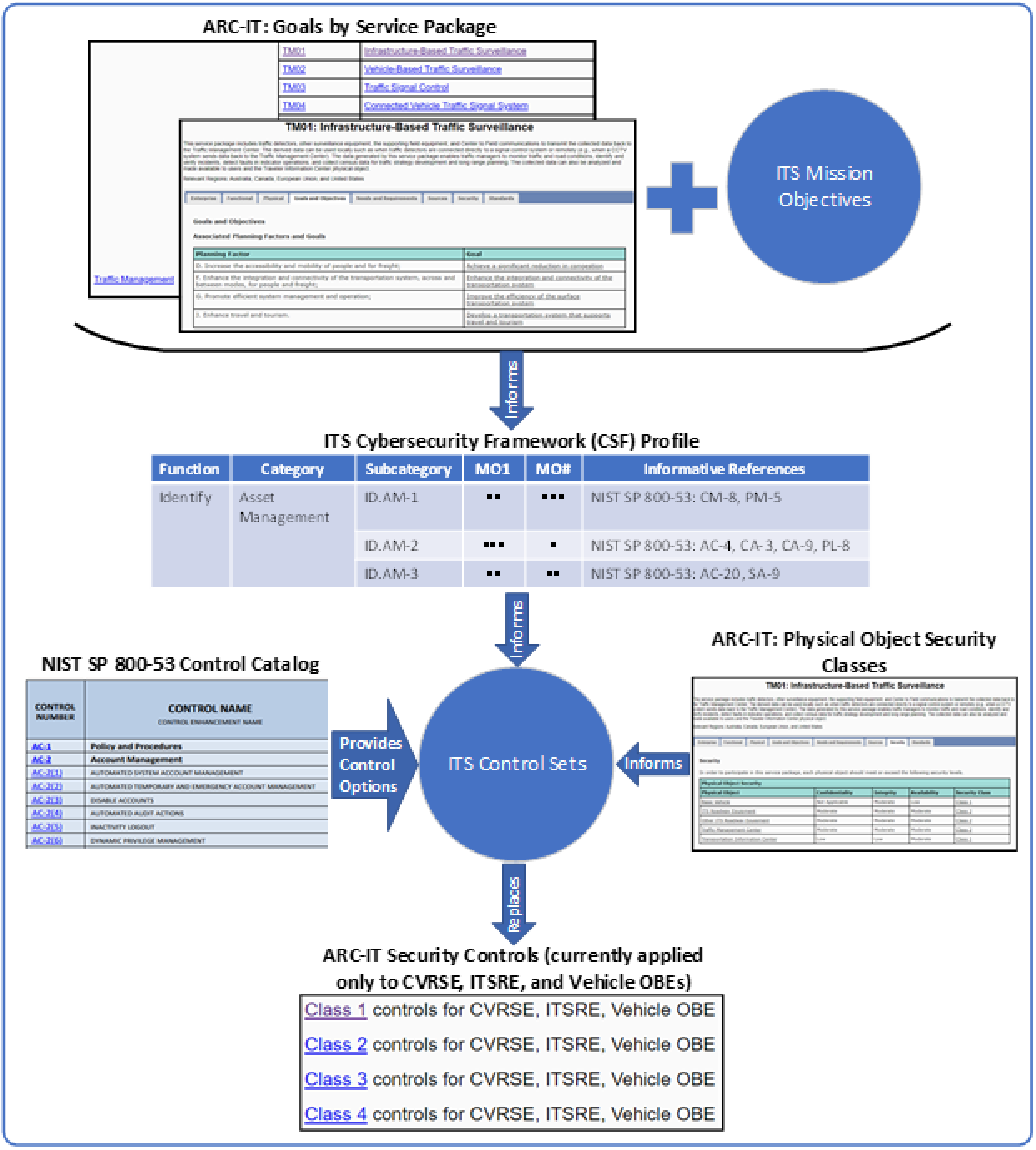
NIST integrated the discussion of privacy and security where there are overlaps between the two areas in many of the controls in NIST SP 800-53. These ITS control sets contemplate only the security aspects of the controls. Practitioners should evaluate whether and how the privacy aspects may apply in their environment.

Chapter 2. Introduction: ARC-IT Cybersecurity Framework Profiles, and Control Sets

Figure 1 was designed to help users of the ITS controls sets understand the relationship between ARC-IT, the ITS Profile, and ITS controls sets.

ARC-IT includes service packages that represent slices of the physical view that address specific services like traffic signal control. A service package collects several different physical objects (systems and devices), their functional objects, and information flows that provide the desired service. In **Figure 1**, the table in the upper left titled “ARC-IT Goals by Service Package” starts with a sample of a menu of 150 service packages, focusing in on the Traffic Management area. Hovering over that table is the table titled “Infrastructure-Based Traffic Surveillance” service package (short name TM01) within the Traffic Management area. Each service package includes relevant goals and objectives (from the overall list of ARC-IT Goals) that are very detailed in comparison to, but can inform or support, the Mission Objectives identified in the ITS Profile (blue circle in the upper right of **Figure 1**).

The combination of the ARC-IT Goals and Mission Objectives identified in the ITS Profile can help inform identification of priority Cybersecurity Framework Categories and subsequently priority Subcategories that are most supportive of a given Mission Objective’s success. The table in the middle of **Figure 1** titled, “ITS Cybersecurity Framework Profile,” is a notional sample of prioritized Subcategories (represented by the dots) informed by stakeholder workshops. The table also includes Informative References (e.g., the controls) from the Cybersecurity Framework that support the Subcategories. Subcategory priorities associated with each Mission Objective inform control selections in the ITS control set for a physical object that supports the Mission Objective.


ARC-IT: Goals by Service Package
Traffic Management
TM01: Infrastructure-Based Traffic Surveillance
Goals and Objectives
Associated Planning Factors and Goals
ITS Mission Objectives
Informs
ITS Cybersecurity Framework (CSF) Profile
Informs
NIST SP 800-53 Control Catalog
Provides Control Options
ITS Control Sets
Informs
ARC-IT: Physical Object Security Classes
TM01: Infrastructure-Based Traffic Surveillance
Security
Physical Object Security
Replaces
ARC-IT Security Controls (currently applied only to CVRSE, ITSRE, and Vehicle OBEs)

TM01	Infrastructure-Based Traffic Surveillance
TM02	Vehicle-Based Traffic Surveillance
TM03	Traffic Signal Control
TM04	Connected Vehicle Traffic Signal System

Planning Factor	Goal
D. Increase the accessibility and mobility of people and for freight;	Achieve a significant reduction in congestion
F. Enhance the integration and connectivity of the transportation system, across and between modes, for people and freight;	Enhance the integration and connectivity of the transportation system
G. Promote efficient system management and operation;	Improve the efficiency of the surface transportation system
J. Enhance travel and tourism.	Develop a transportation system that supports travel and tourism

Function	Category	Subcategory	MO1	MO#	Informative References
Identify	Asset Management	ID.AM-1	■■	■■■	NIST SP 800-53: CM-8, PM-5
		ID.AM-2	■■■	■	NIST SP 800-53: AC-4, CA-3, CA-9, PL-8
		ID.AM-3	■■	■■	NIST SP 800-53: AC-20, SA-9

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME
AC-1	Policy and Procedures
AC-2	Account Management
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT
AC-2(2)	AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT
AC-2(3)	DISABLE ACCOUNTS
AC-2(4)	AUTOMATED AUDIT ACTIONS
AC-2(5)	INACTIVITY LOGOUT
AC-2(6)	DYNAMIC PRIVILEGE MANAGEMENT

Physical Object	Confidentiality	Integrity	Availability	Security Class
Basic Vehicle	Not Applicable	Moderate	Low	[illegible]
ITS Roadway Equipment	Moderate	Moderate	Moderate	[illegible]
Other ITS Roadway Equipment	Moderate	Moderate	Moderate	[illegible]
Traffic Management Center	Moderate	Moderate	Moderate	[illegible]
Transportation Information Center	Low	Low	Moderate	[illegible]

Class 1 controls for CVRSE, ITSRE, Vehicle OBE
Class 2 controls for CVRSE, ITSRE, Vehicle OBE
Class 3 controls for CVRSE, ITSRE, Vehicle OBE
Class 4 controls for CVRSE, ITSRE, Vehicle OBE

Figure 1: Relationship Between the Cybersecurity Framework, ARC-IT, and ITS Control Sets

The NIST CSF[1] is comprised of cybersecurity outcomes and activities and mappings of those cybersecurity best practices. The NIST CSF provides a means to align organizational goals, called Mission Objectives in a Profile, to priority NIST CSF cybersecurity outcomes, activities, and groups of cybersecurity best practices. These cybersecurity best practices, called Informative References, are a mapping of existing standards, guidelines, and practices (e.g., security controls) to cybersecurity activities or Subcategories.[2] Prioritized Subcategories communicate which cybersecurity activities and outcomes are most important to leadership and reflect an organization's business/mission requirements, risk tolerance, and resources. Those priorities can be used to inform updates to the risk management strategy[3] and guide efforts to select, tailor, implement, and manage controls over time at the system/program level, especially given limited resources.

The ITS Cybersecurity Framework Profile (ITS Profile) provides a risk-based approach for managing cybersecurity activities, reducing cyber risk, and protecting the ITS ecosystem. The ITS Profile uses the NIST CSF to align ITS goals (i.e., Mission Objectives) to NIST CSF cybersecurity outcomes and activities. The ITS Profile contains 14 ITS-specific Mission Objectives. For each Mission Objective, the ITS Profile includes the prioritized CSF Subcategories (i.e., cybersecurity activities) most supportive of that Mission Objective. These Mission Objectives and the prioritized Subcategories reflect input from the ITS community. State and local transportation organizations can use the ITS Profile as a strategic planning tool to communicate priority cybersecurity outcomes within their organization and to other organizations within the ITS community. The ITS Profile's overall purpose is focused on high-level strategic and broad actions versus specific requirements implementations and precise actions typically conducted at the system level.

In comparison to the ITS Profile's applicability, ITS control sets are applied at the system/physical object level to provide detailed controls and implementation specifics. ITS control sets are specifications of controls needed to mitigate the risk of operating ITS physical objects. ITS control sets are comprised of selected controls from the NIST Special Publication (SP) 800-53 controls catalog and include specifications based on the risk (i.e., a combination of threats, vulnerabilities, likelihood, and impact) associated with the physical objects. Developers of ITS control sets can examine the ITS Profile to understand which Mission Objectives are supported by the physical object which is the topic of the control set. Once that is understood, the developers of control sets can examine a Subcategory's priority and review the controls mapped to the Subcategory in the Informative References. Implementers of the ITS control set can then determine which mapped controls are a priority for a physical device based on

[1] https://www.nist.gov/cyberframework/framework

[2] While CSF v1.1 Informative References are mapped to NIST SP 800-53 Revision 4 controls, NIST provides a mapping of Subcategories to NIST SP 800-53 Revision 4 and Revision 5 controls in its Cybersecurity and Privacy Reference Tool available at: https://csrc.nist.gov/projects/cprt/catalog#/cprt/home.

[3] NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*

priority Subcategories within the ITS Profile compared to the selected controls within an ITS control set for that physical device.

Although ITS control sets can be developed for internal use, they are typically developed by a community that spans organizations and include individuals with expertise specific to a given control set topic. ITS control sets are best when developed and used in the context of the ITS Profile. Doing so contributes to overall enterprise risk management and informed risk management decisions throughout an organization. ITS control sets address more specific circumstances beyond those that are reflected in the ITS Profile—for this reason, ITS control sets typically do not influence the ITS Profile, but the two work as complementary cybersecurity risk management tools within the community.

The table titled “ARC-IT: Physical Object Security Classes” in **Figure 1** provides device security classes for the physical objects that comprise that same service package, “Infrastructure-Based Traffic Surveillance.” A device security class is a statement of the security requirements for a device in terms of its requirements for confidentiality, integrity, and availability (i.e., security objectives). Each security objective has an associated impact level expressed as low, moderate, or high. Within the ITS Architecture, devices are the building blocks for physical objects. These device security classes were derived by analyzing the requirements associated with application-constrained information flows, and then combining those flows at physical object boundaries to determine device requirements. Each physical object may require different levels of protection for confidentiality, integrity, and availability based on their information flows. This results in a security class of 1 through 5, 5 being the highest level of protection required.[4]

The device security class for each physical object informs the control specifications in the ITS control set. The ITS Control Set Template indicates how the device security class is used when selecting controls. Developers of a control set complete **Table 1, *Physical Object Device Security Class by Service Package***, in the ITS Control Set Template to indicate which service packages are supported by the physical object and which device security class (1-5) is assigned for that physical object in each 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 the control set, Table 6, *Control Specifications by Device Security Class*. Note that a control might not be specified at lower device security classes, as that protection may not be required at lower impact levels for confidentiality, integrity, and availability.

The ITS Control Set Template provides instructions on how to identify vulnerabilities and threats specific to ITS physical objects. Developers of ITS control sets must assess the risk to the physical object by

[4] In the example in Figure 1 for CVRSE, ITRSE, and Vehicle OBE, Class 5 is not indicated as there were no requirements identified for High confidentiality, integrity, and availability at the time the ARC-IT page was published. Later when the methodology was applied to the entire ITS architecture, analysis revealed high availability was required in some instances, so Class 5 was required.

considering the potential impact caused by a relevant threat source exploiting a vulnerability. There may be degrees of rigor in the approaches used to assess that risk. For example, MITRE ATT&CK® for Industrial Control Systems (ICS)[5] uses a rigorous approach to identifying threat sources' techniques but does not provide full coverage of all controls. NIST SP 800-82[6] provides more coverage of controls but possibly not as much rigor as ATT&CK. ARC-IT provides rigor (e.g., translates control text to requirements-like statements) across all relevant controls, but it provides coverage for only three physical objects (ITSRE, CVRSE, and OBE). Where there may be gaps in rigor or coverage, subject matter expertise based on years of experience with ITS and/or controls is needed to identify controls to mitigate risk. ARC-IT is discussed in detail above, and the other approaches are discussed more fully below.

ITS are similar to ICS; therefore, ATT&CK for ICS is one fairly rigorous risk-based resource that may be used to gain insight into the adversary's behavior (tactics and techniques) and identify controls necessary to mitigate some but not all ITS risks. ATT&CK for ICS identifies 51 mitigations developed to lessen or eliminate the impact of attackers' techniques. There can be a man-to-many relationships between mitigations and techniques. Those mitigations are mapped to security controls, some having a many-to-many relationship. But the controls identified in ATT&CK for ICS are 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 or all the controls within a family. The focus is on the more technical controls, as opposed to management or operational controls.

ATT&CK is organized into three matrices. In addition to the ATT&CK for ICS matrix, there is the ATT&CK Enterprise matrix and ATT&CK Mobile matrix. And within the ATT&CK Enterprise matrix, there are sub-matrices for PRE (Preparatory), Windows, macOS, Linux, Cloud (with sub-sub-matrices), Network, and Containers. If the ITS system or component of concern uses typical IT, mobile technologies, Linux, or traditional technologies, it would be prudent to examine each of the ATT&CK matrices to identify relevant techniques and mitigations and the controls mapped to those mitigations.

NIST SP 800-82 may also be used as another risk-based resource for identifying controls to mitigate risk to ICS. NIST SP 800-82 contains a control overlay that lists controls typically needed to mitigate cybersecurity risks to ICS. ICS are similar to ITS, so those controls can be examined to determine which of those controls are also relevant to ITS and may be selected for the ITS control set.

In addition to the above resources, it is usually necessary for developers of control sets to consult subject matter experts in both the ITS community and in the controls from NIST SP 800-53. Together, the experts reference as many resources as appropriate to assess all the risk factors (*threats*, *vulnerabilities*, *likelihood*, and *impact*) before selecting controls. Experts must identify the *threats* and *vulnerabilities* relevant to ITS, determine the *likelihood* that a threat source could initiate an attack and be successful in exploiting a *vulnerability*, determine the *impact* to the system and to operations if that exploit is successful, identify the risk level based on all these risk factors, and ultimately select the controls

[5] https://attack.mitre.org/matrices/ics/

[6] Revision 3 of NIST SP 800-82 is in draft and the scope is increasing from ICS to the more inclusive operational technology (OT).

necessary to mitigate that risk. The degree of rigor used by the experts is dependent on available resources, which typically drives anywhere from a rigorous quantitative approach to a somewhat less rigorous qualitative approach. Reference SP 800-30 for details on the risk factors and the risk assessment process. If resources are limited, the input from subject matter experts becomes increasingly important and significant to the development of a control set.

Developers of control sets should 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. The *Detailed Control Specifications* should reference in the Justification the risk that is to be mitigated.

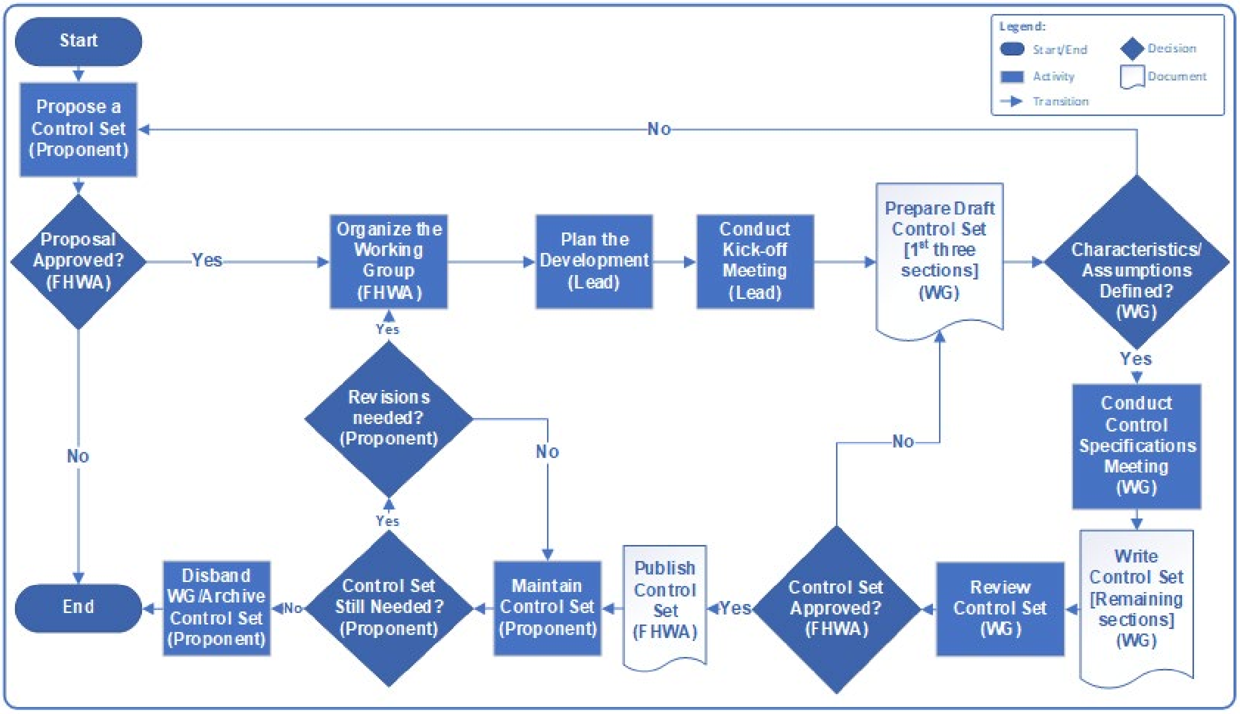
Chapter 3. Control Set Oversight

USDOT oversees and manages the process to publish all control sets that will be used across the ITS community. USDOT uses control sets to build consensus across the ITS community of interest and identify relevant control specifications that have broad-based support for specific security circumstances, situations, or conditions relevant to ITS physical objects. USDOT develops and maintains the processes and tools (e.g., USDOT collaboration site) necessary to create and publish (e.g., to a USDOT website) control sets in development for review/comment or final control sets.

Chapter 4. Process

The process for developing ITS control sets consists of the following activities, which are depicted in the process flow diagram in **Figure 2** and described in detail in this document:

- Propose/Approve Control Set Development
- Organize a Control Set Working Group
- Plan Control Set Development
- Conduct Kickoff Meeting
- Prepare Draft Control Set
- Conduct Control Specification Meetings
- Write the Control Set
- Review/Approve the Control Set
- Publish the Control Set
- Maintain the Control Set



Legend:
Start/End
Decision
Activity
Document
Transition
Start
Propose a Control Set (Proponent)
No
Proposal Approved? (FHWA)
Yes
Organize the Working Group (FHWA)
Plan the Development (Lead)
Conduct Kick-off Meeting (Lead)
Prepare Draft Control Set [1st three sections] (WG)
Characteristics/ Assumptions Defined? (WG)
Yes
Conduct Control Specifications Meeting (WG)
Yes
Revisions needed? (Proponent)
No
No
Yes
No
Write Control Set [Remaining sections] (WG)
Review Control Set (WG)
Control Set Approved? (FHWA)
Yes
Publish Control Set (FHWA)
Maintain Control Set (Proponent)
Control Set Still Needed? (Proponent)
No
Disband WG/Archive Control Set (Proponent)
End

Figure 2: Control Set Development Process

The parentheses in each activity box, decision diamond, or document icon in **Figure 2** indicate who is responsible for that activity, decision, or document. A summary of the tasks and recommended responsible parties is provided in **Table 2, Control Set Development Tasks**.

4.1 Propose a Control Set

4.1.1 Proposal Submission

A control set proponent identifies the potential need for a control set and contacts USDOT to submit a proposal. The proponent can be, for example, a State, County, or City Department of Transportation, Toll Authority, Transit Authority, Compliance or Certification Authority, ITS device manufacturer, ITS integrator, or community recognized technical body. USDOT can also serve as a proponent based on its broad understanding of controls, completed control sets, control sets in progress, and the need for additional control sets.

The proponent proposes the control set topic[7] to USDOT. USDOT discusses the proposed topic with the proponent, provides guidance on the proposal process, and schedules the proposal for discussion at an upcoming USDOT meeting with the ITS community. The proponent, along with any supporting team members, prepares answers to the questions below, which will be used to evaluate the need for a control set.

The proponent provides answers to the following questions:

1. **Can a set of assumptions or characteristics be clearly and distinctly defined to characterize the risk of operating the physical objects, which the control set will address?**

   What is unique about the topic of the proposed control set (i.e., the physical object) that would influence a selection of controls?

   Provide sufficient detail on the assumptions and characteristics related to the planned control set so USDOT can determine how the assumptions and characteristics will influence selection of controls and enhancements and how they differ from other proposed, planned, or published control sets.

   For example, one NIST assumption is that information in systems is relatively persistent. However, a control set for ITS physical objects may assume instead that the information is not persistent. The control set discussion of assumptions and characteristics should then indicate that ITS physical object information is typically more perishable than persistent in nature and, therefore, may not require the same protections as persistent data.

[7] The topic is the physical object or objects for which controls must be selected in the control set.

2. **How does the proposed control set topic apply to types of physical objects across the ITS community?**

   Does the control set topic apply equally to all those physical objects? If not, what portion of ITS physical objects is related to the control set topic?

3. **Which ITS community organizations are likely to be proponents?**

   What resources (i.e., participants with the required expertise in the topic as well as participants with control expertise) are available from the proponent or other community organization(s) to develop the control set?

   Identify, by name, the community organizations that are collaborating on the control set, how many people they can provide, and the skills of those people (e.g., subject matter experts [SME] with knowledge of the control set topic and control knowledge).

4. **Which ITS community organization offers to maintain the control set over its lifecycle?**

   If the proposing community organization that develops the control set does not also maintain the control set, another organization must be willing and able to do so.

5. **Which ITS community organizations may use and benefit from the control set? What proportion (e.g., one, seven, a third, half, most, all) of the systems within those organizations could use and benefit from the control set?**

   The intent is to determine if it is worthwhile to develop the control set.

6. **How is the control set topic similar to or different from other existing control sets or planned / in-development control sets?**

   For example, surveillance cameras and dynamic message signs operate in the same environment as ATCs, connect to ATCs, and share similar risks, which means a single control set could be used to address all three rather than creating separate control sets.

7. **Are there existing statutes, regulations, or policies that direct or recommend implementation of capabilities related to controls that should be selected in a control set?**

   Identifying if any applicable existing statutes, regulations, or policies can consistently guide implementation of capabilities related to selected controls for an ITS control set.

8. **Are there any pending statutory, regulatory, or policy decisions that could have a critical bearing on the control selections in the control set?**

   If so, defer development until those policy decisions have been made.

4.1.2 Proposal Review and Approval

The control set proponent provides the answers to the questions at least 2 weeks prior to a USDOT meeting for distribution to members of the ITS community. The members of the ITS community review the proposal, evaluate the impact/value of the proposed control set, and determine any intersections it may have with other published or in-development control sets. The control set proponent attends the USDOT meeting to answer any questions from the ITS community members and discuss the merits of the proposed control set.

USDOT asks the members to reach back into their respective organizations on the proposed control set to determine the need for a control set and return to the next USDOT meeting with their organization's response. At the subsequent USDOT meeting, the members validate the merit of the control set and discuss whether to recommend development of the proposed control set.

If the USDOT recommends that the control set be developed, the USDOT will provide an official response (via email) to the proponent. If the USDOT does not recommend that the control set be developed, the USDOT will provide an official response (via email) to the proponent, including the rationale behind the non-recommendation.

4.2 Organize a Control Set Working Group

For proposed control sets approved for development, the USDOT, together with the control set proponent, identifies a working group (WG) Lead or co-leads who performs the control set development. The USDOT assigns a WG Advisor to the WG. The WG Lead should be an expert in the control set topic, but they also perform the administrative tasks to establish, manage, and guide the WG. The WG Advisor provides guidance on the control set development process and the review and approval process. Detailed recommended roles and responsibilities are provided in **Table 1**.

The WG needs a balance of SMEs on the control set topic and SMEs knowledgeable on the controls. The WG Lead(s) and WG Advisor identify the types of skills and resources needed to develop the control set. The WG Lead(s) may invite ITS project engineers or system integrators from across the ITS community who have experience in identifying security requirements and designing or building ITS. SMEs may be invited from design/developer companies or original equipment manufacturers, at the discretion of the WG Lead. SMEs who manage or support standards bodies may also be invited.

The USDOT sends out a call for participants to the ITS community to establish a control set WG, requesting individuals with defined SME knowledge, and identifying the control set topic, planned kickoff date, expected level of effort (e.g., timeline and the frequency, duration, and location of meetings), and anticipated duration to develop the control set.

The participants should be sought from the ITS community organizations and be official representatives for their organizations. The WG membership will be decided by the WG Lead, who will notify all

Experience in group dynamics and activities similar to developing control sets indicates the ideal number for a WG is 6-10 active participants, with at least two of those participants being control SMEs and other SMEs providing expertise in ITS physical objects, communications, and networking. Too small of a group may risk not having the appropriate expertise, and too large of a group may risk distractions and confusion. Both could impact a WG's progress. However, there is no required WG size; the specific number of participants is at the discretion of the WG Lead/s.

The initial controls selection for the draft ITS control set may require anywhere from 6-9 months of WG meetings involving SMEs familiar with NIST SP 800-53 controls and the topic of the control set The duration depends on the complexity of the control set topic, the team's familiarity with controls and ITS, the level of commitment and availability of the team members, and the frequency and length of meetings (e.g., 2 hour meetings three times a week).

volunteers of their inclusion or exclusion. Any objections to the WG Lead's decisions to include or exclude members can be elevated to the USDOT to reconcile.

A control set development WG consists of the following member roles. One person may be able to perform multiple roles if necessary.

Table 1: Control Set Working Group Roles and Responsibilities

Role	Responsibility
Control Set Proponent	• Recognizes the need for a control set. • Champions the control set to the USDOT. • Willing to support the development, approval, and ongoing maintenance of the control set. • Provides individuals with the relevant skills and experience on the control set topic. • Typically provides or may serve as the WG Lead for the control set WG. • Can be a USDOT member. • If the proponent is a technical body led by a contractor or an employee of a company that develops physical objects, there must be a government sponsor identified and included on all correspondence.
WG Lead	• An expert in the control set topic. • Manages the development of the control set. • Plans development meetings, gathers initial documentation, identifies members, and manages WG membership over time, and guides the WG discussions. • With assistance from the WG Advisor, prepares for and facilitates the kickoff meeting with the control set WG. • Guides the WG in developing the control set and assigning responsibilities to the WG members for specific tasks. • Negotiates with critical commenters to resolve identified issues. • Arranges the administrative requirements for the development meetings. • Liaison with the USDOT.
WG Advisor	• Expert on the control set development process and controls. • Provides guidance to the WG on how to develop control sets and explains the intent of controls and enhancements. • Engaged more in the early stages of a specific control set development. • Not involved in the day-to-day development of the control set after the initial stages but serve as advisors throughout the development and approval processes and being available for periodic reviews, questions, etc. • Liaison to the USDOT to raise and address any controversial and technical issues identified by the WG that cannot be resolved by the WG Lead, and to provide status updates during USDOT meetings on the control set's development.
Subject Matter Expert (SME)	• Experts in the control set's topic and controls are the core participants of the control set WG. • Determine applicable controls and their specifications and help write the control set document, when assigned this responsibility by the WG Lead. • Includes people from different community organizations, representing the full range of the impacted ITS community, including contractors, consultants,

	academics, representatives of design/development/manufacturing companies, or standards bodies, at the discretion of the WG Lead. • There should be at least two SMEs on controls to provide a balanced understanding of the controls.

4.3 Plan Control Set Development

The WG Lead and WG Advisor meet to document the purpose and intent of the control set, building on the materials prepared during the control set initiation and any feedback received during presentation to the USDOT at the initial and follow-up meetings (see **Chapter 4.1, Propose a Control Set**). The WG Lead may ask the WG Advisor questions on the ITS Control Set Template or development process. The WG Lead determines the meeting format and logistics for the WG, invites WG members to the kick-off meeting, and runs the kick-off meeting.

The WG Lead, with support from the WG Advisor, establishes an agenda for the initial or kick-off meeting. Typically, the initial meeting agenda includes the following information:

- Opening (e.g., welcome, introduction of members, purpose of the group).
- Control set topic.
- Administrative information, including the anticipated timeline/schedule and requested level of commitment.
- Introduction to NIST SP 800-53, ARC-IT, the NIST Cybersecurity Framework, and the ITS Profile.
- ITS Control Sets Template and development process.
- Business rules, such as which controls to consider, how to consistently interpret controls, or how to justify the control selections.
- Documentation needed to support control set development (e.g., policies, standards, guidance, standard operating procedures, threats, vulnerabilities, MITRE ATT&CK for ICS mitigations).
- Documentation (e.g., spreadsheet) to consolidate information from various resources (e.g., ARC-IT, NIST SP 800-82, MITRE ATT&CK for ICS) used to inform control selection decisions, to capture those decisions of the WG, and to provide a historical log.

4.4 Conduct Kickoff Meeting

At the initial meeting, the WG Lead reviews the ITS control set topic with the WG members. The WG Lead provides the administrative details on how the WG will operate (e.g., expected SME knowledge; meeting logistics such as frequency and duration of meeting, location of the meetings or the need for virtual meetings; anticipated deliverables; planned timeline). The WG Advisor conveys the background information needed to produce the control set, explaining the control selection processes from NIST SP 800-53 control catalog, the control set template, and the control set development process.

The WG Lead advocates for and documents the business rules for developing the control sets, to include as a minimum:

- Develop the control sets for the “majority of systems” (i.e., the 80% approach) across the ITS community. Exceptions (i.e., the 20%) can be addressed by system-specific tailoring.
- Identify and document the assumption that each selected control meets to provide traceability.

The WG Lead assigns to an individual or a subset of the WG the responsibility for writing the control set and maintaining supplemental materials used to develop the control set. Individuals are identified for this smaller group based on their specific knowledge, commitment to completing the control set, and availability over the expected control set duration. The WG members identify any documentation needed to develop the control set (e.g., regulations, related policies or legislation, standards, common definitions) and prepare for the upcoming control set development meetings.

4.5 Prepare Draft Control Set

The WG (or a subset of the WG[8]) develops a draft of the front matter of the control set to include *Identification* (*Purpose, Scope, and Applicability*) and *Physical Object Characteristics* sections using the ITS Control Set Template. The front matter needs to be drafted before working on control selections and other control set guidance. These front matter sections focus on describing the environment, information, or functions associated with the physical object that is the topic of the control set; the characteristics of the physical object; any assumptions related to the physical object; and the specific questions to determine applicability of the control set.

If the control set WG cannot agree on aspects of the control set (e.g., purpose, scope, applicability, assumptions, characteristics), it may mean the group is too divergent in their understanding of the control set topic to come to agreement or it may mean the topic is not appropriate for a control set as no basis for the control selections can be defined. If this is the case, the WG Lead should seek guidance from the USDOT.

These initial meetings are critical to developing and providing a common understanding and documented agreement on the control set. When developing an ITS control set, it takes time for the SMEs to understand controls and those knowledgeable on controls to understand the physical object and which are the appropriate control specifications. After the foundational purpose, scope, applicability, assumptions, and characteristics are agreed upon, the control selection process begins.

4.6 Conduct Control Specification Meetings

The WG convenes to identify the control specifications (e.g., control selections, justifications,

[8] The WG Lead may assign subsets of the working group to write certain sections of the control set document; for example, when specific expertise is needed or when sections need to be developed simultaneously.

implementation or tailoring guidance, parameter values, references) for the control set. The WG Advisor should be at the initial control specification meeting to help guide the WG. The WG Advisor provides the WG with a spreadsheet that includes the NIST SP 800-53 controls and enhancements and areas to record the control set's specifications. After the initial control specification meeting, the WG Advisor takes the role of a reviewer to address control and control set related questions, as needed.

The WG's decisions can be captured in the control specification spreadsheet or written directly into the control set document. The spreadsheet may be useful for groups without experience with control sets or who are creating a control set on a newly defined topic. Information documented during the control set specification discussions is used to write the *Detailed Control Specifications* section. The WG must capture discussions on potential justifications, guidance, parameter values, and references. Examples of each of these items are provided in the box below.

Example of NIST SP 800-53 Control Enhancement

This is an example of a control enhancement from NIST SP 800-53 with the control number, base control title, enhancement title, control text (with parameter values in brackets), discussion, and related controls. This information is examined as the control is being considered for inclusion in the control set being developed. This example is for reference only.

SC-8(1), Transmission Confidentiality and Integrity | Cryptographic Protection

Implement cryptographic mechanisms to [*Selection (one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission.

Discussion: Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPsec. Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

Related Controls: SC-12, SC-13.

The WG must also capture notes on decisions made during the discussions (e.g., decisions to include or not include certain controls, or controls that could be candidates for other control sets. These notes can be used later to refresh memories when presenting decision rationales (e.g., during comment adjudication), or when a control set is updated over time and may be informative to new WG members regarding historical context and rationales for control specifications.

The WG designates one or more WG members to maintain all working control set documentation including the draft control set and control specification spreadsheet. After the control set is approved, the WG provides copies of their working documentation to the USDOT to facilitate future updates to the control set. Maintaining the working documentation is a valuable tool for the team because it provides a historical record of the decisions made. The working document is useful for future WG members as membership evolves over time and for refreshing the WG's collective memory between control set versions.

The control set identifies controls and enhancements selected from NIST SP 800-53 due to the characteristics of the environment, information, or functions associated with the topic of the control set (i.e., the physical object).

Each control set specification includes entries as illustrated in the box below. Some entries are mandatory, and some are optional. The entries are:

- Control/Enhancement Number (mandatory) (enhancement in parentheses, e.g., in the example below the base control is SC-8, and the enhancement is SC-8(1).)
- Base Control Title and Enhancement Title (mandatory), separated by vertical line (e.g., in the example below, the base control title is “Transmission Confidentiality and Integrity”, and the enhancement title is “Cryptographic Protection”)
- Responsible Party (Manufacturer/Infrastructure Owner Operator [IOO])
- Justification to Select (mandatory)[9]
- Guidance (optional)
- Parameter Value(s) (optional)
- Risk References and Resources (optional) (e.g., ARC-IT Mechanisms, NIST SP 800-82 guidance, ATT&CK for ICS mitigations and techniques)
- Standards (optional)

[9] There may be scenarios where it is necessary to indicate that a control should never be selected for a given physical object. In that case, change “Justification to Select” to “Justification to Not Select” and provide the risk-based rationale.

Example of a Detailed Control Specification

This is an example of an entry as it might appear in the *Detailed Control Specifications* section of a control set. It includes each of the possible entries from the above bulleted list. Each entry is explained below. For a detailed explanation, see the ITS Control Set Template.

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

Standards: IEEE 1609.2, RFC 8446

Control specifications should only be identified in a control set if there is clear risk-based justification related to the control set topic, as defined in the *Physical Object Characteristics* section. As conveyed in the ITS Control Set Template, that section lists the relevant threats that have a certain likelihood of exploiting a vulnerability of the physical object to create an impact to ITS.

The mandatory *justification to select* statement explains the logic behind the decision to include a control in the control set. Justifications are useful in bridging the knowledge/experience gap between control SMEs and control set topic SMEs. Justifications are also helpful for users (e.g., ITS practitioners) implementing the control set and making any risk decisions related to the control.

If a control should be implemented differently from the way it would be implemented for a typical system due to the control set’s characteristics or assumptions, include that information in *guidance* in the *Detailed Control Specifications* section. The optional *guidance* entry may be used to explain the relevance of the control to the control set topic or to help support the unique implementation of the control for the physical object.

A *parameter value* is the variable part of a control or control enhancement. An organization-defined value can be assigned, or a value can be selected from a predefined list provided as part of the control or control enhancement. The Control Set Working Group will include representatives of that community and will assign parameter values where appropriate. Assigning a value allows the community to customize a specific, organization-defined value to the control or control enhancement, such as assigning a list of roles to be notified or a value for the frequency of testing. Selecting from a predefined list allows a community organization to select one or more values from a narrow range of items provided as part of the control or control enhancement (e.g., selecting to either restrict an action or prohibit an action). Establishing parameter values gives community organizations the capability to customize controls based on desired security safeguards and can reflect policy, existing guidance, or best practices.

A *risk reference or resource* points to other sources of information that may be relevant to the control selection or implementation (e.g., ARC-IT mechanisms, ATT&CK for ICS mitigations and techniques, or NIST SP 800-82 guidance for ICS).

Control sets may also offer advice or recommendations for controls that may not typically be applicable, but have relevance when selected through other means, such as during system-specific tailoring, or design/engineering decisions (e.g., choosing wireless communications). In these situations, the controls should be addressed in the *Implementation Considerations* section. Addressing these controls in the *Implementation Considerations* section offers a means to provide additional guidance related to a control without including the control in the *Detailed Control Specifications* section.

Some control sets are closely tied to standards or best practices. If so, the *standards* statement in the *Detailed Control Specification* section should cite the relevant standard or best practice to help users of the control set locate additional relevant information.

Some WGs have found it useful to review documentation such as policies, standards, best practices, or the control set characteristics (particularly the threats and vulnerabilities) and then search through the NIST SP 800-53 control catalog to identify the control or enhancement most relevant to the objective or practice defined in the control set-related documentation. As another approach, WGs may review each control and enhancement in the control catalog to identify controls potentially relevant to the physical object that is the topic of the control set.

Control set WGs may find answering the following questions helpful when discussing and selecting controls and enhancements:

- Does the control or enhancement broadly apply to the type of environment, information, or functions specifically and uniquely covered by the control set, and why?
- Does the control or enhancement have a specific tie to the characteristics of the control set topic (as defined in the *Physical Object Characteristics* section)? If there is no specific tie, the control or enhancement may not be appropriate for the control set or the *Physical Object Characteristics* section may need to be revised if a new characteristic is identified.
- Does the control or enhancement help meet a requirement of a standard or a best practice? If so, document the standard or best practice.
- Is the control or enhancement introduced by other means (e.g., during system-specific tailoring, design/engineering decisions), but requires guidance specific to the control sets' topic? If so, the control or enhancement may be best addressed in the *Implementation Considerations* section.
- Does the control apply in certain situations with modification or require compensating controls? If so, the guidance needed for these controls may be best addressed in the *Implementation Considerations* section.

The following assumptions apply to control selections:

- Control sets are used to identify controls and enhancements necessary to implement existing policies, requirements, standards, or best practices that are associated with the control set topic. Control sets are not used to establish policy.
- Per NIST SP 800-53[10], if a control enhancement is selected, the corresponding base control must also be selected. This is so, because the control enhancements are inherently related to their base control, as the enhancements provide capability that augment a base control.
- Controls or enhancements should not be included in the control set unless they have a direct relation to the control set topic and its defined characteristics.
- Related controls listed in the NIST SP 800-53 catalog should be considered in control set development. Related controls impact or support the implementation of a particular control or control enhancement, address a related security capability, or are referenced in the discussion section.
- The allocation of controls to specific components within an ITS physical object or areas within the environment of operation is beyond the scope of a control set. Allocation decisions are most often made in design and engineering processes.

Other tips:

- In addition to NIST SP 800-53, have the draft control set *Physical Object Characteristics and Applicability* sections available and open during the control selection process. The characteristics guide selection decisions.
- If a control selection cannot be agreed upon, note it as a parking lot item and revisit it later to remain on schedule.
- Maintain the draft control set and control set specification spreadsheet, if used, in a manner that provides version control during control set development.
- Note needs for tailoring decisions, definitions, and other items in the spreadsheet or parking lot for consideration when writing the control set.

4.7 Write the Control Set

Once the control selections have been made, the control set WG completes the *Summary of Control Specifications*, *Detailed Control Specifications*, and *Implementation Considerations* sections in the draft control set document, based on the examples in the ITS Control Set Template.

- The *Summary of Control Specifications* section is a table that summarizes the information in the *Detailed Control Specifications* section.

[10] See Chapter 2.2, page 10.

- The *Detailed Control Specifications* section includes control set specifications (e.g., the mandatory Justification to Select and the conditional Guidance, Parameter Values, and Risk References and Resources elements as appropriate) for control selections.
- The *Implementation Considerations* section provides general guidance that should be considered for conditional controls while conducting system-specific tailoring or while designing and engineering a solution.
- In addition, the *Glossary* section is also added at this time and includes terms unique to the control set.

The following summarizes the steps to write a control set. While the steps are listed in a linear manner, it may be necessary to repeat steps as more information is gained and the control selections are refined. In addition, WGs may find it beneficial to combine steps when working through the controls. For example, WGs may determine the justification (step 5) and other relevant information (step 6) when a control is selected (step 3).

1. Determine control set *Assumptions and Characteristics* and write the section using the ITS Control Set Template as a guide.
2. Determine *Applicability* questions and write the section using the ITS Control Set Template as a guide.
3. Write the *Identification* section using the ITS Control Set Template as a guide.
4. Identify the controls and enhancements that should be selected.
5. Develop a Justification to Select for each control or enhancement selected.
6. For each control or enhancement selected, develop additional specifications, if necessary. This includes *Guidance*, *Parameter Values*, and *Risk References and Resources*.
7. Write the *Detailed Control Specifications* section using the ITS Control Set Template as a guide.
8. Create the table and write any text for the *Summary of Control Specifications* section based on the *Detailed Control Specifications* section using the ITS Control Set Template as a guide.
9. Determine general guidance and write the *Implementation Considerations* section using the ITS Control Set Template as a guide.
10. Maintain the *Glossary* section using the ITS Control Set Template as a guide as entries arise rather than creating the *Glossary* as a last step.

After a draft ITS control set is written, the WG Lead shares it with the entire control set WG, including the WG Advisor for an internal review, comment, and comment resolution. Once comments are resolved by the WG, the WG Lead and WG Advisor present the draft control set to the USDOT to begin the external review and approval process.

4.8 Review / Approve the Control Set

The WG Advisor may have other WG Advisors (from other control set development efforts if those exist and are active) review the draft control set to provide a more comprehensive review, ideally saving the WG time during the review process. After the WG completes its internal review of the completed control set draft in coordination with the WG Advisor, the control set begins the USDOT review process. The WG Advisor, having been involved in the WG review process, can identify to the USDOT potential issues that can be expected when the USDOT distributes the control set for comment to the wider ITS community.

The USDOT's review process should be used for reviews of the control set. This may include an informal and a formal review process. Informal reviews assist in identifying and adjudicating potential critical comments early in the coordination process, to enable a draft control set to move along more smoothly in the formal review process.

The WG can include a "Note to Reviewers" section in the draft control set and/or in an accompanying email to focus reviewers' attention on specific sections of the control set (e.g., questions about a control or enhancement, highlight changes from a previous version).

Informal Review Process

- The USDOT conducts an initial review to determine whether the control set is logical, consistent with the guidance in the control set template, and ready to move into the informal review process. The control set is passed on to key members of the ITS community, who have 2-3 weeks to review the control set and provide comments using the USDOT-provided comment matrix.
- The control set WG adjudicates the comments, revises the control set, and updates the spreadsheet (if used). A WG member captures the results of the adjudication session in a consolidated comment matrix. The WG should be allowed no more than 2 weeks to adjudicate the comments during the informal review process, but that timeframe may be dependent on the number and complexity of comments received. The WG Lead should make a recommendation on the allotted time.
- Once a control set WG and the USDOT are satisfied with the draft control set, the USDOT will prepare it for pre-coordination review by the key ITS community members, who are expected to further distribute the control set to the SMEs on the control set's topic within their organization. Recommended changes, justifications, and comments are recorded in a comment matrix. A WG member gathers all comment matrices and captures the results of the adjudication session in a consolidated comment matrix, revises the control set as appropriate, and updates the spreadsheet (if used). The WG Lead may recommend the allotted time the WG may take to adjudicate the comments. The results of the adjudication session are posted back to the USDOT website and any critical comments are addressed directly with the commenters.
- The USDOT, in conjunction with the control set proponent, determines when a control set WG is ready to move into the formal review process. Depending on the range of comments received, if there were significant changes to the draft control set, and the number and source of critical comments, the USDOT may require multiple informal reviews.

Formal Review Process

- Once a draft control set enters the formal review process, it is on a set timeline for review and adjudication of comments. It is during this process that, at a minimum, the WG Lead and WG Advisor must be prepared and available to follow the schedule to meet suspense dates and stay on schedule.
- During the Formal Review process, the control set is widely distributed to all affected ITS community members for a 20-working day review. Key ITS community members distribute the control set within their organizations, including to SMEs on the control set's topic, and provide comments using the USDOT-provided comment matrix. Each primary member gathers their organization's comments and formally posts their comments to the USDOT website.
- The control set WG allocates a fixed time to adjudicate the comments (e.g., 5-15 working days), captures the adjudication results in the comment matrix, revises/updates the control set

document, updates the spreadsheet (as necessary), resolves issues with any critical and/or substantial commenters, and posts the document and adjudicated comments to the USDOT website for the next review.

- If the control set is not approved, the USDOT will advise the WG as to why. It is most likely one of the fundamental aspects described in the first three sections of the control set is flawed or incomplete. For that reason, the WG should review and update those sections (*Identification and Physical Object Characteristics*) and progress through the process steps again. If it turns out the topic of the control set does not lend itself well to identifying a clear set of assumptions and characteristics, the WG may need to return to the Propose a Control Set step to redefine the scope or approach. If that cannot be done, it is likely the USDOT should recommend dropping the effort as the topic of the control set was never a good candidate. Any lessons learned should be documented for other proposers to consider as they enter this process for other physical objects.

4.9 Publish the Control Set

After the Formal Review is completed and the control set is approved, the USDOT publishes the control set on the website. The control set proponent monitors for changes that influence the control specifications for the control set and initiates any updates as necessary. Users of control sets may also propose changes to a control set by contacting the USDOT.

4.10 Maintain the Control Set

The WG posts their working papers or provides copies to USDOT to post to the USDOT collaboration site. The working papers serve as the starting point for a follow-on WG to maintain and update/revise the published control set. The USDOT is aware of changes in the NIST SP 800-53 control catalog as well as changes to laws, regulations, policies, or standards. Those changes or changes to threats, vulnerabilities, operations, or supported missions may trigger a need to review the control set and determine if updates are required.

The control set proponent must monitor for changes specific to the control set topic, such as new laws, regulations, policies, or standards, which may affect the control specifications in the control set. If the proponent notes new requirements that trigger changes in the control set, the control set proponent contacts USDOT to initiate a new WG to review the control set and determine what revisions and updates may be necessary. USDOT, in consultation with the control set proponent, determines an appropriate starting point in the control set development process.

The USDOT, in consultation with the proponent(s), should periodically review (e.g., annually) all published ITS control sets to determine if they are still needed. If an ITS control set is no longer needed, the control set will be archived for historical purposes.

Chapter 5. Additional Information and Material

The USDOT maintains documentation and tools to support control set development. In addition, each control set will have subject-specific documentation as determined by the WG Lead and SMEs. The USDOT can provide the following:

- Control Set Introduction/Lessons Learned Brief.
- Control Set Template and Instructions.
- Spreadsheet and/or tool containing all controls and enhancements.
- Current version of NIST SP 800-53 (for reference).

Chapter 6. Control Set Development Tasks

Table 2 provides a non-exhaustive checklist of key activities that are performed in the development of a control set. It also indicates which role has primary responsibility for those activities. The list of activities complements and correlates to the list of process steps in **Chapter 4, Process**, but is not intended to replace it. As developers of control sets work through the process steps, they should check off completed items in this checklist and update the checklist to include any additional activities that should be included, as appropriate.

Table 2: Control Set Development Tasks

√	Task	Responsibility
	1. Initial Planning	
	Validate need for WG	USDOT
	Identify candidate WG SMEs through initial data call	USDOT
	Invite additional SMEs to ensure adequate representation	USDOT
	2. Kick-off Meeting	
	Compile list of selected SMEs; finalize SME selection	WG Lead
	Set up kick-off meeting (web access, dial-in, meeting room)	WG Lead
	Send meeting invitation	USDOT /WG Lead
	Update initial presentation (from 4.1, Propose a Control Set)	WG Lead/WG Advisor
	Prepare agenda (NIST SP 800-53, goals, SME commitment)	WG Lead/WG Advisor
	Distribute materials (agenda, presentation, template, frequently asked questions, spreadsheet, task list)	WG Lead
	At kick-off meeting, identify WG Lead and validate SME commitment	USDOT
	Prepare and distribute subject-specific materials	WG Lead

√	Task	Responsibility
	Discuss importance of work, expectations for completion, work with advisors	USDOT
	Discuss subject-specific concerns and issues, if known	WG Lead/WG Advisor
	Identify the NIST SP 800-53 revision to be used to develop the control set	WG Lead/WG Advisor
	3. Initial Leadership Meeting	
	Prepare agenda (goals, responsibilities, tasks, schedule, documentation)	WG Advisor
	Discuss importance of work, expectations for completion, work with advisors	USDOT
	Establish partnership among leads/validate their perspectives and goals	WG Lead/WG Advisor
	Identify SME to draft front matter	WG Lead
	Identify SME to identify initial control allocations (ideal, but not required)	WG Lead
	Establish meeting schedule (frequency, length of meetings, expected duration)	WG Lead/WG Advisor
	4. Control Set Initial Draft	
	Prepare initial draft of control set – **Chapter 1** and **Chapter 2** and revise with the WG advisor	SME/WG Advisor
	Define the physical object/s and the types of environments, information, or functions associated with the control set	SME/WG Advisor
	Define assumptions and characteristics associated with each physical object	SME/WG Advisor
	Define how the assumptions and characteristics vary within each environment, information, or function	SME/WG Advisor
	List the applicability questions used to distinguish the physical object/s	SME/WG Advisor
	Document the NIST SP 800-53 revision used to develop the control set	SME/WG Advisor
	Review other control sets (published or in development) and determine if any are used in conjunction with the control set in development	SME/WG Advisor
	5. Spreadsheet	

√	Task	Responsibility
	Modify the control specification spreadsheet to meet the needs of the WG	SME/WG Lead
	Incorporate multiple recommendations into the spreadsheet	SME/WG Lead
	Maintain spreadsheet during control set development	SME/WG Lead
	6. Control Set Development Meetings	
	Lead discussion on controls and their applicability to the control set	WG Advisor/WG Lead
	Record decisions made during the control allocation meetings	WG Lead/SME
	Create “parking lot” for difficult issues and return to them at designated time	WG Lead
	Identify need for and content of guidance for selected controls	SME/WG Advisor
	Identify parameter values specific to the control set	SME/WG Advisor
	Identify risk references and resources relevant to control selections	SME/WG Advisor
	Identify standards relevant to control selections	SME/WG Advisor
	7. Control Set Documentation	
	Update control set as decisions are made	SME/WG Lead
	Incorporate table of controls	SME/WG Lead
	Incorporate controls required by standards or best practices	SME/WG Advisor
	Incorporate control set-specific parameter values	SME/WG Advisor
	Prepare, edit, and incorporate control set guidance	SME/WG Advisor
	Complete any needed definitions	SME/WG Advisor
	Clean up spreadsheet, removing columns added for discussion and data collection	SME/WG Lead
	Update formatting for control set and spreadsheet for consistency	SME/WG Lead
	Gain approval for final control set documentation	WG Advisor/WG Lead
	8. Final Review and Approval Meeting	

√	Task	Responsibility
	Distribute final control set documentation to WG	WG Lead
	Review control set documentation and provide comments	WG members
	Compile comments and distribute to WG at least 1 week before meeting (if needed)	WG Lead
	Adjudicate comments and come to agreement	WG Members/WG Lead/WG Advisor
	Update control set documentation	SME/WG Lead
	9. Ongoing WG Administrative Tasks	
	Maintain list of SMEs	WG Lead
	Set up meetings (web access, dial-in, meeting room)	WG Lead
	Send meeting invitations	WG Lead
	Send updated versions of documents to WG	WG Lead
	Provide ongoing status to USDOT	WG Lead
	Submit final control set documents to USDOT	WG Lead
	Monitor regulations, laws, technology, threat environment, etc. that may require an update to the control set.	WG Lead/SME

Chapter 7. References

ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation https://www.arc-it.net/html/architecture/architecture.html
ARC-IT Goals	Architecture Reference for Cooperative and Intelligent Transportation Goals https://www.arc-it.net/html/archuse/goals.html
ATT&CK Enterprise	MITRE ATT&CK Enterprise https://attack.mitre.org/matrices/enterprise/
ATT&CK ICS	MITRE ATT&CK® for Industrial Control Systems https://collaborate.mitre.org/attackics/index.php/Main_Page
ATT&CK Linux	MITRE ATT&CK Linux https://attack.mitre.org/matrices/enterprise/linux/
ATT&CK Mobile	MITRE ATT&CK Mobile https://attack.mitre.org/matrices/mobile/
ITS Control Set Template	*Intelligent Transportation Systems (ITS) Control Set Template and Instructions*. https://placeholder
ITS Profile	*Intelligent Transportation Systems (ITS) Cybersecurity Framework Profile* https://placeholder
NIST Cybersecurity Framework	National Institute of Standards and Technology, Gaithersburg, MD, *NIST Cybersecurity Framework, Version 1.1* https://www.nist.gov/cyberframework
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
NIST SP 800-30	National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-30, Rev. 1, *Guide for Conducting Risk Assessments*, September 2012. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
NIST SP 800-53	National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020 (includes updates as of December 10, 2020).

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 800-82 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-82, Rev. 2, *Guide to Industrial Control Systems (ICS) Security*, May 2015
https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

Appendix A. Acronyms and Abbreviations

ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
CVRSE	Connected Vehicle Roadside Equipment
FAQ	Frequently Asked Questions
FHWA	Federal Highway Administration
ICS	Industrial Control System
IOO	Infrastructure Owner/Operator
IPsec	Internet Protocol Security
IT	Information Technology
ITS	Intelligent Transportation Systems
ITSRE	Intelligent Transportation Systems Roadway Equipment
NIST	National Institute of Standards and Technology
OBE	Onboard Equipment
OT	Operational Technology
SME	Subject Matter Expert
SP	Special Publication (NIST)
TLS	Transport Layer Security
USDOT	United States Department of Transportation
WG	Working Group

Appendix B. Glossary

Control Set

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.

Physical Object (ARC-IT)

System or device that provides 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.

Parameter Value

(Formerly "organization-defined control parameter.") The variable part of a control or control enhancement that is instantiated by an organization during the tailoring process by either assigning an organization-defined value or selecting a value from a predefined list (e.g., a control set) provided as part of the control or control enhancement.

Security Control

Safeguards or countermeasures prescribed for a system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

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