Cybersecurity Language for the Procurement of Intelligent Transportation System Equipment

www.its.dot.gov/index.htm

January 22, 2024
FHWA-JPO-23-118

U.S. Department of Transportation

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

Notice

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the use of the information contained in this document.

The U.S. Government does not endorse products or manufacturers. Trademarks or manufacturers’ names appear in this document only because they are considered essential to the objective of the document. They are included for informational purposes only and are not intended to reflect a preference, approval, or endorsement of any one product or entity.

Non-Binding Contents

The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide information to the public regarding existing requirements under the law or agency policies. However, compliance with applicable statutes or regulations cited in this document is required.

Quality Assurance Statement

The Federal Highway Administration (FHWA) provides high-quality information to serve Government, industry, and the public in a manner that promotes public understanding. Standards and policies are used to ensure and maximize the quality, objectivity, utility, and integrity of its information. FHWA periodically reviews quality issues and adjusts its programs and processes to ensure continuous quality improvement.

Technical Report Documentation Page

1. Report No.

FHWA-JPO-23-118

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle

Cybersecurity Language for the Procurement of Intelligent Transportation System Equipment

5. Report Date

January 22, 2024

6. Performing Organization Code

HOIT

7. Author(s)

Dan Lukasik, Jack Oden, Robert Sanchez (ORCID: 0000-0002-0763-6146), Brian Russell, Kyle Rush, Adam Chandler

8. Performing Organization Report No.

9. Performing Organization Name and Address

Leidos Inc.
1750 Presidents Street
Reston, VA 20190

10. Work Unit No. (TRAIS)

11. Contract or Grant No.

693JJ322A000005

12. Sponsoring Agency Name and Address

Federal Highway Administration
1200 New Jersey Avenue, SE
Washington, DC 20590

13. Type of Report and Period Covered

Final; February–January 2024

14. Sponsoring Agency Code

HOIT

15. Supplementary Notes

The task order manager is Usman Ali.

16. Abstract

This report presents the cybersecurity procurement language document for the intelligent transportation systems (ITS) equipment. The purpose of this document is to provide information about cybersecurity language that can be inserted into procurement specifications for procurement of new ITS components. The document incorporates security principles to consider when designing and procuring ITS products and services (software updates/patch, systems, maintenance, vulnerability disclosure policies, breach notification, and initial device or system configurations) and provides example language to incorporate into procurement specifications.

17. Keywords

Procurement Language, Cybersecurity, Apps, Intelligent Transportation System, ITS

18. Distribution Statement

No restrictions. This document is available to the public through the National Technical Information Service, Springfield, VA 22161. http://www.ntis.gov

19. Security Classif. (of this report)	**20. Security Classif. (of this page)**	**21. No. of Pages**	**22. Price**
Unclassified	Unclassified	46	N/A

SI* (MODERN METRIC) CONVERSION FACTORS

APPROXIMATE CONVERSIONS TO SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
LENGTH				
in	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
AREA				
in^2	square inches	645.2	square millimeters	mm^2
ft^2	square feet	0.093	square meters	m^2
yd^2	square yard	0.836	square meters	m^2
ac	acres	0.405	hectares	ha
mi^2	square miles	2.59	square kilometers	km^2
VOLUME				
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft^3	cubic feet	0.028	cubic meters	m^3
yd^3	cubic yards	0.765	cubic meters	m^3
NOTE: volumes greater than 1,000 L shall be shown in m^3				
MASS				
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2,000 lb)	0.907	megagrams (or “metric ton”)	Mg (or “t”)
TEMPERATURE (exact degrees)				
°F	Fahrenheit	5 (F-32)/9 or (F-32)/1.8	Celsius	°C
ILLUMINATION				
fc	foot-candles	10.76	lux	lx
fl	foot-Lamberts	3.426	candela/m^2	cd/m^2
FORCE and PRESSURE or STRESS				
lbf	poundforce	4.45	newtons	N
lbf/in^2	poundforce per square inch	6.89	kilopascals	kPa

APPROXIMATE CONVERSIONS FROM SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
LENGTH				
mm	millimeters	0.039	inches	in
m	meters	3.28	feet	ft
m	meters	1.09	yards	yd
km	kilometers	0.621	miles	mi
AREA				
mm^2	square millimeters	0.0016	square inches	in^2
m^2	square meters	10.764	square feet	ft^2
m^2	square meters	1.195	square yards	yd^2
ha	hectares	2.47	acres	ac
km^2	square kilometers	0.386	square miles	mi^2
VOLUME				
mL	milliliters	0.034	fluid ounces	fl oz
L	liters	0.264	gallons	gal
m^3	cubic meters	35.314	cubic feet	ft^3
m^3	cubic meters	1.307	cubic yards	yd^3
MASS				
g	grams	0.035	ounces	oz
kg	kilograms	2.202	pounds	lb
Mg (or “t”)	megagrams (or “metric ton”)	1.103	short tons (2,000 lb)	T
TEMPERATURE (exact degrees)				
°C	Celsius	1.8C+32	Fahrenheit	°F
ILLUMINATION				
lx	lux	0.0929	foot-candles	fc
cd/m^2	candela/m2	0.2919	foot-Lamberts	fl
FORCE and PRESSURE or STRESS				
N	newtons	2.225	poundforce	lbf
kPa	kilopascals	0.145	poundforce per square inch	lbf/in^2

*SI is the symbol for International System of Units. Appropriate rounding should be made to comply with Section 4 of ASTM E380. (Revised March 2003)

Table of Contents

List of Tables

List of Abbreviations

ALPR	automatic license plate reader
ATMS	advanced transportation management system
AVC	automatic vehicle classification
CCTV	closed-circuit television
CD/DVD	compact disk/digital video disk
CIA	confidentiality, integrity, and availability
CISA	Cybersecurity and Infrastructure Security Agency
CVSS	common vulnerability scoring system
DHS	U.S. Department of Homeland Security
DMS	dynamic message sign
DOE	U.S. Department of Energy
DOT	department of transportation
FHWA	Federal Highway Administration
HBOM	hardware bill of materials
IEEE	Institute of Electrical and Electronics Engineers
IT	information technology
ITS	intelligent transportation system
NIST	National Institute of Standards and Technology
NTCIP	National Transportation Communications for ITS Protocol
OBU	onboard unit
OWASP®	Open Worldwide Application Security Project
PDF	portable document format
PII	personally identifiable information
RSU	roadside unit
RWIS	road weather information system
SBOM	software bill of materials
SP	special publication
USB	universal serial bus
USDOT	U.S. Department of Transportation

Executive Summary

Intelligent transportation systems (ITS) involve deploying technology to help improve the operations, effectiveness, efficiency, and safety of the transportation system. ITS includes physical systems that provide signaling and other traffic control; visual information regarding traffic status; and communications and information infrastructure that transmits and receives, stores and processes, and displays traffic information that engineers and operators use to manage the system and respond to emergencies. ITS includes operating systems, drivers, support and service software, and the applications that provide transportation services.

ITS involves various levels of hardware, software, and firmware interconnected via various communication methods, which makes them subject to the same cybersecurity risks that any computing or electronic device faces. There are also additional risks because ITS are public-facing operational technology /information technology (IT) systems. One example in ITS is hacking dynamic message signs (DMS) along highways to display nefarious unintended messages. This hacking can occur when a DMS is left unprotected with minimal cybersecurity protections, such as firewalls or acceptable settings for password and device configuration. Cybersecurity policies, plans, procedures, tools, techniques, and personnel help protect the valuable information of organizations and the physical systems that provide services to the organization. Such protections mitigate the inappropriate actions of malicious individuals or organizations.

The purpose of this document is to provide recommended cybersecurity language that can be inserted into procurement specifications for ITS components and devices. This language can apply to the following examples of ITS devices:

- Closed-circuit television (CCTV) cameras
- Automatic license plate reader (ALPR) cameras
- DMS
- Traffic signal controllers
- Ramp meter controllers
- Road weather Information systems (RWIS)
- Vehicle detection systems
- Automatic vehicle classification (AVC) systems

This document focuses on these ITS field components only. Other ITS components, such as servers, communication devices, computing environments, and transportation management software, also require cybersecurity protection. Those systems and components are not discussed in this document.

Public agencies, designers, and consultants can use this document to improve procurement specifications for the above-listed ITS components and systems. System integrators and equipment vendors can use this document to assist with and understand changes they may need to make to their products.

To prepare this report, a literature search was conducted (see appendix B). Seven agencies were provided questionnaires and interviewed about their current agency's cybersecurity policies, procedures, and practices for ITS equipment. Key findings of these interviews and questionnaires are described in chapter 2. Some ITS equipment manufacturers were also consulted for their input as well.

For this report, the following key cybersecurity standards, organizational policies, and communities were consulted:

- National Institute of Standards and Technology (NIST)
- Institute of Electrical and Electronics Engineers (IEEE)
- U.S. Department of Homeland Security (DHS)
- U.S. Department of Energy (DOE)
- Open Worldwide Application Security Project (OWASP®)

Table 1 summarizes the specific types of cybersecurity categories and procurement language.

Table 1. Cybersecurity Categories.

Cybersecurity Category	Description of Procurement Language
Software Updates and Patches	Software licenses certifying the release of a secure product that has been tested to an acceptable level. The license identifies security and bug-fix patch levels.
Vulnerability Testing	The practice of undergoing routine cybersecurity vulnerability testing.
Vulnerability Disclosure	The practice of reporting security flaws in computer software or hardware.
Breach Notification	Notification that a systems or data breach to one of the vendor systems has occurred.
Device Configuration	Recommendations on how devices should be configured (e.g., password settings).
Cybersecurity Maintenance	The practices that vendors should follow to keep their products maintained to an acceptable cybersecurity level.
Bug Bounty	System or program by which individuals can be recognized and compensated for reporting bugs, especially pertaining to security exploits and vulnerabilities.

Chapter 1. Introduction

1.1 Background

Cybersecurity policies, plans, procedures, tools, techniques, and personnel help protect the valuable information of organizations and the safety of physical systems that provide services to the organization. Such protections mitigate nefarious actions of malicious insiders, individual hackers, and criminal organizations. Organizations provide explicit specifications to vendors to ensure that vendors understand the organizations' intent to acquire devices, applications, and services with the appropriate cybersecurity protections.

intelligent transportation systems (ITS) are a combination of physical systems that provide signaling and other traffic control; visual information regarding traffic status; and communications and information infrastructure that transmits and receives, stores and processes, and displays traffic information that engineers and operators use to manage the system and respond to emergencies. ITS includes operating systems, drivers, and support and service software, and the applications that provide transportation services.

Since the advent of the internet and expanded use of computers and mobile devices, more and more physical and information technology (IT) systems are being connected by developers, integrators, businesses, organizations, and academia to take advantage of relatively inexpensive communication channels. With all of the systems, applications, and data becoming readily available via public and private network connections, individuals and organizations with negative intentions emerged. Their aim has been to steal information, disrupt communications, disable applications, and hold business hostage (e.g., ransomware) for their own benefit. This caused the need to develop cyber monitoring and protection for these publicly available resources. The technologies and expertise that are now referred to as "cybersecurity" were then developed, which are being continually improved. Any communication system that uses connections that can be accessed from other external sources or connections can face a high level of risk of cyberattack. This is true of ITS as well—where ITS connects with other systems including the internet, there is elevated risk of breach of cybersecurity of ITS. Many agency procurement and ITS specialists lack understanding on the growing cyber threats and risks, hence the reason why ITS procurement specifications have historically lacked language to cover cybersecurity protections. One of the purposes of this document is to help address this.

Cybersecurity policies and plans make clear an organization's intent to apply cybersecurity procedures, tools, techniques, and personnel to mitigate these risks. Many cybersecurity breaches can also occur within an organization caused by its own staff; it is not always individuals from outside an organization who have malicious intent. The cybersecurity topics generally applied across the globe include access control, identification and authentication, awareness and training, audit and accountability, security assessment and authorization, and configuration management. These topics should be considered in ITS or any system development and operation. Most relevant to procurement specifications discussed in this document are system and services acquisition and supply chain and other control areas that impact acquisition and supply chain. Procurement specifications are important aspects of these topics.

1.2 Document Purpose

The purpose of this document is to suggest cybersecurity language that can be applied to procurement specifications for ITS components/devices. This example language can be tailored to an agency's policies, desires, and needs. This language can apply to the following ITS devices:

- Closed-circuit television (CCTV) cameras
- Automatic license plate reader (ALPR) cameras
- Dynamic message signs (DMS)
- Traffic signal controllers
- Ramp meter controllers
- Road weather information systems (RWIS)
- Vehicle detection systems
- Automatic vehicle classification (AVC) systems

Public agencies, designers, and consultants can use this document to improve cybersecurity procurement specifications for the above-listed ITS components and systems. System integrators and equipment vendors can use this document to assist with and understand changes they may need to make to their products.

1.3 Objectives

The objective of this report is to develop cybersecurity procurement requirements for ITS equipment. This report provides example cybersecurity procurement language and practices an ordering agency can use to communicate terms and conditions specific to an agency, site, and project. This document incorporates security principles that should be considered when designing and procuring ITS products and services (e.g., software updates/patch, systems, maintenance, vulnerability disclosure policies, breach notification, and initial device or system configurations). It also provides example language to incorporate into procurement specifications. The example language can be tailored to reflect an agency's specific regulatory and procurement needs. The goal is to simplify the effort of adding cybersecurity consideration to existing procurement documents.

1.4 Target Audience

The target audiences for this report include:

- State, county, and city departments of transportation (DOTs)
- Metropolitan planning organizations
- ITS consultants and equipment venders
- System designers
- System integrators

Chapter 2. Background and Literature Summary

This chapter provides background information about cybersecurity for ITS systems, summarizes the results of the literature search, and presents the agency interviews and questionnaires.

2.1 Cybersecurity for Intelligent Transportation Systems Background

The U.S. Department of Homeland Security (DHS) has identified the U.S. transportation system as one of 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. It is fundamental to the U.S. economy to be able to transfer goods to market and allow people to go to work and conduct business. The roadway infrastructure helps mitigate natural disasters, it provides for national security across the country, and generally provides for the quality of life for the U.S. population.(1)

The ITS Cybersecurity Research Program(2) was developed in response to the urgent need to protect ITS from cyberattacks. Securing transportation's critical assets and infrastructure against cyber threats is a shared responsibility of both the public and private sectors. Executive Order 13800(3) encourages Federal agencies to work with their industries and all entities to adopt the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.(4)

The ITS Cybersecurity Research Program works with the transportation community to:

- Identify needs and gaps.
- Advance the technical research that adopts or adapts implementation practices from other industries or develops new approaches specific to transportation management systems.
- Create the tools and resources for effectively managing cyber risk within transportation systems.
- Provide technology and knowledge transfer to support the transportation workforce in their understanding of cyber issues and mitigations.

The U.S. Department of Transportation (USDOT) cybersecurity research objectives offers four strategies as a path forward for industry, government, and academia to realize and sustain the ITS cybersecurity vision:(5)

- **"Adapt and Implement Protective Measures to Reduce Risk Preferentially.** Next-generation ITS architectures provide "defense in depth" and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident. The National ITS Architecture Reference incorporates Confidentiality, Integrity, and Availability (CIA) analysis for all the data flows in the ITS Architecture. CIA analysis is a basic best practice for all organizations trying to secure their communications, and State and local agencies can use this as a starting point when analyzing their own architectures.

  - ITS Standards activities are underway to identify implementation guidance and best practices that can be added to key ITS infrastructure standards.
  - The U.S. DOT partnered with the National Institute of Standards and Technology (NIST) to tailor the NIST Cybersecurity Framework to address connected vehicle systems.

- **Assess and Monitor Risk.** Continuous cyber risk monitoring of all ITS architecture levels and across cyber-physical domains is conducted by transportation sector asset owners and operators.
  - The U.S. DOT sponsored a penetration test of a state and local agency to demonstrate the value of and provide guidance on conducting this type of testing and identify best practices based on the findings of the testing itself.[6]
- **Manage Incidents.** Transportation sector stakeholders are able to mitigate a cyber incident as it unfolds, sustain critical operations during the incident, return to normal operations quickly, and derive lessons learned from incidents and changes in the ITS environment.
  - USDOT sponsored the development of the Secure Credential Management System proof of concept, which secures vehicle-to-vehicle and vehicle-to-infrastructure communications.[7]
  - USDOT developed a Transportation Cybersecurity Incident Response and Management Framework that improves communication and information sharing with transportation roadway stakeholders when detecting and responding to a cyberattack or vulnerability that spans across devices or other sectors.[8]
- **Creating an Organizational Culture of Security.** Cybersecurity practices are reflexive and expected among all transportation sector stakeholders."

USDOT has developed training through the ITS Professional Capability Building Program on specific cybersecurity topics.[9] USDOT partners in research with NIST and DHS. USDOT departments that are involved with cybersecurity include the Federal Highway Administration (FHWA), Federal Motor Carrier Safety Administration, Federal Transit Administration, and National Highway Traffic Safety Administration.

2.2 Literature Summary

This section summarizes the method used to gather information for this report and presents key findings observed from this literature search. A literature search was conducted, and interviews/questionnaires were completed by several government agencies and some equipment vendors. Some DMS and CCTV manufacturers were contacted as well.

The following government agencies were involved:

- Nevada DOT
- Louisiana Department of Transportation and Development
- New York State DOT
- Florida DOT
- California Department of Transportation headquarters

- Los Angeles County Public Works
- City of Pasadena

Based on initial data collection for the literature review and stakeholder input summary in the first deliverable under task 2, draft technical memorandum, the listed documents were used to focus on adding cybersecurity to ITS operational technology procurement. Configuration at delivery, vulnerability or exploit disclosure, patch support and management policies, and expectation of how coordinated disclosure are handled were addressed. For this report, the results of the literature review were expanded to add detail. The next sections summarize key information gleaned from the literature search.

2.2.1 Agency Questionnaires

Table 2 summarizes the common answers and other observations gleaned from the agency interviews and questionnaire responses. Fifteen 15 questions were asked of each agency.

Table 2. Agency Interview Questions and Summary of Responses.

Question	Responses (Summary)
1) Does your agency have cybersecurity language in your procurement documentation? If so, is it a standard boilerplate or do you customize it for each project? If so, what sources of information do you use to generate cybersecurity-related procurement language for ITS equipment acquisitions? **If not, is there any equipment at your agency that has cybersecurity requirements in their procurement documents?**	Yes, most of the agencies have cybersecurity language in their general procurement documentation, but often does not include cyber-specific language within the procurement documents for specific ITS components. It is in the form of standard boilerplate, which is customized according to projects by some agencies. The sources of information used to generate cybersecurity-related procurement language include agency-specific policies and procedures, State guidelines, and industry standards. Only one agency had no cybersecurity requirements.
2) Do you install software updates to address security vulnerabilities? If so, can you describe how it is done? **What challenges do you face as it relates to providing ITS equipment software updates that address known vulnerabilities?**	Yes, agencies install software updates to address security vulnerabilities. Different scans are performed according to policies to assess vulnerabilities. Further, the vendor is contacted for assistance if needed. Vulnerabilities are prioritized according to risk level and access ease. Challenges include system downtime, coordination with vendors, understanding security flaws, identifying necessary updates, and managing aging devices that may lose support.

Question	Responses (Summary)
3) Describe typical service level agreement clauses that you have in place with your ITS equipment vendors related to lifecycle cybersecurity support (incident handling, vulnerability management, etc.).	The overall response indicates that the presence and specificity of service level agreement clauses related to lifecycle cybersecurity support with ITS equipment vendors vary among the transportation agencies surveyed with most of them having it. While some contracts and policies address incident handling and cybersecurity requirements, there is a need for improvement in terms of comprehensive coverage for all ITS projects and equipment.
4) What are your contractual requirements for ITS equipment vendors to communicate device end-of-support and/or end-of-life dates to their end customers/users? As a customer/user, what expectations do you have on this type of communications?	The overall response indicates a lack of specific contractual requirements for ITS equipment vendors to communicate end-of-support and end-of-life dates to their customers/users. While some agencies expect vendors to proactively notify them, others rely on vendor websites and communication channels to stay informed. There is a need for improvement in this area to ensure timely and transparent communication about end-of-life and end-of-support milestones.
5) Do you currently implement cybersecurity process gates within your procurement lifecycle for ITS equipment? If so, can you describe the required process gates?	The overall response indicates a mixed implementation status of cybersecurity process gates within the procurement lifecycle for ITS equipment. While some agencies have implemented specific measures such as vulnerability scanning, penetration testing, and system upgrades, others have not implemented such processes or have limited understanding of the concept. There is a need for further development and improvement in ensuring consistent cybersecurity measures throughout the procurement lifecycle.
6) Are there policies in place that require a vulnerability scan/penetration test conducted against any newly procured ITS equipment type? Can you please describe the specifics of the scanning (e.g., must it be done by an independent third party)? Must the scan conform to certain standards? Is the scan required to be repeated (e.g., on an annual basis)?	The responses indicate a mixed implementation of policies requiring vulnerability scans or penetration tests on newly procured ITS equipment. While some agencies have routine scanning and third-party testing practices in place, others do not currently have such policies. The frequency of scans, involvement of third parties, and compliance with certain standards may vary depending on the agency.

Question	Responses (Summary)
7) Do you have sufficient visibility into the hardware and software components that make up ITS equipment (e.g., software bill of materials [SBOM], hardware bill of materials [HBOM])?	The level of visibility into the components of ITS equipment varies across the agencies. Some agencies have access to third-party component lists for central software systems, while others rely on scanning and inventory tools to gather information. The availability of component information for field equipment may be limited, and there is a need for comprehensive asset management solutions in some cases. Efforts are being made to engage with vendors to ensure modern secure protocols and standards are implemented in new ITS device procurements.
8) Do you have contractual requirements for delivery of cybersecurity-related documentation (secure operations manuals, secure configuration guides, diagrams, etc.) from ITS equipment vendors upon acquisition of new equipment? If so, can you describe the documentation that is required?	The overall responses indicate the level of contractual requirements for cybersecurity-related documentation varies across the agencies. Some agencies have specific requirements and reference cybersecurity policies and procedures, while others have no explicit contractual language in place. The inclusion of documentation may depend on the project scope and deliverables.
9) Do you have processes and systems in place to monitor ITS equipment for potential intrusion or introduction of malware? If so, can you describe the process, systems and/or tools that are used? **Are there associated standards that ITS equipment must adhere to in order to integrate into these processes/systems? If so, can you please name the standards?**	Some agencies have implemented monitoring systems, such as intrusion detection systems, intrusion prevention systems, and malware tools, while others rely on third-party monitoring solutions and vulnerability scanning with tools such as Tenable Nessus®. The standards followed include NIST Special Publication (SP) 800-53,[10] agency policies and directives, State administrative manuals, and National Transportation Communications for ITS Protocol (NTCIP) in some cases.
10) What existing authentication frameworks must be supported to enable remote management of ITS equipment?	The authentication frameworks for remote management of ITS equipment include site-specific passwords and roles/levels of access; various vendor-specific protocols such as lightweight directory access protocol, active directory integration, multifactor authentication, virtual private network access with permission requests, the disabling of unsecure protocols; and adherence to relevant standards and policies. The specific frameworks used vary across districts and align with relevant policies and standards.

Question	Responses (Summary)
11) What are your contractual requirements for vendor security of any software-as-a-service cloud systems interfaced to ITS equipment?	The contractual requirements for vendor security of software-as-a-service cloud systems interfaced to ITS equipment range from being to be determined or covered by specific forms and manuals to incorporating standard boilerplates referencing cybersecurity policies and procedures. The specific requirements may vary based on policies, governance, and relevant standards.
12) Can you share your current standard equipment procurement specifications for the following components? **a. CCTV cameras** **b. DMS** **c. Traffic signal controllers** **d. Ramp meter controllers** **e. Connected vehicle roadside units (RSU)/onboard units (OBU)** **f. Communication hardware/switches** **g. Cellular modems** **h. Advanced transportation management system (ATMS) software** **i. ATMS servers** **j. Video servers**	Based on the provided responses, the summary of the current standard equipment procurement specifications for various components in the ITS domain is listed below. Some agencies provide their sample or standard procurement documents for these components: a. CCTV cameras b. DMS c. Traffic signal controllers d. Ramp meter controllers e. Connected vehicle RSUs/OBUs f. Communication hardware/switches g. Cellular modems h. ATMS software i. ATMS server j. Video servers Very few of the example procurement documents contained cyber language.
13) Can you describe any cyber challenges that you have had within the ITS solutions (e.g., compromised network, unprotected devices, etc.)?	The challenges faced within the ITS solutions include concerns related to equipment sourcing, information deficit, standardization efforts, and security measures such as patching vulnerabilities, controlling access, and addressing limitations of older devices and protocols. Overall, there have been little to no reported breaches or cyber incidents.
14) Which groups/departments within your agency control cybersecurity guidelines for ITS equipment and software purchase?	The responsible departments/groups for cybersecurity guidelines in ITS equipment and software purchases include State IT, agency (e.g., DOT) IT, transportation management center operations, and ITS departments. These departments collaborate to establish and maintain cybersecurity guidelines and address risks associated with hardware and software within the ITS domain.

Question	Responses (Summary)
15) What cybersecurity and ITS standards are followed/used as it relates to the procurement of ITS components?	The agencies follow a combination of industry standards, specific agency standards, and cybersecurity policies and procedures to guide the procurement of ITS components. These include internal guidelines, industry specifications, and references to agency cybersecurity policies. Vulnerability scanning and risk assessment are also conducted for new ITS components.

2.2.2 Vendor Questionnaires

Table 3 summarizes the common answers and other observations gleaned from the vendor interviews and questionnaire responses. Twenty-five percent of the requested vendors provided responses. Nine questions were asked of these vendors.

Table 3. Vendor Interview Questions and Responses.

Question	Response
How is device security configuration guidance communicated to your customers today? For example, is there security configuration documentation? Is there security configuration training? Are there online tutorials? Other methods?	We currently do not have any documentation with regards to device security configurations, as each end user network is different.
Do you participate in vulnerability disclosure programs? If so, can you describe them? **What is your process for handling unsolicited feedback from the cybersecurity research community? For example, do you have an open system to allow the research community (or others) to provide feedback, provide suggestions, or offer enhancements to your product's security?**	We do not currently participate in any vulnerability programs. We adhere to and update our devices in cases of known vulnerabilities that have been discovered. We do not have a process for handling unsolicited feedback from the cybersecurity research community.
Do you participate in bug bounty programs? If yes, can you describe the specifics of the program?	We do not participate in any bounty programs.
Do you publish anticipated end-of-life product dates for your devices?	We only publish the end-of-life for cameras that have been discontinued. We do not normally publish anticipated end-of-life product dates.
Do you provide support tools to customers (e.g., scripts or aids) that are designed to assist in the secure configuration of your ITS equipment in the field? If so, can you describe these tools and how they are provided? What type of documentation is provided with the tools?	We provide a camera tool (Costar™ Utility) to use when configuring, discovering, and maintaining our cameras. The documentation for basic level 1 usage is located on our knowledge-based authentication site.

Question	Response
What cybersecurity practices do you follow for secure development of your ITS equipment?	The access to the camera hardware design files and software source code is restricted. This information is accessible to the authorized personnel using encrypted communication.
Do you have sufficient visibility into the hardware and software components that make up ITS equipment (e.g., SBOMs/HBOMs)?	We do have sufficient visibility into the SBOM/HBOM of the cameras.
Which group/department within your agency controls cybersecurity guidelines for ITS equipment and software purchase?	Product steering committee (quality assurance, engineering, and product management) controls the cybersecurity guidelines for ITS equipment and software purchase.
What cybersecurity and ITS standards are followed/used as it relates to the procurement of ITS components?	Components are selected to be compliant with the National Defense Authorization Act.(11)

2.3 Intelligent Transportation System Equipment Procurement Documentation

ITS equipment procurement documentation was obtained from several agencies to check what useful cybersecurity wording (if any) can be used within the procurement specifications. Most ITS procurement documents obtained from public agencies lacked sufficient detail on cybersecurity. These documents included standard and nonstandard special provision for ITS equipment and hardware. Some agencies provided general cybersecurity specifications from their agency IT departments, but the specifications were not specific to purchasing ITS field equipment.

2.3.1 Standards Documentation

Standards and cybersecurity specifications were reviewed from the following:

- America Public Transit Association
- American Society for Testing and Materials
- Cybersecurity & Infrastructure Security Agency (CISA)
- DHS
- Institute of Electrical and Electronics Engineers (IEEE)
- Institute of Transportation Engineers
- NTCIP
- NIST
- Society of Automotive Engineers
- U.S. Department of Energy (DOE)

2.3.2 Vendor Product Information

Product cut sheets and specifications were reviewed to determine application cybersecurity provisions that equipment vendors have already called out. Manufacturer cut sheets were obtained from camera, RSU, and OBU manufacturers; DMS vendors; and traffic signal controllers.

2.3.3 Cybersecurity Documentation

the following USDOT material was researched:

- ITS Cybersecurity Research Program[2]
- *How the U.S. Department of Transportation Is Protecting the Connected Transportation System from Cyber Threats*[12] fact sheet
- ITS standards[14]

After reviewing the documentation, an internet search was conducted, first for other transportation standards, and then for other cybersecurity procurement standards. Experience and knowledge in cybersecurity, generally, as well as in cybersecurity standards and specifications, specifically, was applied to craft the search terminology. Knowledge and experience in applying cybersecurity standards and specifications to acquisition projects for U.S. Government, rail, and energy customers was also applied.

This document provides information about cybersecurity language that can be inserted into procurement specifications for ITS components and devices. While cybersecurity standards exist, none are specifically associated with ITS field hardware and associated software/firmware. Other standards were collected that are either general for cybersecurity, and may apply to ITS, or specific to other operational areas. On further analysis, it is possible to directly apply these standards to FHWA and ITS or modify and adapt them to FHWA and ITS. The standards may not be available to cover all ITS cybersecurity areas of interest. In those cases, the most appropriate procedure to follow further analysis is to determine the risk, threat, and vulnerability to FHWA and ITS operations and areas of interest; select cybersecurity controls to mitigate the risk, threat, and vulnerability; establish a policy, plan, and/or procedure; and/or select and implement a tool and/or technique. In selecting the implementation of a control under consideration, cybersecurity effective practices may be considered, moderated by the age of the effective practice and currently available cybersecurity tools and techniques. Recent threats, vulnerabilities, and attacks may also be considered. The end of this process can also include establishing and publishing a standard that specifically applies to ITS cybersecurity areas of interest. Boilerplate cybersecurity language used to procure ITS products should include: 1) how the vendor describes and protects its systems, 2) how the vendor describes specifications of initial device or system configurations, 3) how the vendor provides maintenance, and 4) requirements for how and when the vendor discloses vulnerabilities, provides and delivers software updates and patches, and notifies customers about breaches of vendor operations and customer data.

2.4 Descriptions of Processes, Plans, and Practices in Use Today

Cybersecurity is assumed to include the families in table 4, as per NIST's Security and Privacy Control Families. After the table these families are further described as the cyber practices in use today. Many of these are not considered topics of standards. To ensure thoroughness, each of these topics should be examined for applicability to DOT’s purpose.

Table 4. Security and Privacy Control Families.

ID	Family	ID	Family
AC	Access control	**PE**	Physical and environmental protection
AT	Awareness and training	**PL**	Planning
AU	Audit and accountability	**PM**	Program management
CA	Assessment, authorization, and monitoring	**PS**	Personnel security
CM	Configuration management	**PT**	PII processing and transparency
CP	Contingency planning	**RA**	Risk assessment
IA	Identification and authentication	**SA**	System and services acquisition
IR	Incident response	**SC**	System and communications protection
MA	Maintenance	**SI**	System and information integrity
MP	Media protection	**SR**	Supply chain risk management

PII = personally identifiable information.

Source: NIST, *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53, rev. 5 (September 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

The following list is a description of each control family and the cyber practices used today, based on NIST SP 800-53:[(10)]

- **Access control —** controlling the use of the system via its collection of various accounts, such as individual, group, system, and application; managing, monitoring, and controlling using automated tools and in such a manner as to ensure the system is used by who the organization authorizes, in the way described by the account role.
- **Awareness and training —** providing basic and role-based system and physical security awareness training to all system users, including managers, executives, and contractors, as initial training for new users and continuing training to refresh or introduce new topics or procedures.
- **Audit and accountability —** collecting system information and examining that information for compliance with security policies and procedures; establishing accountability for system users, managers, executives, and contractors for the system use, using automated tools and in such a manner as to ensure the required level of accountability.
- **Security assessment, authorization, and monitoring —** assessing risk; establishing and implementing security controls, controlling interconnections with other systems, testing and assessing the adequacy of implemented security controls, developing plans of action and milestones to resolve discrepancies found during testing and assessment, providing documented security authorization through an appropriate organization, and continuously monitoring compliance with the controls.
- **Configuration management —** establishing and documenting a system baseline configuration; managing the baseline through change control; performing security impact analysis on all suggested changes to the baseline; controlling permissions to perform changes; documenting all configuration settings; establishing control to a setting of least functionality; developing,

documenting, and maintaining an inventory of all system components; and establishing and maintaining a plan for the conduct of all configuration management activities.

- **Contingency planning —** addressing physical and electronic risks to the system, preparing a contingency plan (or similar plans), training assigned personnel on the contingency plan, testing the plan, establishing a system backup, and providing for system recovery and reconstitution.
- **Identification and authentication —** providing identification and authentication of authorized organizational and non-organizational users and devices, managing identifiers and authenticators, and providing authenticator feedback.
- **Incident response —** providing incident response training, testing, handling, monitoring, reporting, and assistance and codifying them in an incident response plan.
- **System maintenance —** providing for controlled preventive and remedial maintenance, including tools and personnel.
- **Media protection —** accessing, marking, storing, transporting, and sanitizing all removable media, such as compact disks/digital video disks (CD/DVD), universal serial bus (USB) (i.e., thumb drives), flash drives, portable disk drives, and laptop and tablet computers.
- **Physical and environmental protection —** controlling transmission medium, power equipment, cabling, and output devices; monitoring physical access; controlling visitors; providing emergency shutoff and lighting, fire/water/chemical damage protection, temperature and humidity controls, and delivery and removal of equipment; and controlling information leakage and these controls at the alternate work site.
- **Personnel security —** assigning position risk designation, screening personnel, verifying formal indoctrination, developing access agreements, managing third-party personnel security, and employing personnel sanctions.
- **Security planning —** planning security-related activity, which may include sections related to other security topics, or refer to separately published plans.
- **Program management —** assigning a senior information security officer, planning for information security resources, and establishing and acting on plans of action and milestones to correct deficiencies, maintaining a system inventory, measuring and reporting on performance, developing an enterprise architecture, establishing a critical infrastructure plan and a risk management strategy, document the process for security authorizations, and define the system mission and business process.
- **Risk assessment —** categorizing security of information, assessing risk, and scanning for vulnerabilities.
- **System and services acquisition —** managing controlled acquisition of systems and services, including allocating resources, managing the system development lifecycle, controlling the acquisition process, identifying the functional properties of security controls, using information assurance products, documenting the system, establishing software restrictions (especially user-installed software), applying software engineering principles, identifying and controlling connections to external systems, ensuring developers maintain configuration management and conduct testing and evaluation, and applying supply chain security.
- **System and communications protection —** partitioning applications, controlling information in shared resources, protecting against denial-of-service attacks, protecting the system boundaries, protecting confidentiality and integrity during transmission, terminating network connection appropriately, establishing a trusted path, establishing and managing network keys, controlling mobile code, controlling voice over internet protocol, providing secure name and address resolution, authenticating sessions, addressing fails in a known state, protecting information at rest, and partitioning information.

- **Supply chain risk management —** addressing the controls over the dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers; presenting an increasing level of risk to an organization and addressing threats such as unauthorized production, insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain, whether endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation.
- **System and information integrity —** remediating flaws, protecting from malicious code, and monitoring information systems.
- **Personally identifiable information (PII) processing and transparency —** addressing the within-systems and organizations that contribute to security and privacy assurance; updating PII processing and transparency that result from assessment or audit findings, privacy breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Chapter 3. Sample Cybersecurity Procurement Language

This section provides sample cybersecurity procurement and implementation language and practices that an ordering agency can use to communicate terms and conditions specific to an agency, site, and project. The language incorporates security principles that should be considered when procuring ITS products and services specific to delivering or providing ITS equipment (e.g., software updates/patch, systems, maintenance, vulnerability disclosure policies, breach notification, and initial device or system configurations).

The sample procurement language is not regulatory guidance from FHWA. It is intended to serve as a starting point for an agency to develop procurement language to address its cybersecurity objectives. It may be helpful for agencies to consult internal legal teams and relevant information security managers and staff to consider local regulations related to cybersecurity assistance. Table 5 summarizes the specific types of cybersecurity categories and procurement language.

Table 5. Recommended Cybersecurity Categories and Procurement Language.

Cybersecurity Category	Description of Procurement Language
Software Updates and Patches	Software licenses certifying the release of a secure product that has been tested to an acceptable level. The license identifies security and bug-fix patch levels.
Vulnerability Testing	The practice of undergoing routine cybersecurity vulnerability testing.
Vulnerability Disclosure	The practice of reporting security flaws in computer software or hardware.
Breach Notification	Notification that a systems or data breach to one of the vendor systems has occurred.
Device Configuration	Recommendations on how devices should be configured (e.g., password settings).
Cybersecurity Maintenance	The practices that vendors should follow to keep their products maintained to an acceptable cybersecurity level.
Bug Bounty	System or program by which individuals can be recognized and compensated for reporting bugs, especially pertaining to security exploits and vulnerabilities.

3.1 Intelligent Transportation System Device-Specific Language

Table 6 lists the types of cybersecurity language recommended to include for each device type, based on the recommended procurement language in chapter 3.

Table 6. Types of Cybersecurity Language Recommended for Specific ITS Devices.

ITS Device	Software Updates and Patches	Vulnerability Testing	Vulnerability Disclosure	Breach Notification	Device Configuration	Cybersecurity Maintenance	Bug Bounty
CCTV camera	x	x	x	x	x	x	x
ALPR camera	x	x	x	x	x	x	x
DMS	x	x	x	x	x	x	x
Traffic signal controller	x	x	x	x	x	x	x
Ramp meter controller	x	x	x	x	x	x	x
RWIS	x	x	x			x	
Vehicle detection system	x	x	x			x	
AVC system	x	x	x			x	

3.2 Software Updates and Patches Language

For all ITS device software and firmware provided for a specific project or agency, it is suggested to issue some type of documentation (e.g. a license, release notes, etc.) to the owning government agency, typically by the vendor or supplier. The documentation would stipulate the time period for which software is valid and supported. It should be for a period determined by the agency (e.g., of no less than X number of years). It is not suggested there is a subscription or service fee, just documentation on support for the software or firmware.

The documentation must also include a maintenance agreement for the agency-determined period for periodic software and firmware updates, including:

- Security and bug-fix patches issued by the software and firmware manufacturer.
- Security patches to address any identified vulnerability, such as in the National Vulnerability Database[15] with a common vulnerability scoring system (CVSS) severity rating of medium or higher. Software and firmware manufacturers must agree to patch for high and critical security issues within 60 days or a term determined by the agency.
- Provision of a single software licenses submittal with documentation of the software licenses for all provided software.

The following is suggested example procurement language for software updates and patches:

> **"For ITS software/firmware provided with this ITS component, a software license document shall be issued by the manufacturer that includes:**
>
> **a. Listing of all security and bug patches that have been applied to the delivered version of software/firmware and a description of the purpose for each patch.**
>
> **b. Certification that the delivered software/firmware has been tested for acceptable cybersecurity compliance and has a common vulnerability scoring system (CVSS) qualitative rating of medium or higher.**
>
> **c. Maintenance and warranty of the software/firmware.**
>
> **d. Duration of the warranty is [AA] years.**
>
> **e. Duration of the maintenance period is [BB] years."**

Agencies should evaluate their own IT polices, desires, staffing levels, and budget availability for warranty and maintenance periods. The type and maturity of the equipment may also be a factor. In certain cases, agencies may be able to handle maintenance in-house or by a third party. Most equipment will come with a minimum 1-year warranty, but 2 years is not uncommon.

3.3 Vulnerability Testing Language

It is recommended that ITS equipment vendors routinely test their products for cybersecurity vulnerabilities and correct any moderate to significant vulnerabilities prior to product release. As an option, vulnerability testing can be conducted via independent third parties using standard testing and industry accepted scoring systems. Some vendors provide Open Worldwide Application Security Project (OWASP®) Application Security Verification Standard reports that show either no high or crucial severity findings or show that all findings have been addressed.[16] Other methods and standards can provide a basis for testing application technical security controls, as well as any technical security controls in the environment, and are relied on to protect against known vulnerabilities. The validation method employed should provide agencies additional confidence in the security posture of the supplied products and the supply chain of third-party software, as well as dependencies used in the software and firmware.

The following is suggested example procurement language for cybersecurity vulnerability testing:

> **"Any ITS Component web applications under consideration shall be tested annually for vulnerability against the [Security Standards of Choice] and the results shall be included in a report and made available to the agency. The vendor shall provide a report that verifies there are no high or critical severity findings, or that all findings have been addressed."**

3.4 Vulnerability Disclosure Language

Vulnerability disclosure is the practice of reporting security flaws in computer software or hardware. When an ITS equipment manufacturer discovers a security flaw in its product, the manufacturer should have a means of disclosing this to end users of its products.

The following is suggested example procurement language for vulnerability disclosure:

> **"Vendors shall disclose testing for vulnerabilities of their hardware, software, and firmware products. For all products provided, the vendor shall disclose to our agency via electronic mail, under the following circumstances:**
>
> **a. No later than ([time period—i.e., 72 hours)] of awareness through observation or notification that any vulnerability has been identified.**
>
> **b. No later than [(time period—i.e., 24 hours)] following notification of the development of a mitigation to fix the vulnerability, along with information about how the patch may be retrieved and installed.**
>
> **c. All notification will provide details about the vulnerability and patch, if provided, along with related operational concerns."**

Another consideration for the time period can be based on the severity of the vulnerability that was discovered. For example, a very short time period may be desirable for a vulnerability with a fairly high CVSS score. The demarcation line for this is something agencies can discuss with their IT manager and staff to determine what is reasonable.

3.5 Breach Notification Language

It is desired that ITS equipment vendors notify the responsible officials of the specified organization or user (via electronic mail within a specified time period [e.g., 30 days] or as dictated by the State in which the organization or site is operating or by the responsible Federal agency) of any unauthorized access to the vendor's operation, including business, sales, and development.(17) This is particularly desirable for ITS devices that required third-party software for operation. One example is that certain wireless communications vendors require or recommend using cloud data collection tools to obtain data from the sensors.

Like the consideration given to vulnerability disclosure language, breaches that may affect a field device ability to operate safely should have a shorter response time then breaches that may not pose an operational safety risk.

The following is suggested example procurement language for breach notification:

> **"If a vendor has discovered that a breach has occurred to any of its software or firmware components, the vendor shall notify the agency within [CC] days via electronic email. This breach shall include active exploitations including unauthorized access to the client systems that impact operations or data security. The vendor shall also provide information on the process/procedure to temporarily remedy mitigate the situation within [DD] days and permanently remedy the situation within [EE] days."**

3.6 Device Configuration Language

This section provides sample cybersecurity procurement language that agencies can use to communicate their desired provisions for cybersecurity in the ITS equipment.

3.6.1 Recovery Images

For each device on which software or firmware is installed, it is expected that contractors provide a recovery image of the final as-built computer. This image must allow for bare-metal restore such that restoration of the image is sufficient to restore system operation to the imaged state without the need for reinstallation of software. If additional user permissions are required to meet this requirement, coordinate the creation of the image with the identified computer access point of contact.

3.6.2 Backup Configuration

For all controllers, provide a backup of the controller configuration for all loaded application programs (all software that is not common to every controller of the same manufacturer and model).

3.6.3 Documentation

For every component (device or software/firmware) with manufacturer-provided cybersecurity documentation, procedure, or method for secure configuration or installation, provide a report documenting how the component was configured and any deviation from the manufacturer instructions.

For all software applications and firmware running on devices, provided the following:

- Administrator documentation that describes:
  - Secure configuration of the software
  - Secure installation of the software
  - Secure operation of the software
  - Effective use and maintenance of security functions or mechanisms for the software
  - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions for the software
  - Condition and status of all input/output ports on the device, whether physical or logical, at the time of delivery
- User documentation that describes:
  - User-accessible security functions or mechanisms in the software and how to effectively use those security functions or mechanisms
  - Methods for user interaction that enable individuals to use the software in a more secure manner
  - User responsibilities in maintaining the security of the software

3.6.4 Passwords

For all devices with a password, change the password from the default password. Coordinate selection of passwords with the password point of contact. Do not use the same password for more than one device unless specifically instructed to do so. Provide a confidential password report documenting the password for each device and describing the procedure to change the password for each device. Vendors/contractors should provide the password summary report electronically in both portable document format (PDF) and Microsoft® Excel® using a file that is password protected in a mutually agreed-upon method.

Provide [two] [or other quantity] hardcopies of the password summary report, each copy in its own sealed envelope.] [For all devices with a password, coordinate the changing of passwords with the project site following testing of the system but prior to turnover to the [specify organization or site]. Coordinate with the password point of contact to determine appropriate project site personnel to complete password changes. Accompany identified personnel to each device with a password and instruct personnel on the process of changing password. Record the time, date, and personnel present when each device's password is changed and submit a password change summary report documenting this information.

Configuration shall not allow for a weak password to be set. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords. Weak passwords may consist of dictionary words, names, words based on the username, or common variations on these themes. It is recommended to use NIST SP 800-63, *Digital Identity Guidelines*,(18) as a reference.

Consider providing a mode, especially for devices with a large amount of computing power, such as the traffic signal controller, where the factory-provided password must be changed before any configuration can be made by the agency.

Additionally, there should be clarity on how lost passwords are addressed. If a lost password to a device is unrecoverable and the only way to restore a device to operation is to reset it to factory condition, the vendor may want to clearly indicate this. It may also be important for customers to understand that losing a password is not a trivial incident. There should be a good understanding and expectation of multiple levels of reauthentication to recover or reset a device password—at a minimum, a manager may be expected to be notified when a device needs its password reset.

3.6.5 Encryption Protocols

Deprecated encryption protocols (for example, SSLv3, TLSv1, TLSv1.1) should not be supported and must be disabled during configuration when supported by the software or firmware of the device. Encryption protocols must be enabled on all devices, when supported. Non-encrypted protocols must be disabled, and vendors completing configuration must provide a port scan report validating that no insecure protocols have been left enabled on the device across all ports (or this can be vice versa, showing on open ports).

The list of deprecated encryption protocols will change over time. It is suggested that the list of deprecated protocols be maintained in cooperation with the agency's IT support group and the manufacturer of the devices, and that this information be updated in the procurement language as it changes over time. Alternatively, it may be easier at some point in the future to list acceptable encryption protocols instead of listing deprecated encryption protocols that should not be used. This choice is up to the agencies using the procurement language.

When supported to the device, configuration vendors and installers must configure network access controls to restrict device access to only approved devices. All internet protocol addressable devices must be scannable, such that the device can be scanned by industry-standard internet protocol network scanning utilities without harm to the device, application, or functionality. If a government agency IT department has a preferred scanner, this is the place to insert the name into the contract.

The following is example procurement language for device configuration:

“Contractors shall not deliver devices (e.g., CCTV cameras, DMS controllers) to the agency with default manufacturer passwords (e.g., 9999). The password should be changed to something that is a minimum of eight characters, contains both capital and lowercase letters, and contains numbers and miscellaneous characters (e.g., $, %, #, &). The password naming and delivery method should be discussed and agreed to by the agency. It is recommended to use NIST SP 800-63, Digital Identity Guidelines(18) as a reference. Vendors/contractors should provide the password summary report electronically in both PDF and Microsoft Excel using a file that is password protected.

Deprecated encryption protocols [(SSLv3, TLSv1, TLSv1.1)FF] should not be supported and must be disabled during configuration when supported by the software or firmware of the device. Encryption protocols must be enabled on all devices, when supported. Non-encrypted protocols must be disabled, and vendors completing configuration must provide a port scan report validating that no insecure protocols have been left enabled on the device.

All internet protocol addressable devices must be scannable, such that the device can be scanned by industry-standard internet protocol network scanning utilities without harm to the device, application, or functionality.

For all controllers, provide a backup of the controller configuration for all loaded application programs.

For each device on which software or firmware is installed for it is expected that contractors provide a recovery image of the final as-built computer device. This image must allow for bare-metal restore such that restoration of the image is sufficient to restore system operation to the imaged state without the need for reinstallation of software.”

3.7 Cybersecurity Maintenance Language

Submit and license to the [specify organization or site] all software required to operate, maintain, and modify the control system devices such the [specify organization or site] or their agents are able to repair, replace, upgrade, and expand the system without subsequent or future dependence on the contractor, vendor, or manufacturer. Submit hard copies of user manuals for each software with the software submittal.

For software provided and licensed to the [specify organization or site] under the requirements of another section, submit a statement indicating the section and submittal under which the software was provided. For software provided to meet the requirements of this section and not provided and licensed under another section, submit software and software user manuals on removable media (i.e., USB/thumb drives, DVD, or CD) as a technical data package and submit [one hard copy] [and/or [number of] hard copies] of the software user manual for each piece of software (see applicable language in chapter 4).

The following is suggested procurement language for cybersecurity maintenance:

> **“The contractor shall license that all software can be configured, patched, and maintained as it relates to cyber-related configurations, settings, and software updates without the need for manufacturer assistance.”**

3.8 Bug Bounty Program

A bug bounty program is a service offered by many software companies, websites, organizations, and software developers by which individuals can be recognized and potentially compensated for reporting bugs, especially pertaining to security exploits and vulnerabilities. They are also known as vulnerability rewards programs. As part of a vulnerability management strategy, companies often use these crowdsourcing programs to supplement penetration tests and internal code audits. These programs also involve conducting cyber research and allow safe harbor for security researchers.

The bug bounty program should contribute something of interest to the agency’s customers. For example, it should define the minimum scope of the bug bounty program to vulnerabilities that can affect the safe operation of field devices, impact the ability to remotely manage devices, and hijack the device to perform functions it was not intended to perform.

The following is suggested procurement language for bug bounty programs:

> **“Vendors should have in place a bug bounty program to openly encourage reporting of security-related bugs and vulnerabilities while allowing safe harbor to do so. This is in addition to routine security penetration testing and security code audits. The vendor should clearly indicate where the rules for its bug bounty program can be found.”**

Chapter 4. Key Considerations

This chapter discusses key considerations related to ITS cybersecurity procurement language.

4.1 Descriptive versus Prescriptive Specifications

Prescriptive specifications identify the specific make and model that should be installed. Description specifications are more generic and are intended to be met my multiple vendors potentially. On one hand, to be useful, procurement specifications must be written in such a way to make certain that vendors understands that to acquire, integrate, install, and, potentially, operate the system for the government, the vendors “shall” follow the specifications. On the other hand, to maintain appropriate flexibility for vendors, the Government should try to be descriptive rather than prescriptive. Descriptive means not specifying a make and model, except when providing an example. The only time the make should be used is to describe the network to which the vendor is integrating the devices; specifying the make may ensure successfully integrating the new devices.

4.2 Bidding Compliance

Because many ITS equipment vendors do not have all of the systems and processes in place today, agencies may elect to allow a grace period for vendors to show compliance, perhaps up to 1 year. Agencies should consider some way of publicly notifying all prospective bidders that the cybersecurity procurement additions will take place at some particular time in the future, perhaps this can occur during a presolicitation process. Retention payment can be held back (e.g., 10 percent of the payment item) with full payment made after proving compliance. Without this language, certain vendors may not be permitted or able to bid the project.

Appendix A. Applicable Standards, Policies, and Organizations

Appendix A discusses the applicable standards, policies, and organizations that are most relevant to collecting and developing cybersecurity language for ITS equipment. This list includes specific NIST, IEEE, and other documents. On one hand, to be useful, procurement specifications must be written in such a way to make certain that vendors understands that to acquire, integrate, install, and, potentially, operate the system for the government, the vendors “shall” follow the specifications. On the other hand, to maintain appropriate flexibility for vendors, the Government should try to be descriptive rather than prescriptive. Descriptive means not specifying a make and model, except when providing an example. The only time the make should be used is to describe the network to which the vendor is integrating the devices; specifying the make may ensure successfully integrating the new devices.

National Institute of Standards and Technology

The mission of NIST is to promote American innovation and industrial competitiveness. NIST’s principal focus comprises physical science laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement.(19)

NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, Federal agencies, and the broader public. Some NIST cybersecurity assignments are defined by Federal statutes, executive orders, and policies. For example, the Office of Management and Budget mandates that all Federal agencies implement NIST’s cybersecurity standards and guidance for non-national security systems.(20) NIST’s *Framework for Improving Critical Infrastructure Cybersecurity*(4) is a set of guidelines for mitigating organizational cybersecurity risks based on existing standards, guidelines, and practices. The framework provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes.

While NIST has established and maintained standards in many areas of technology over the years, it has developed the practice of cybersecurity using its 800 series and 1800 series of publications. These publications provide general and technical guidance rather than standards. The premier guidance in NIST SP 800-53, revision 5,(2) takes the form of families of controls. The controls are written in such a way that they individually and collectively call on the implementing organization to define specific parameters related to a control, such as the responsible organization or official; timing and techniques; the people, tools, and procedures needed to implement the controls; and operating the system using those controls. These documented control implementations would then be the standard for the specific organization.

The following may be taken as guidance for Federal agencies to apply in the specific area of supply chain:

- *Software Supply Chain Security Guidance Under Executive Order (EO) 14028*, Section 4e:(21)
  - This document directs NIST to publish guidance on practices for software supply chain security.
- *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*:(22)

  - This document discusses risks associated with products and services that are counterfeit, vulnerable because of poor manufacturing and development practices within the supply chain, or that may potentially contain malicious functionality. These risks are associated with an enterprise's decreased visibility into and understanding of how the technology it acquires is developed, integrated, and deployed or the processes, procedures, standards, and practices it uses to ensure security, resilience, reliability, safety, integrity, and quality of its products and services. This document provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of an organization. The document integrates C-SCRM into risk management activities by applying a multilevel C-SCRM-specific approach, including guidance on developing C-SCRM strategy implementation plans, C-SCRM policies, C-SCRM plans, and risk assessments for products and services.
- *Security Considerations in the System Development Life Cycle*:[23]
  - This guide assists agencies in building security into their IT development processes. This should result in more cost effective, risk-appropriate security control identification, development, and testing. This guide focuses on the information security components of the system development life cycle (SDLC). Overall system implementation and development is considered outside the scope of this document. Also considered outside the scope is an organization's information system governance process. The guideline describes key security roles and responsibilities needed in development of most information systems. Sufficient information about the SDLC is provided to allow a person who is unfamiliar with the SDLC process to understand the relationship between information security and the SDLC.

Institute of Electrical and Electronics Engineers

IEEE is the professional association for electronics engineers, electrical engineers, and other related disciplines. IEEE is the world's largest technical professional organization dedicated to advancing technology, and its members and audience include a global community, reached through frequently cited publications, conferences, technology standards, and professional and educational activities.[24]

IEEE has an active portfolio of 1,032 standards and more than 1,045 projects under development. The IEEE Cybersecurity Standards collection is designed to help improve the quality of exchange frameworks, cryptographic assets, data authentication, e-commerce, Internet of Things, interoperability, omnidirectional, supply chain, and surveillance worldwide.

The following IEEE cybersecurity standards could potentially apply to ITS:

- *Draft Standard for Intelligent Electronic Devices Cyber Security Capabilities*[25]
  - These standard addresses security regarding access, operation, configuration, firmware revision and data retrieval from an intelligent electronic device.
- *Recommended Practice for Cybersecurity in the Implementation of the Experience Application Programming Interface (xAPI)*[26]
  - This recommended practice describes the technical implementation of cybersecurity for xAPI and includes information an implementer would find useful related to matters in privacy and security and matters in conformance and testing.
- *Trial Use Recommended Practice for Decentralized Clinical Trials Threat Modeling, Cybersecurity, and Data Privacy*[27]
  - This recommended practice describes a set of minimum requirements and useful considerations that can be applied to threat modeling when assessing the cybersecurity and data privacy of protocol design and technology implementation for decentralized clinical trials.

- *Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems*[28]
    - This document provides guidelines for cybersecurity of distributed energy resources interconnection with electric power systems.
- *Cybersecurity Testing in Electric Power Systems*[29]
    - This document provides test guidance for cybersecurity controls used in electric power systems.
- *Function Designations used in Electrical Power Systems for Cyber Services and Cybersecurity*[30]
    - This standard applies to the definition of function designations for cyber-related services, and the cybersecurity controls and measures used to detect, identify, protect from, respond to, and recover from security threats to electric power systems.
- *Interface Between the Rail Subsystem and the Highway Subsystem at a Highway Rail Intersection*[31]
    - This standard applies to the interface between the railroad side and the highway side of a highway-rail grade crossing.

Other IEEE standards also apply to the ITS industry but not necessarily to cybersecurity specifically:

- *Common Incident Management Message Sets for use by Emergency Management Centers (EMCs)*[32]
- *Traffic Incident Management Message Sets for Use by Emergency Management Centers* (EMCs)[33]
- *Public Safety Incident Management Message Sets for Use by EMCs*[34]
- *Hazardous Material Incident Management Message Sets for Use by Emergency Management Centers (EMCs)*[35]
- *Common Traffic Incident Management Message Sets for Use in Entities External to Centers*[36]
- *IEEE 1609.0-2013, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Architecture*[37]
- *Wireless Access in Vehicular Environments (WAVE) – Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)*[38]
- *Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages*[39]
- *Wireless Access in Vehicular Environments (WAVE) – Networking Services*[40]
- *Wireless Access in Vehicular Environments (WAVE) – Multi-Channel Operation*[41]

U.S. Department of Homeland Security

DHS is the Federal executive department responsible for public security, roughly comparable to the interior or home ministries of other countries. Its stated missions involve anti-terrorism, border security, immigration and customs, cybersecurity, and disaster prevention and management.

Under the purview of DHS are some other key cybersecurity agencies:

- “CISA leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. The agency connects its stakeholders in industry and government to each other and to resources, analyses, and tools to help them fortify their cyber, communications, and physical security and resilience, which strengthens the cybersecurity posture of the Nation.

- CISA is at the center of the exchange of cyber defense information and defensive operational collaboration among the Federal Government, and State, local, Tribal and territorial (SLTT) governments, the private sector, and international partners. The agency has two primary operational functions. First, CISA is the operational lead for Federal cybersecurity, charged with protecting and defending Federal civilian executive branch networks in close partnership with the Office of Management and Budget, the Office of the National Cyber Director, and Federal agency chief information officers and chief information security officers. Second, CISA is the national coordinator for critical infrastructure security and resilience, working with partners across government and industry to protect and defend the nation's critical infrastructure.
- The Cyber Safety Review Board (CSRB), an independent public-private advisory body administered by DHS through CISA, brings together public and private sector cyber experts/leaders to review and draw lessons learned from the most significant cyber incidents. Under the leadership of the Board's Chair, DHS Under Secretary for Policy Robert Silvers, and Deputy Chair, Google VP for Security Engineering Heather Adkins, the CSRB recently published its first report on the Log4j software vulnerability. The report included 19 actionable recommendations for the public and private sectors to work together to build a more secure software ecosystem. DHS is already leading by example to implement the recommendations, through CISA guidance and Office of the Chief Information Officer initiatives to enhance open-source software security and invest in open-source software maintenance."(42)

DHS CISA does not publish standards, but guidelines. The following DHS CISA standards/guidelines are applicable to this project:

- *Cyber Security Procurement Language for Control Systems*(43)
  - This guideline includes procurement language that addresses general cybersecurity topics that are not specific to any industry, with explanation and testing concepts. It also includes references to standards and other guidelines. It is a general document, addressing procurement language across industry sectors, including transportation.
- *Transportation Systems Sector-Specific Plan*(44) and *Cybersecurity Framework Implementation Guide*(45)
  - The transportation systems sector includes aviation, maritime, mass transit, passenger rail, freight, pipelines, postal, and shipping. Appropriate to this discussion is the highway and motor carrier subsector, which encompasses more than 600,000 bridges, 350 tunnels, and 4 million miles of roadway. Vehicles include trucks, such as those carrying hazardous materials; other commercial vehicles, such as commercial motorcoaches and school buses; vehicle and driver licensing systems; traffic management systems; and cyber systems used for operational management.

U.S. Department of Energy

"The mission of the Energy Department is to ensure America's security and prosperity by addressing its energy, environmental and nuclear challenges through transformative science and technology solutions."(46)

"The DOE Cybersecurity Program is a shared, distributed enterprise risk management approach to protect DOE information systems to comply with the Federal Information Security Modernization Act of 2014 (FISMA) and in alignment with the National Institute of Standards and Technology (NIST) *Risk Management Framework* of NIST Special Publication 800-37 and NIST *Framework for Improving Critical Infrastructure Cybersecurity*."(47)

For energy systems and procurement language specifically, DOE is more prescriptive but still provides guidelines, such as the following:

- *Cybersecurity Procurement Language for Energy Delivery Systems*(48)—Similar to the DHS CISA document, this is not a standard, but a guideline. It includes procurement language that is general enough to be considered for ITS. There is less explanation in each section, but a good how-to-apply guide up front.
- *Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities*(49)—This document is too general to be of specific use; it references both the DOE and the DHS CISA documents.
- Cybersecurity Considerations for Procurement Process(50)—This flowchart is a process, not a standard, but is useful for considering cybersecurity in the procurement process.

Open Worldwide Application Security Project

OWASP works to improve the security of software through its community-led, open-source software projects, worldwide chapters, tens of thousands of members, and global conferences. OWASP is a nonprofit foundation that works to improve the security of software.(51)

OWASP publishes research entitled "OWASP Top 10 Web Application Security Risks," along with the reasons for a change in position. The latest version, published in 2021, is quoted below:

- "**A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
- **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
- **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
- **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.
- **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
- **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.
- **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.

- **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.
- **A09:2021-Security Logging and Monitoring Failures** was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.
- **A10:2021-Server-Side Request Forgery** is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time."[52]

Each web application security risk is a hyperlink to a web page that provides an overview, factors, descriptions, prevention comments, example attack scenarios, references, and a list of mapped common weakness enumerations. The common weakness enumerations provide information about each weakness, common vulnerabilities and exposures (CVE), detection methods, and potential mitigations.

Vulnerability testing is a basic cybersecurity requirement for any operational network. Tools draw on cybersecurity intelligence—such as the abovementioned CVEs—and scan active devices on the target network addresses to determine if vulnerabilities addressed in the CVEs are present (i.e., the proper patches have not been applied). Thus, the CVEs are likely to be included in those scans. For the purposes of this report, any ITS component web applications under consideration should be tested for vulnerability against the OWASP Top Ten, with a report on the results made available for deciding among alternatives (see applicable language in chapter 4).

References

1. Cybersecurity & Infrastructure Security Agency. “Critical Infrastructure Sectors.” https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

2. Intelligent Transportation Systems Joint Program Office (ITS-JPO). “ITS Cybersecurity Research Program.” USDOT. https://www.its.dot.gov/research_areas/cybersecurity/.

3. *Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Cybersecurity & Infrastructure Security Agency. May 11, 2017. https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure.

4. National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*. U.S. Department of Commerce. April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

5. ITS-JPO. *Cybersecurity for ITS*. USDOT. https://www.its.dot.gov/factsheets/pdf/PR_CyberSecurity_Factsheet.pdf.

6. ITS-JPO. *Cybersecurity and Intelligent Transportation Systems: Best Practice Guide*. FHWA-JPO-19-763. USDOT. September 17, 2019. https://rosap.ntl.bts.gov/view/dot/42461.

7. Vehicle Safety Communications 5 (VSC5) Consortium. Security Credential Management System (SCMS) Proof of Concept (POC) Implementation (project). https://www.campllc.org/security-credential-management-system-scms-proof-of-concept-poc-implementation/.

8. ITS-JPO. *Transportation Cybersecurity Incident Response and Management Framework: Final Report*. FHWA-JPO-21-851. USDOT. July 2021. https://rosap.ntl.bts.gov/view/dot/57007.

9. ITS Professional Capacity Building Program. “ITS Training and Resource Hub.” USDOT. https://www.pcb.its.dot.gov/ITSCourses/Default.aspx#training.

10. NIST. *Security and Privacy Controls for Information Systems and Organizations*. NIST SP 800-53. Rev. 5. U.S. Department of Commerce. September 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

11. National Defense Authorization Act for Fiscal Year 2023. Pub. L. No. 117-263. 117th Congress. 2021–2022.

12. ITS-JPO. *How the U.S. Department of Transportation is Protecting the Connected Transportation System from Cyber Threats*. FHWA JPO-11-021. USDOT. https://www.its.dot.gov/factsheets/pdf/cybersecurity_factsheet.pdf.

13. ITS Cybersecurity Specs and Apps. Technical Memorandum: Literature Review and Stakeholder Input Summary—Task Order 693JJ322F00374N. February 15, 2023.

14. ITS-JPO. "ITS Standards Program." USDOT. https://www.standards.its.dot.gov/.

15. NIST. National Vulnerability Database. U.S. Department of Commerce. http://nvd.nist.gov.

16. Open Worldwide Application Security Project (OWSAP®). "OWASP Application Security Verification Standard." https://owasp.org/www-project-application-security-verification-standard/.

17. IT Governance. "Data Breach Notification Laws by State." https://www.itgovernanceusa.com/data-breach-notification-laws.

18. NIST. *Digital Identity Guidelines*. SP 800-63. U.S. Department of Commerce. June 2017.

19. U.S. Department of Commerce. "National Institute of Standards and Technology." https://www.commerce.gov/bureaus-and-offices/nist.

20. NIST. "Cybersecurity." U.S. Department of Commerce. https://www.nist.gov/cybersecurity.

21. *Software Supply Chain Security Guidance Under Executive Order (EO) 14028*. Section 4e. February 4, 2022. https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf.

22. NIST. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. NIST Special Publication. NIST SP 800-161r1. U.S. Department of Commerce. May 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf.

23. NIST. *Security Considerations in the System Development Life Cycle*. U.S. Department of Commerce. October 16, 2008. https://www.nist.gov/publications/security-considerations-system-development-life-cycle.

24. Institute of Electrical and Electronics Engineers (IEEE). https://www.ieee.org/.

25. IEEE. *Draft Standard for Intelligent Electronic Devices Cyber Security Capabilities.* IEEE Standard P1686/D15. July 2013.

26. IEEE. *Recommended Practice for Cybersecurity in the Implementation of the Experience Application Programming Interface*. IEEE Standard P9274.4.2. November 2019.

27. IEEE. *Trial Use Recommended Practice for Decentralized Clinical Trials Threat Modeling, Cybersecurity, and Data Privacy*. IEEE Standard P2968.2. February 2021.

28. IEEE. *Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems*. IEEE Standard P15473. June 2023.

29. IEEE. *Cybersecurity Testing in Electric Power Systems*. IEEE Standard P2658. November 2022.

30. IEEE. *Function Designations used in Electrical Power Systems for Cyber Services and Cybersecurity*. IEEE Standard P2808. March 2019.

31. IEEE. *Interface Between the Rail Subsystem and the Highway Subsystem at a Highway Rail Intersection*. IEEE Standard 1570-2002. October 2002.

32. IEEE. *Common Incident Management Message Sets for Use by Emergency Management Centers*. IEEE Standard 1512-2006. Revised August 2006. https://www.standards.its.dot.gov/Standard/368.

33. IEEE. *Common Incident Management Message Sets for Use by Emergency Management Centers*. IEEE Standard 1512.1-2006. Revised January 2006. https://www.standards.its.dot.gov/Standard/375.

34. IEEE. *Public Safety Incident Management Message Sets for Use by EMCs*. IEEE Standard P1512.2-2004. Superseded.

35. IEEE. *Hazardous Material Incident Management Message Sets for Use by Emergency Management Centers (EMCs)*. IEEE Standard 1512.3-2006. Revised July 2006. https://www.standards.its.dot.gov/Standard/391.

36. IEEE. *Common Traffic Incident Management Message Sets for Use in Entities External to Centers*. IEEE Standard P1512.4. January 2006.

37. IEEE. *Wireless Access in Vehicular Environments (WAVE) – Architecture.* IEEE Standard 1609.0-2013. March 2014. https://www.standards.its.dot.gov/Standard/518.

38. IEEE. *Wireless Access in Vehicular Environments (WAVE)—Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS).* IEEE Standard 1609.11-2010. January 2009.

39. IEEE. *Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*. IEEE Standard 1609.2-2016. March 2016. https://www.standards.its.dot.gov/Standard/405.

40. IEEE. *Wireless Access in Vehicular Environments (WAVE) – Networking Services*. IEEE Standard 1609.3-2020. March 2021. https://www.standards.its.dot.gov/Standard/406.

41. IEEE. *Wireless Access in Vehicular Environments (WAVE) – Multi-Channel Operation*. IEEE Standard 1609.4-2016. March 2016.

42. U.S. Department of Homeland Security. “Mission.” https://www.dhs.gov/mission.

43. U.S. Department of Homeland Security. *Cyber Security Procurement Language for Control Systems*. September 2009. https://www.cisa.gov/sites/default/files/2023-01/Procurement_Language_Rev4_100809_S508C.pdf.

44. U.S. Department of Homeland Security. *Transportation Systems Sector-Specific Plan 2015*. Revised December 2017. https://www.cisa.gov/publication/nipp-ssp-transportation-systems-2015.

45. U.S. Department of Homeland Security. *Cybersecurity Framework Implementation Guide.* December 2020. https://www.cisa.gov/publication/tss-cybersecurity-framework-implementation-guide.

46. U.S. Department of Energy. “About Us.” https://www.energy.gov/about-us.

47. U.S. Department of Energy. *Department of Energy Cyber Security Program*. Directive DOE O 205.1C. Approved May 15, 2019; Chg 1 (LtdChg), February 3, 2022. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf.

48. Energy Sector Control Systems Working Group. *Cybersecurity Procurement Language for Energy Delivery Systems*. April 2014. https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf.

49. Pacific Northwest National Laboratory. *Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities*. PNNL- 28661. May 2019. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-28661.pdf.

50. Pacific Northwest National Laboratory. *Cybersecurity Considerations for Procurement Process*. https://www.energy.gov/sites/default/files/2020/07/f76/cyber-procurement-decision-tree.pdf.

51. OWSAP®. “About the OWASP Foundation.” https://owasp.org/about/.

52. OWSAP®. “OWASP Top Ten.” https://owasp.org/www-project-top-ten/.

US Department of Transportation
ITS Joint Program Office – HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free "Help Line" 866-367-7487

www.its.dot.gov

FHWA-JPO-23-11

U.S. Department of Transportation