

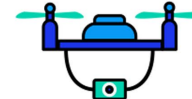
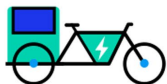


Welcome FY22 SMART Grantees

July 10th, 2024



U.S. Department of Transportation



Why is Cybersecurity Important?

Ed Fok

Federal Highway Administration

July 2024



U.S. Department of Transportation
Federal Highway Administration



Disclaimer

Except for any statutes or regulations cited, the contents of this presentation do not have the force and effect of law and are not meant to bind the public in any way. This presentation is intended only to provide information regarding existing requirements under the law or agency policies.



Operational Benefits from Technology Deployment

- Improve health monitoring of infrastructure
- Improve operational efficiency
 - Improved mobility information
 - Quicker control ability
 - Better automation
- Improve user experiences
 - Transit arrival time
 - Travel time estimates



Risks from Technology Deployment

- Shorter device and system life cycle
- Increased exposure to maintenance challenges
- Cybersecurity vulnerability



History of Attacks and Vulnerabilities

Back in the 20 th Century...	<ul style="list-style-type: none">• Homemade signal preemption kit• Hijacked Ethernet switches on broadband cable modem
Early 2000's	<ul style="list-style-type: none">• West Coast Toll tag vulnerability discovered• Portable Dynamic Message Signs hack instruction online
2010's	<ul style="list-style-type: none">• Digital parking meters vulnerabilities discovered• Transit payment system and transit vehicles vulnerabilities discovered• Public safety radio spectrum (4.9GHz) vulnerabilities discovered• Center to field network attacked• Sensors and controllers attacked, and vulnerabilities discovered• Ransomware attacks on agency enterprise systems
Early 2020's	<ul style="list-style-type: none">• Monitoring interrupted on State highway due to ransomware attack



Why is this my problem?

- **Information Technology** – IT or Technology Department
 - Email systems
 - General Internet services
- **Operation Technology** – Transportation agency's responsibility
 - Traffic signal control
 - Optimization and management software
 - Advance traveler information systems



Cybersecurity vs. Cyber Resilience

Cyber Resilience	The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources
Cybersecurity	<p>The process of protecting information by preventing, detecting, and responding to attacks. Prevention of damage to, protection of, and restoration of</p> <ul style="list-style-type: none">• computers,• electronic communications systems and services,• wire and electronic communication,• including information contained therein, to ensure its confidentiality, availability, integrity, authentication, and nonrepudiation.

NIST Special Publication 800-160, Volume 2, Revision 1, “Developing Cyber-Resilient Systems: A Systems Security Engineering Approach”



Classification and Motivations

- **Use the right name**
 - Don't call them "hackers"
 - Cyber Threat Actors present a threat
 - Security Researchers discover vulnerabilities
- **Motivations Vary**
 - Curiosity, bragging rights
 - Greed
 - Political causes
 - Warfare

All cyber attacks follow a similar cycle:



U.S. Department of Transportation
Federal Highway Administration



Scanning and Breaching the Perimeter



Mapping the Interior



Exploitation and Egress



What Must Be Protected?

- What is your agency's mission?
- Common mission:
 - Safe operation
 - Efficient mobility
 - Trusted information

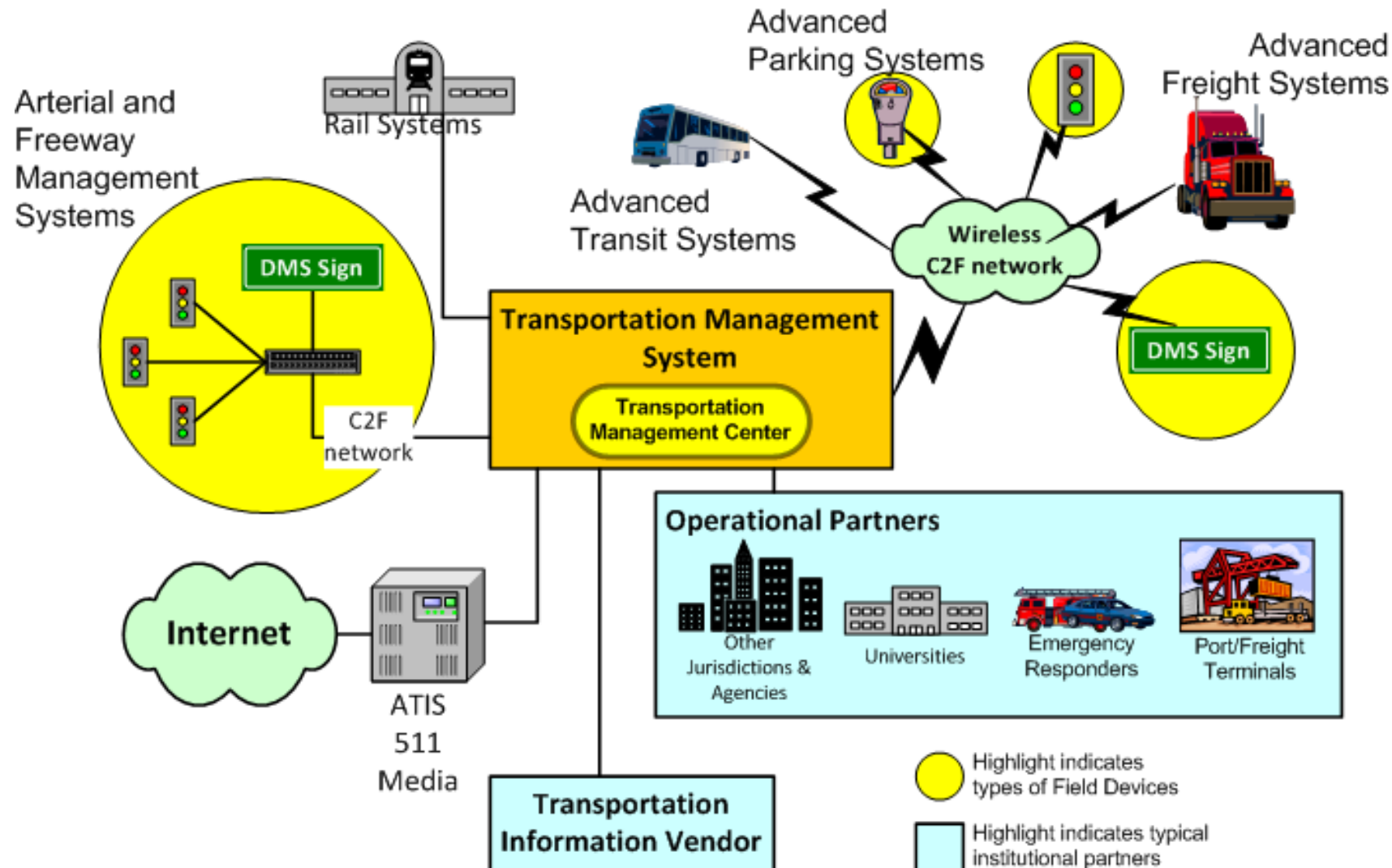


Surmountable Challenge

- Focus on delivering agency objectives
- Apply known defense concept to
 - Disrupt the “kill chain”
 - Minimize exposure of agency objectives
- Identify a sustainable level of engagement



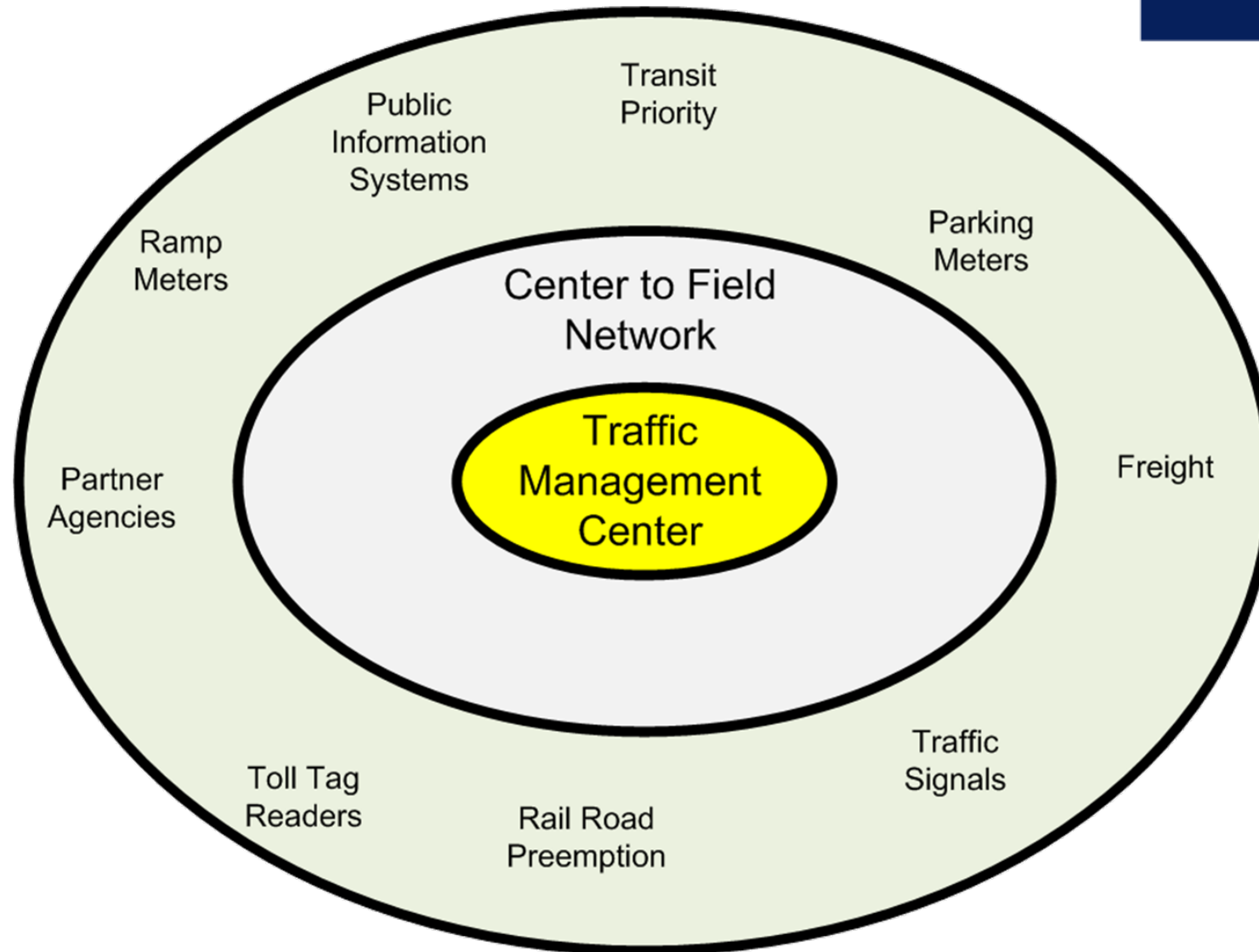
So where are we vulnerable?



Source: USDOT



So where are we vulnerable?



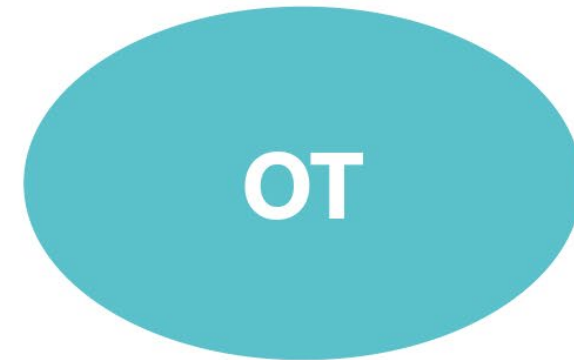
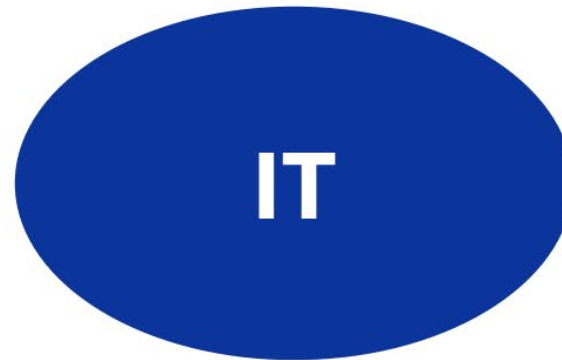
Source: USDOT



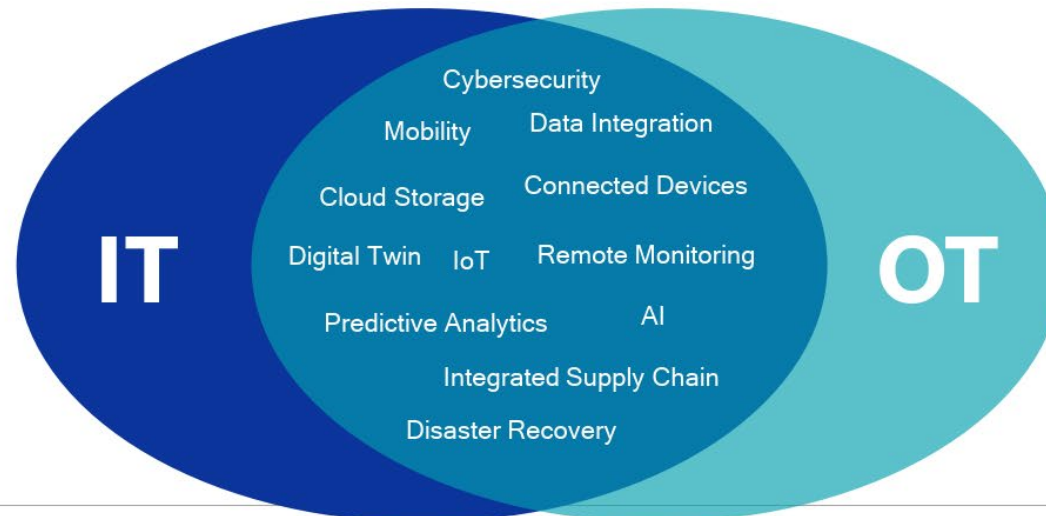
U.S. Department of Transportation
Federal Highway Administration

Information Technology (IT) vs. Operational Technology (OT)

**The
Past**



**The
Future**



(Source: M. Rao, Virginia Department of Transportation. National Operations Center of Excellence (NoCoE) Webinar Series, October 6, 2020, [webinar-series-part-2-how-leverage-it-resources-improve-tsmo](#))

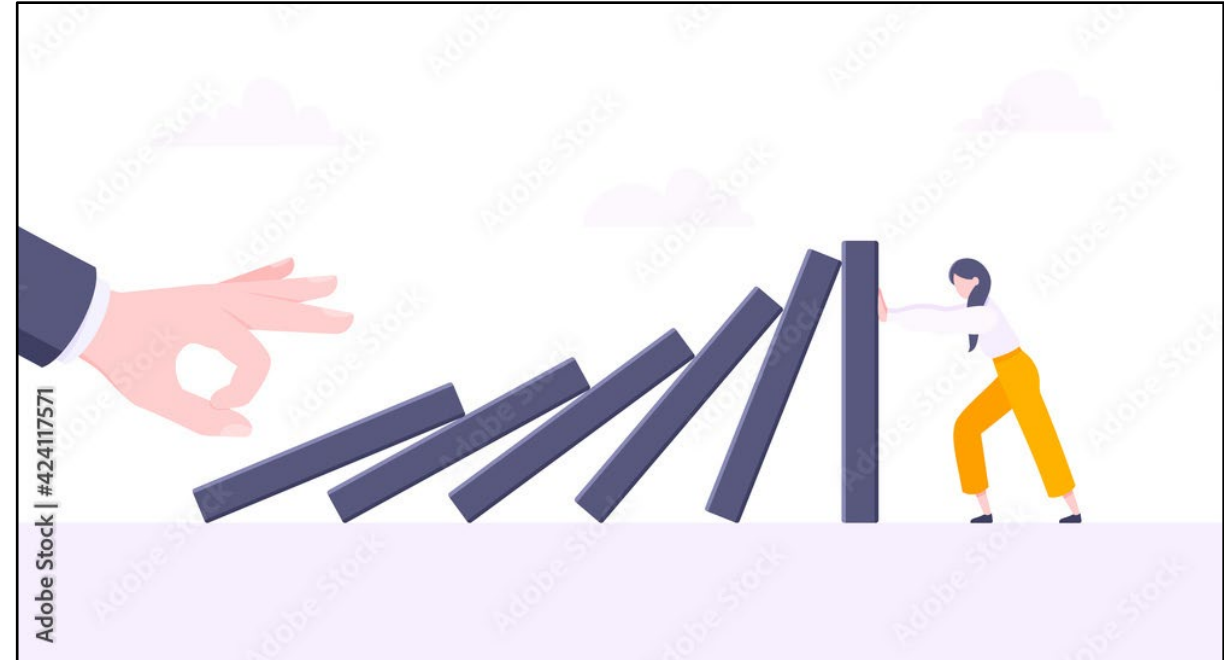
HPA Approved
6/10/2024

Balancing Security and Resilience



U.S. Department of Transportation
Federal Highway Administration

- **Resilience**
 - The capacity to recover quickly from a fault and maintain service
 - Transportation agencies are very good at resilience
- **Security** – freedom from danger





Principles of Protection

- Cyber Security Framework offers a structured approach
- Developed by National Institute of Standards and Technology

The Core Functions of the Framework:

- Identify
- Protect
- Detect
- Respond
- Recover



Context of an Attack

- Not all attacks are battle worthy
- Not all nuisance attacks can be ignored





Staff is the line between disaster and hero

- **Example San Francisco Metropolitan Transit Authority (2016)**
 - Turn a ransomware attack into “Black Friday Miracle”
 - Search Term: “San Francisco MTA ransomware 2016”
- **Example Hawaii Emergency Operation Center (2017)**
 - Turn a press opportunity into a password breach incident.
 - Search Term: “Hawaii EOC password photo”

All Protection can be Circumvented by Staff



U.S. Department of Transportation
Federal Highway Administration

- **Unintended Risks**
 - Poor security habits
 - Vulnerability from balancing customer service and security
- **Insider Risk**
 - Human Resources and organizational policies will be critical for insider attack





Teams should be functionally cross-cutting

- **Cross-Cutting Technical Team**
 - Operational technology team
 - Information technology team
- **Internal and external communication team**
 - Keep manager informed and ready to make decisions when required
 - Allow the technical team to stay focused on technical restoration
 - Keep stakeholder and public informed and coordinated
- **Management and Human Resources**
 - Sustainable staff training and management



Presidential Executive Orders

- **Executive Order 13636** (EO 13636) Improving Critical Infrastructure Cybersecurity
- **Executive Order 13800** (EO 13800) Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- **Presidential Policy Directive 21** (PPD-21) Critical Infrastructure Security and Resilience
- **Presidential Policy Director 41** (PPD-41) U.S. Cyber Incident Coordination

Federal Regulations US Department of Transportation vs. Department of Homeland Security



U.S. Department of Transportation
Federal Highway Administration

- **USDOT does not have regulations** on transportation cybersecurity at State, Local, Tribal, and Territorial (SLTT) agencies
- Any **Federal Regulation will come from Department of Homeland Security**
 - Transportation Security Agency (TSA)
 - Cybersecurity and Infrastructure Security Agency (CISA)



State Laws on incident disclosure

- Each State can have its own regulation around cybersecurity
 - Privacy
 - Incident or breach disclosure
 - Consider impacts from local regulations



Possible Next Steps for your Organization

- **Short Term**
 - Identify what's important and the regulatory landscape
- **Medium Term**
 - Develop physical and human assets needs
 - Create the security process based on established model such as National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- **Long Term**
 - Keep security process current as threat changes
 - Maintain workforce competency

NHI 137055 Transportation Cyber Security Online Course



U.S. Department of Transportation
Federal Highway Administration

- Web based training on fundamentals of transportation cybersecurity
- Designed for transportation professionals new to cybersecurity
- Available from NHI's new Blackboard LMS site accessible from their old site.

Cybersecurity Wargames for Small ITS Teams



U.S. Department of Transportation
Federal Highway Administration

- Design as an independent training tool for very small agencies and groups
- Target audience are transportation professionals new to cybersecurity
- Game can be played by an individual, but best with a small group of 2 to 3.

Document reference: FHWA-JPO-24-137

HPA Approved
6/10/2024

ITS Profile for NIST Cybersecurity Framework



U.S. Department of Transportation
Federal Highway Administration

ITS specific profiles to for NIST's Cybersecurity Framework

- ITS Cybersecurity Framework Profile
- ITS Security Control Set For Traffic Signal Controllers
- ITS Security Control Set Template and Instructions
- Operating Procedures for Developing Security Control Sets for ITS

Document reference: FHWA-JPO-23-120 to FHWA-JPO-23-123

HPA Approved
6/10/2024

Intelligent Transportation Systems Penetration Testing Guide



U.S. Department of Transportation
Federal Highway Administration

- Methodology of scoping a test: type, management, and test readiness
- Template test plan for your own penetration testing
- “Cybersecurity and Intelligent Transportation Systems – A Best Practice Guide” (source: ROSA-P)

Cybersecurity and Intelligent Transportation Systems

A Best Practice Guide

www.its.dot.gov/index.htm

Best Practice Guide – September 17, 2019
Publication Number: FHWA-JPO-19-763



U.S. Department of Transportation

Source: USDOT

HPA Approved
6/10/2024

Cybersecurity Language for the Procurement of ITS Equipment



U.S. Department of Transportation
Federal Highway Administration

- Design to help agency add cybersecurity requirements to their existing procurement contract
- Intended to serve as a starting point to be customized per applicable regulations and policies

Document reference: FHWA-JPO-23-118



Updated National ITS Architecture

ARC-IT Version 9.0

The National ITS Reference Architecture

Architecture ▼ Architecture Use ▼ Architecture Resources ▼ Architecture Terminology ▼ Contact The Architecture Team

ENHANCED E

[Home](#) > [Security](#) > Device Classes

Device Classes

A device class, or more precisely, a device security class, is a statement of the security requirements for a device in terms of its requirements for Confidentiality, Integrity, and Availability, expressed as LOW, MODERATE or HIGH ratings for each of the three. Within the ITS Architecture, devices are the building blocks for physical objects. So if the devices that implement a physical object collectively meet a given device class, that physical object does as well.

Device security classes are intended to be of use to suppliers of devices and systems for use in C-ITS deployments. A device can only be used to play a role in a particular application if it meets the security requirements of that role; however, higher security requirements will in general translate to more expensive devices. The concept behind the device security class is to develop collections of security requirements which suppliers can develop to, allowing them to provide the most cost-effective solutions that meet the security requirements.

Since there are three security levels, there are potentially 27 (3³) different device security classes. In principle, suppliers could develop devices in each of these classes. In practice, there will likely be economies of scale in reducing the number of classes. As such, various analyses have led to the establishment of five device classes:

a. Every physical object is covered by a device class that matches or exceeds its security requirements

b. Every physical object is covered by a device class that exceeds its security requirements under no more than two headings

The first property ensures that physical objects meet the security requirements; the second ensures that implementations are not significantly more expensive than necessary, relative to security requirements. Device security classes are intended to be of use to suppliers of devices and systems for use in C-ITS deployments. A device can only be used to play a role in a particular application if it meets the security requirements of that role; however, higher security requirements will in general translate to more expensive devices. The concept behind the device security class is to develop collections of security requirements which suppliers can develop to, allowing them to provide the most cost-effective solutions that meet the security requirements.

There are currently five physical object device security classes defined:

Class	Confidentiality	Integrity	Availability
Class 1	LOW	MODERATE	MODERATE
Class 2	MODERATE	MODERATE	MODERATE
Class 3	MODERATE	HIGH	MODERATE
Class 4	HIGH	HIGH	MODERATE
Class 5	HIGH	HIGH	HIGH

These device security classes were derived by [analyzing](#) the requirements associated with application-constrained information flows, and then combining those flows at physical object boundaries to determine matching device requirements. While this resulted in roughly one dozen device classes, a more moderate number is desirable to realize economies of scale. While additional classes may be added in the future, these five provide a baseline.

A more detailed analysis was conducted on the V2I environment that led to selection of specific security controls that should be applied to Connected Vehicle Roadside Equipment (CVRSE), ITS Roadway Equipment (ITSRE), and Vehicle OBEs. These controls can be seen from the following:

[Class 1](#) controls for CVRSE, ITSRE, Vehicle OBE

[Class 2](#) controls for CVRSE, ITSRE, Vehicle OBE

[Class 3](#) controls for CVRSE, ITSRE, Vehicle OBE

[Class 4](#) controls for CVRSE, ITSRE, Vehicle OBE

Control documentation is largely sourced from NIST 800-53r4 (revision 5 was not available at the time of the analysis), with the notable exception of privacy-focused content which is based on ISO 15408-2. For the NIST-sourced material, the control definition and supplemental guidance are largely consistent with the NIST source (i.e., limited customization relevant to the V2I environment); all of the content in the Approved Mechanisms and Protocol Implementation Conformance Statements (PICS) sections were created as a result of the analysis and specifically for the V2I environment. For the ISO-

ARC-IT Version 9.0

The National ITS Reference Architecture

Architecture ▼ Architecture Use ▼ Architecture Resources ▼ Architecture Terminology ▼ Contact The Architecture Team

ENHANCED E

[Home](#) > [Security](#) > Device Class 1 Controls

Device Class 1 Controls

Device Class 1 Security Requirements:

- Confidentiality: LOW
- Integrity: MODERATE
- Availability: MODERATE

Devices of class 1 must meet controls from NIST 800-53 and ISO/IEC 15408 in the following areas:

- [Access Control](#)
 - [AC-3 Access Enforcement](#) (Class 1)
 - [AC-4 Information Flow Enforcement](#) (Class 1)
 - [AC-6 Least Privilege](#) (Class 1)
 - [AC-7 Unsuccessful Authentication Attempts](#) (Class 1)
 - [AC-8 System Use Notification](#) (Class 1)
 - [AC-11 Session Lock](#) (Class 1)
 - [AC-12 Session Termination](#) (Class 1)
 - [AC-17 Remote Access](#) (Class 1)
 - [AC-18 Wireless Access](#) (Class 1)
- [Audit and Accountability](#)
 - [AU-2 Audit Events](#) (Class 1)
 - [AU-3 Content Of Audit Records](#) (Class 1)
 - [AU-4 Audit Storage Capacity](#) (Class 1)
 - [AU-5 Response To Audit Processing Failures](#) (Class 1)
 - [AU-7 Audit Reduction And Report Generation](#) (Class 1)
 - [AU-8 Time Stamps](#) (Class 1)
 - [AU-9 Protection Of Audit Information](#) (Class 1)
 - [AU-12 Audit Generation](#) (Class 1)
- [Configuration Management](#)
 - [CM-7 Least Functionality](#) (Class 1)
 - [CM-11 User-Installed Software](#) (Class 1)
- [Contingency Planning](#)
 - [CP-12 Safe Mode](#) (Class 1)
- [Identification and Authentication](#)
 - [IA-2 Identification And Authentication \(Organizational Users\)](#) (Class 1)
 - [IA-5 Authenticator Management](#) (Class 1)
 - [IA-6 Authenticator Feedback](#) (Class 1)
 - [IA-7 Cryptographic Module Authentication](#) (Class 1)
 - [IA-11 Re-authentication](#) (Class 1)
- [Incident Response](#)
 - [IR-5 Incident Monitoring](#) (Class 1)
 - [IR-6 Incident Reporting](#) (Class 1)
- [Media Protection](#)
 - [MP-6 Media Sanitization](#) (Class 1)
- [Privacy](#)
 - [ISO FPR PSE 1 Pseudonymity](#) (Class 1)
 - [ISO FPR PSE 2 Reversible Pseudonymity](#) (Class 1)
 - [ISO FPR UNL 1 Unlinkability](#) (Class 1)
- [Risk Assessment](#)
 - [RA-5 Vulnerability Scanning](#) (Class 1)
- [System and Communications Protection](#)

Source: USDOT

Updated National Transportation Communications for ITS Protocol (NTCIP) Standards



U.S. Department of Transportation
Federal Highway Administration

A Working Group Draft of the NTCIP BSP2 WG

NTCIP 9014 v01.01

National Transportation Communications for ITS Protocol Infrastructure Standards Security Assessment

Draft v01.01 July 21, 2020

This is a draft document, which is distributed for review, vote/acceptance, and comment purposes only. You may reproduce and distribute this document within your organization, but only for the purposes of and only to the extent necessary to facilitate review, vote/acceptance, and comment. Please ensure that all copies include this notice. This document contains preliminary information that is subject to change.

Published by

American Association of State Highway and Transportation Officials (AASHTO)
444 North Capitol Street, N.W., Suite 249
Washington, D.C. 20001

Institute of Transportation Engineers (ITE)
1627 Eye Street, N.W., Suite 600
Washington, D.C. 20006

National Electrical Manufacturers Association (NEMA)
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209-3801

- Provides direction to other NTCIP Standards working group
- Focuses on
 - Simple Network Management Protocol (SNMP)
 - Replace SNMPv1 protocol with SNMPv3+ protocol
 - Mitigate SNMPv1 use cases that have technical barrier to upgrades
- Balances between Interoperability and security

Source: USDOT

HPA Approved
6/10/2024

Improve Cybersecurity Communication

- Identify and address existing gaps in vulnerability and exploit information sharing
- A framework for communication and information sharing for vulnerabilities and incident response
- Develop of glossary of common terms
- “Transportation Cybersecurity Incident Response and Management Framework” (available from ROSA-P)



U.S. Department of Transportation
Federal Highway Administration

Transportation Cybersecurity Incident Response and Management Framework

Cybersecurity Incident Exercise
Summary Report

May 2021



U.S. Department of Transportation
Federal Highway Administration

Transportation Cybersecurity Incident Response and Management Framework

Final Report

July 2021



U.S. Department of Transportation
Federal Highway Administration

Source: USDOT

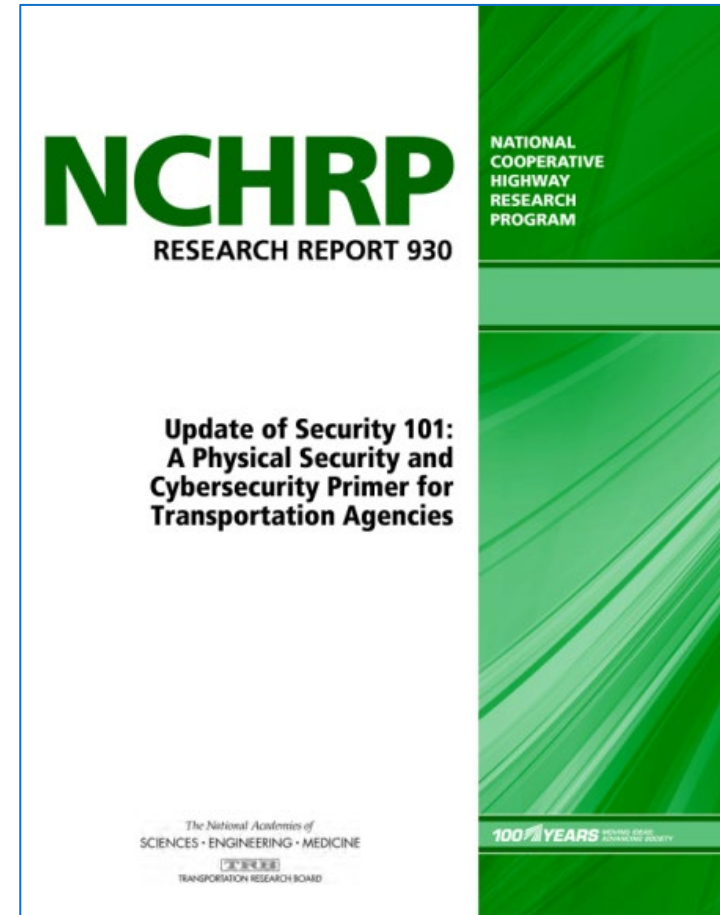
HPA Approved
6/10/2024

NCHRP Cybersecurity Projects



U.S. Department of Transportation
Federal Highway Administration

- TRB Snap Search - Cyber
- Cybersecurity of Traffic Management Systems (NCHRP 3-127)
- Security 101: A Physical Security and Cybersecurity Primer for Transportation Agencies (NCHRP Research Report 930)
- Guidelines for State Transportation Agency Chief Executive Officers on Cybersecurity Issues and Protection Strategies (NCHRP 23-03, In Development)



Source: TRB

HPA Approved
6/10/2024



Additional Resources

- MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) searchable terms
- Transportation Management Center Information Technology Security (available from ROSA-P)
- ITS Joint Program Office Professional Capacity Building Program for additional training

ATT&CK® for Industrial Control Systems

ATT&CK for ICS is a knowledge base useful for describing the actions an adversary may take while operating within an ICS network. The knowledge base can be used to better characterize and describe post-compromise adversary behavior. Please see the [overview page](#) for more information about ATT&CK for ICS.

You may start with the following links to become more familiar with ATT&CK for ICS:

- [ATT&CK for ICS - Philosophy Paper](#)
- [Full list of ATT&CK for ICS techniques](#)
- [Software used by ICS threats](#)
- [Adversary groups from ICS related incidents](#)
- [Assets present in ICS](#)
- [Contribute or contact us](#)

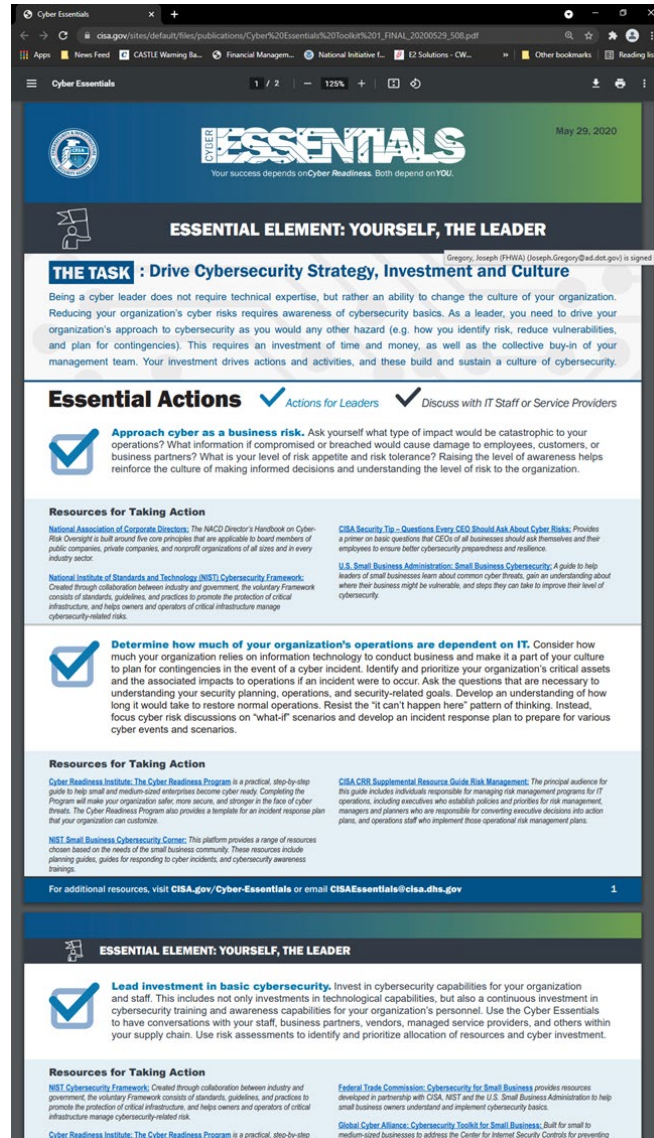
The MITRE ATT&CK for ICS Matrix is an overview of the tactics and techniques described in the ATT&CK for ICS knowledge base. It visually aligns individual techniques under the tactics in which they can be applied. Some techniques span more than one tactic because they can be used for different purposes.

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control

Source: MITRE



Additional Resources (continued)



- Follow Cybersecurity & Infrastructure Security Agency (CISA)
- Monitor and issues cybersecurity threat and vulnerability warning
- Search term “Industrial Control Systems (ICS) cybersecurity training ICS-CERT” for training
- Source: CISA

ITS JPO Cybersecurity Research Program



U.S. Department of Transportation
Federal Highway Administration

Intelligent Transportation Systems Joint Program Office (ITS JPO)

ITS CYBERSECURITY RESEARCH PROGRAM

Home About ITS Cybersecurity ITS Cybersecurity Implementation Tools and Resources ITS Cybersecurity Research ITS Cybersecurity Workforce Development **Cyber Incident Reporting**

ITS CYBERSECURITY RESEARCH PROGRAM

Cybersecurity is a serious and ongoing challenge for the transportation sector. Cyber threats to transportation systems can impact national security, public safety, and the national economy. The ITS Cybersecurity Research Program was developed in response to the urgent need to protect Intelligent Transportation Systems (ITS) from cyber-attacks.



About ITS Cybersecurity



ITS Cybersecurity Implementation



Tools and Resources



ITS Cybersecurity Research



ITS Cybersecurity Workforce Development



Cyber Incident Reporting

 This site describes the ITS Cybersecurity Research Program. If you are experiencing a cybersecurity attack, click [Report a Cyber Incident](#) to view a list of resources.

Contact

Contact the ITS Cybersecurity Research Program with your questions or for more information: ITS_CybersecurityResearch@usdot.onmicrosoft.com

Links

Cybersecurity Across USDOT **Report a Cyber Incident**

HPA Approved
6/10/2024

Questions?

Ed Fok

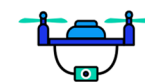
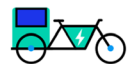
FHWA Operations Technical Services Team

edward.fok@dot.gov



U.S. Department of Transportation
Federal Highway Administration

BREAK



Workforce Impact Planning

Ross Templeton

Labor Policy Advisor, US DOT



Bipartisan Infrastructure Law

- Product of partnership between branches of government, political parties, and labor and business.
- Historic investments matched with historic labor standards.
- Focus on workforce throughout implementation.



US DOT Innovation Principles

- **Support workers** – The Department will empower workers and expand access to skills, training, and the choice of a union. They will have a seat at the table in shaping innovation.
- **Provide opportunities to collaborate** – The Department will embrace public private partnerships that share risk, foster purpose-driven innovation and protect the interests of the public, workers, and communities. The Department must encourage an outcomes-based approach that is technology neutral.



US DOL Good Jobs Principles

- **Empowerment and Representation** – Workers can form and join unions. Workers can engage in protected, concerted activity without fear of retaliation. Workers contribute to decisions about their work, how it is performed, and organizational direction.
- **Skills and Career Advancement** – Workers have equitable opportunities and tools to progress to future good jobs within their organizations or outside them. Workers have transparent promotion or advancement opportunities. Workers have access to quality employer- or labor-management-provided training and education.



Example - Rivet Gangs

- Four-person crews
- Highly skilled, specialized work
- Hard to replace workers



Tension Bolts

- Righty-tighty, lefty-loosey
- Cheaper and better – quickly replaced rivet gangs
- Workforce adapted by focusing on safety



Union Partners

- Transportation sector – e.g., TTD, Teamsters
- Construction – e.g., NABTU, Carpenters
- Utilities and operations – e.g., IBEW, AFSCME



Workforce Tools

- Registered Apprenticeships – Upskill the workforce
- Project Labor Agreements (PLAs) – Deliver jobs on time
- Neutrality Agreements – Free and fair chance to join a union



Communication and Partnership

- Open and early dialogue with labor partners is the best way to start assessing workforce impacts.
- Consider and engage all types of workers affected by the project.
- DoT is here to help. We can facilitate conversations and provide expertise.



Let's get to work

- Ross Templeton, Labor Policy Advisor
- ross.templeton@dot.gov
- 771-223-2117

- www.transportation.gov/priorities/transformation/us-dot-innovation-principles
- www.dol.gov/general/good-jobs/principles





SMART Grants

**Contractor or Subrecipient Determinations
& Procurement Under Grants**





Agenda

- Contractor or Subrecipient Determination
- Procurement Under Grants
- Top Procurement Mistakes
- Questions and Discussion



Contractor or Subrecipient Determination

Key Definitions



2 CFR §200.1

Contract	A legal instrument by which a recipient or subrecipient conducts procurement transactions under a Federal award.
Contractor	An entity that receives a contract.
Pass-Through Entity	A recipient or subrecipient that provides a subaward to a subrecipient (including lower tier subrecipients) to carry out part of a Federal program. The authority of the pass-through entity flows through the subaward agreement between the pass-through entity and subrecipient.
Recipient	An entity that receives a Federal award directly from a Federal agency to carry out an activity under a Federal program. Does not include subrecipients or individuals that are participants or beneficiaries of the award.
Subrecipient	An entity that receives a subaward from a pass-through entity to carry out part of a Federal award. The term subrecipient does not include a beneficiary or participant. A subrecipient may also be a recipient of other Federal awards directly from a Federal agency.
Subaward	An award provided by a pass-through entity to a subrecipient for the subrecipient to contribute to the goals and objectives of the project. Does not include payments to a contractor, beneficiary, or participant. May be provided through any form of legal agreement consistent with criteria in with § 200.331, including a contract.



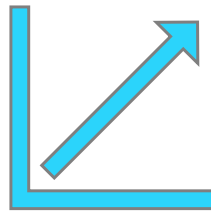


Planning Your Determination

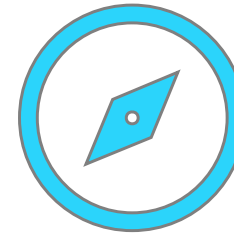
Subrecipient vs
Contractor
Characteristics



Subrecipient vs
Contractor
Monitoring



Pass-Through
Entity
Responsibility



Compliance
with 2 CFR



Subrecipient Characteristics

2 CFR §200.331



Determines who is eligible to receive what Federal assistance.



Performance is measured in relation to whether objectives of a Federal program were met.



Has responsibility for programmatic decision making.



Has responsibility for adherence to applicable program requirements specified in the Federal award.



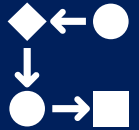
Uses the Federal funds to carry out a program for a public purpose, as opposed to for the benefit of the pass-through entity.

Cost Matching
is a unique
subrecipient
characteristic



Contractor Characteristics

2 CFR §200.331



Provides the goods and services within normal business operations.



Provides similar goods or services to many different purchasers.



Provides goods and services that are ancillary to the operation of the Federal program.



Operates in a competitive environment (normally).



Is not subject to compliance requirements of the Federal program as a result of the agreement, though similar requirements may apply for other reasons.



Subrecipient Monitoring



The pass-through entity must monitor subrecipient activities to ensure compliance with Federal statutes, regulations, and the terms and conditions of the subaward.

- Review financial and performance reports.
- Ensure the subrecipient takes corrective action on all significant developments that negatively affect the subaward.
- Issue a management decision for audit findings pertaining only to the Federal award.
- Resolve audit findings specifically related to the subaward.

Following the risk assessment, steps to ensure accountability and achievement of goals may include:

- Providing subrecipients with training and technical assistance on program-related matters.
- Performing site visits to review subrecipient program operation.
- Arranging for agreed-upon-procedures engagements.

When evaluating risk, a pass-through entity should consider the subrecipient's:

- Experience with similar subawards.
- Previous audit results.
- New personnel or changed systems.
- Extent and results of any Federal agency monitoring.



Contractor Monitoring



The recipient or subrecipient must:

Maintain records sufficient to detail the history of each procurement transaction.

These records must include the rationale for the procurement method, selection of contract type selection, contractor selection or rejection, and the basis for the contract price.

Maintain and use documented procedures for procurement transactions under a federal award or subaward.

These documented procurement procedures must be consistent with State, Local, and Tribal Laws and regulations and the standards identified in 2 CFR 200.317-327.

Maintain oversight to ensure contractors perform according to the terms, conditions, and specific of their contracts or purchase orders.

For procurement transactions in which the contractor is made responsible for meeting program requirements, the auditee must ensure those requirements are met.



Requirements for Pass-Through Entities

2 CFR §200.332



A pass-through entity must:

Verify the subrecipient is not excluded or disqualified in accordance with § 180.300.

Evaluate each subrecipient's fraud risk and risk of noncompliance with a subaward.

Verify that a subrecipient is audited as required by subpart F of part 200.

Consider whether the results of a subrecipient's audit, site visits, or other monitoring necessitate adjustments to the pass-through entity's records.

Consider taking action against noncompliant subrecipients.

A pass-through entity must provide:

- Federal Award Identification.
- Requirements of the subaward.
- Indirect cost (& de minimis) rate.
- Requirements regarding certifications of and accessibility to financial and performance reports.



Knowledge Check



???



Knowledge Check #1



When should you determine if you will be using a contract vs a subaward?



Knowledge Check #1



When should you determine if you will be using a contract vs a subaward?

Before you issue an award is recommended.



Knowledge Check #2



Should you include language in the agreement to clarify if an agreement is a contract or subaward?



Knowledge Check #2



Should you include language in the agreement to clarify if an agreement is a contract or subaward?

Yes



Knowledge Check #3



Can a contract include cost share or cost matching?



Knowledge Check #3



Can a contract include cost share or cost matching?

No



Knowledge Check #4



Do the procurement requirements in 2 CFR 200.317-327 apply to both subrecipients and recipients?



Knowledge Check #4



Do the procurement requirements in 2 CFR 200.317-327 apply to both subrecipients and recipients?

Yes, as applicable.



Conclusion



Create a checklist to help
identify a subrecipient
versus contractor



Review 2 CFR to further
understand the
requirements of each





Procurement Under Grants Overview & Associated 2024 2 CFR Updates





Disclaimer

Except for any statutes and regulations cited, the contents of this presentation do not have the force and effect of law and are not meant to bind grant recipients in any way.

This presentation is intended only to provide information and clarity on existing requirements under the law or agency policies.

Text in **blue** indicates new/updated language that will be included in the revised 2 CFR version becoming official on October 1, 2024. Award date or terms and conditions of an award will determine which version of 2 CFR applies.





2 CFR 200 Subpart D

Procurement Standards

200.317	Procurements by States and Indian Tribes.
200.318	General procurement standards.
200.319	Competition.
200.320	Procurement methods.
200.321	Contracting with small businesses, minority businesses, women's business enterprises, veteran-owned businesses, and labor surplus area firms.
200.322	Domestic preferences for procurements.
200.323	Procurement of recovered materials.
200.324	Contract cost and price.
200.325	Federal agency or pass-through entity review.
200.326	Bonding requirements.
200.327	Contract provisions (including Appendix II).



Procurements by States and Indian Tribes



New/Updated
Language

A State **or Indian Tribe** must follow the same policies and procedures it uses for procurements with non-Federal funds when conducting procurement transactions under a Federal award.

§§ 200.318 through 200.327 apply if such policies and procedures do not exist.

Procurement
Standards

200.317

200.318

200.319

200.320

200.321

200.322

200.323

200.324

200.325

200.326

200.327





General Procurement Standards

Procurement Standards

200.317

200.318

200.319

200.320

200.321

200.322

200.323

200.324

200.325

200.326

200.327

The recipient or subrecipient must maintain:

- Documented procurement procedures consistent with State, local, and tribal laws and regulations.
- Oversight to ensure contractors perform according to their contracts or purchase orders.
- Written conflicts of interest standards governing employees engaged in the selection, award, and administration of contracts.
- Records that detail the history of each procurement transaction.

The recipient or subrecipient must:

- Award contracts only to responsible contractors that can perform successfully.
- Use a time-and-materials contract only if no other contract is suitable.
- Be responsible for settling contractual and administrative procurement transaction issues.

The recipient or subrecipient is encouraged to:

- Enter into intergovernmental or inter-entity agreements.
- Use excess and surplus federal property instead of purchasing it new.
- Use value engineering clauses in contracts for construction projects.



Competition



Procurement Standards

200.317

200.318

200.319

200.320

200.321

200.322

200.323

200.324

200.325

200.326

200.327

All procurement transactions must provide full and open competition.

Written procedures for procurement transactions must:

- Ensure all solicitations clearly and accurately describe the technical requirements for the property, equipment, or service being procured.
- Identify requirements the offerors must fulfill and factors used to evaluate bids.

Prequalified Lists – The recipient or subrecipient must:

- Ensure prequalified lists are current and include qualified sources.
- Consider objective factors that evaluate price and cost to maximize competition.
- Not preclude potential bidders from qualifying during the solicitation period.

Optional scoring mechanisms developed by recipients or subrecipients must be consistent with:

- ✓ The U.S. Constitution.
- ✓ Federal statutes & regulations.
- ✓ The terms and conditions of the Federal award.



Competition



Procurement Standards

200.317

200.318

200.319

200.320

200.321

200.322

200.323

200.324

200.325

200.326

200.327

Contractors that develop or draft specifications, requirements, statements of work, or invitations for bids must be excluded from competing on those procurements.

Examples of situations that may restrict competition include, but are not limited to:






Placing unreasonable requirements on firms to qualify them to do business.	Requiring unnecessary experience and excessive bonding.	Noncompetitive pricing practices between firms or affiliated companies.	Noncompetitive contracts to consultants that are on retainer contracts.
Organizational conflicts of interest.	Specifying only a “brand name” product instead of allowing “an equal” product to be offered.	Describing the performance or other relevant requirements of the procurement.	Any arbitrary action in the procurement process.



Procurement Methods



Procurement Standards
200.317
200.318
200.319
200.320
200.321
200.322
200.323
200.324
200.325
200.326
200.327

Informal Procurement		Formal Procurement		Non-Competitive
				
Micro-Purchase	Small Purchase	Sealed Bid	Proposal	Non-Competitive





Procurement Methods

Procurement Standards

200.317

200.318

200.319

200.320

200.321

200.322

200.323

200.324

200.325

200.326

200.327

Informal Procurement



Micro-Purchase

Cost \leq \$10k (Unless increased with certifications)

- Applies to the purchase of goods and services
- No bid or quote process required.
- Price must be reasonable based on research, experience, and purchase history.
- Document the file with the reasonableness information.
- To the maximum extent practicable, distribute micro-purchases equitably among qualified suppliers.



Small Purchase

\$10k < Cost \leq \$250k

- Applies to the purchase of goods and services
- Price or rate quotes required from an adequate number of sources.
- Price or rate quotes can be collected informally (e.g., phone calls, website research).
- All quotes must be documented in the file.
- Below the Simplified Acquisition Threshold (SAT).





Procurement Methods

Procurement Standards

200.317

200.318

200.319

200.320

200.321

200.322

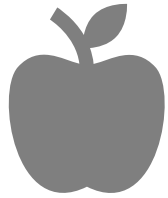
200.323

200.324

200.325

200.326

200.327



Sealed Bid

Formal Procurement

Cost > \$250k

- Must be solicited from an adequate number of qualified sources.
- Invitation for bids must be publicly advertised.
- Bids will be opened at the certain time and place.
- Contract award must be made to the lowest, responsible bidder.
- Firm fixed price contract type.
- A complete, adequate, and realistic specification or purchase description is available.

Cost > \$250k



Proposal

- Fixed price contract or cost-reimbursement contract
- Sealed bidding not appropriate and other factors should be evaluated.
- Solicitation must be public and articulate all evaluation factors and relative importance.
- Must be solicited from an adequate number of qualified offerors.
- A written method for conducting evaluations and award selection.
- Award to the responsible offeror whose proposal is most advantageous with price and other factors considered..





Procurement Methods

Procurement Standards

- 200.317
- 200.318
- 200.319
- 200.320**
- 200.321
- 200.322
- 200.323
- 200.324
- 200.325
- 200.326
- 200.327



Non-Competitive

Non-Competitive

Cost = Any dollar amount

- Applies to situations where competitive procurements would not be appropriate
- Must document rationale for one of the following:
 - Item available from a single source.
 - Public exigency or emergency won't permit a delay resulting from competition.
 - Expressly authorized via written request by the awarding agency (USDOT).
 - Competition is determined to be inadequate after solicitation.
 - Procurement is less than the micro-purchase threshold



Contracting Considerations



Procurement Standards

200.317

200.318

200.319

200.320

200.321

200.322

200.323

200.324

200.325

200.326

200.327

The recipient or subrecipient **should** ensure that small businesses, minority businesses, women's business enterprises, **veteran-owned businesses**, and labor surplus area firms are considered.

Consideration includes:

These business types are included on solicitation lists.

These business types are solicited whenever they are deemed eligible as potential sources.

Dividing transactions into separate procurements to permit maximum participation.

Establishing delivery schedules that encourage participation by these business types.

Utilizing organizations such as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce.

Requiring a contractor under a Federal award to apply this section to subcontracts.





Domestic Preferences for Procurements

Procurement Standards

- 200.317
- 200.318
- 200.319
- 200.320
- 200.321
- 200.322**
- 200.323
- 200.324
- 200.325
- 200.326
- 200.327

The requirements must be included in all contracts and purchase orders for work or products.

“Produced in the United States”

Means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States.

“Manufactured products”

Items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

Federal agencies providing Federal financial assistance for infrastructure projects must implement the Buy America preferences set forth in 2 CFR part 184.

New/Updated
Language



Procurement of Recovered Materials



Procurement Standards

- 200.317
- 200.318
- 200.319
- 200.320
- 200.321
- 200.322
- 200.323**
- 200.324
- 200.325
- 200.326
- 200.327



A recipient or subrecipient that is a State agency or agency of a political subdivision of a State and its contractors must comply with section 6002 of the Solid Waste Disposal Act, which include procuring only items designated in the guidelines of the Environmental Protection Agency (EPA) at 40 CFR part 247.



The recipient or subrecipient should purchase, acquire, or use products and services that can be reused, refurbished, or recycled; contain recycled content, are biobased, or are energy and water efficient; and are sustainable.





Contract Cost and Price

Procurement Standards

200.317

200.318

200.319

200.320

200.321

200.322

200.323

200.324

200.325

200.326

200.327

The recipient or subrecipient
MUST
perform an independent cost or price analysis for every procurement action in excess of the SAT including contract modifications before receiving bids or proposals.



The recipient or subrecipient
MUST NOT
use the “cost plus a percentage of cost” and “percentage of construction cost” methods of contracting.



Federal Agency or Pass-through Entity Review



Procurement Standards

200.317

200.318

200.319

200.320

200.321

200.322

200.323

200.324

200.325

200.326

200.327

When requested by the Federal agency or pass-through entity, the recipient or subrecipient **MUST**:

- **Submit the technical specifications of proposed procurements.**
- Provide procurement documents for pre-procurement review.

The Federal agency or pass-through entity **MAY**:

- Review the technical specifications of proposed procurements under the Federal award to ensure the item or service specified is the one being proposed for acquisition.
- Conduct a pre-procurement review when the recipient or subrecipient fails to comply with procurement standards in subpart D.

New/Updated
Language



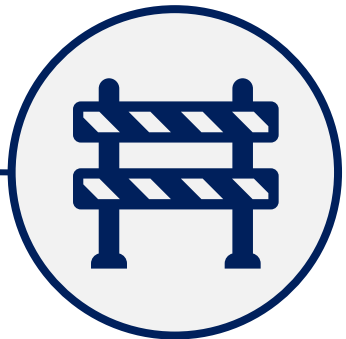


Bonding Requirements

Procurement Standards

- 200.317
- 200.318
- 200.319
- 200.320
- 200.321
- 200.322
- 200.323
- 200.324
- 200.325
- 200.326**
- 200.327

The Federal agency or pass-through entity must determine that the Federal interest is adequately protected before accepting the recipient's or subrecipient's bonding policy and requirements for construction or facility improvement contracts or subcontracts exceeding the simplified acquisition threshold.



Minimum requirements include a bid guarantee from each bidder equivalent to five percent of the bid price and a performance and payment bond on the contractor's part for 100 percent of the contract price.





Common Mistakes and Best Practices



Contract Provisions (Appendix II)

All contracts made by the non-Federal entity under the Federal award must contain provisions covering the following, as applicable.

Remedies
Termination for Cause and Convenience
Equal Employment Opportunity (EEO)
Davis-Bacon Act and Copeland “Anti-Kickback” Act
Contract Work Hours and Safety Standards Act
Rights to Inventions Made Under a Contract or Agreement
Clean Air and the Federal Water Pollution Control Act
Debarment and Suspension
Byrd Anti-Lobbying Amendment

See Appendix for more information on each act



Top Procurement Mistakes (and How to Avoid Them)



Mistake

How to avoid this mistake

1

Restricting full and open competition

Compare the written procurement policy and procurement document prior to solicitation to ensure that competition is not restrictive. See 200.319(b).

2

Not performing detailed price or cost analysis for procurements above \$250,000

Prior to receiving bids or proposals, ensure independent estimate has been completed and in file to be used as part of the bid/proposal assessment. See 200.324(a).

3

Engaging in a non-competitive procurement without documenting the justification and considerations

Use non-competitive procurements only when necessary. Document why and request approval if required. See 200.320 (c).

4

Awarding a “time-and materials” contract without a ceiling price and documenting why no other contract type is suitable

Develop written procedure for time and materials procurement documentation. Ensure a ceiling price in the draft contract prior to execution. See 200.318 (j).



Top Procurement Mistakes (and How to Avoid Them)



Mistake

How to avoid this mistake

5

Not including the required contract clauses

Compare Appendix II contract clause with your draft contract to ensure all applicable contract clauses are included. See Appendix II to Part 200.

6

Awarding a “cost-plus - percentage-of - cost” or “percentage-of - construction-cost” contract

Ensure that the written procurement policy does not allow this type of contract for federal grant projects. See 200.324(d).

7

Awarding a contract to contractors that are suspended or debarred

Ensure that the written procurement policy requires Sam.gov to be checked for all contracts prior to award. Document the file that Sam.gov was checked. See 200.214.

8

Not documenting all steps of a procurement to answer questions that could arise months or years later

Ensure the written procurement policy has required document for all procurement transaction. See 200.318.
Record retention is three years from the date of submission of the final expenditure report. See 200.334.



Knowledge Check #5



Do you need to perform a cost price analysis on a \$300,000 contract?



Knowledge Check #5



Do you need to perform a cost price analysis on a \$300,000 contract?

Yes



Knowledge Check #6



Can a contractor add a percentage increase to the grand total that is not a part of the goods and services of the award?



Knowledge Check #6



Can a contractor add a percentage increase to the grand total that is not a part of the goods and services of the award?

No, cost plus pricing is never allowed under a federal award.





Knowledge Check #7

TRUE or FALSE?

Does 2 CFR 200.317-327 apply to both recipients and subrecipients?





Knowledge Check #7

TRUE or *FALSE*?

Does 2 CFR 200.317-327 apply to both recipients and subrecipients?

TRUE



A dark blue background featuring silhouettes of several people sitting around a table, engaged in a meeting or discussion. The word "Questions?" is centered in white text.

Questions?





Contract Provisions (Appendix II)

Remedies	Contracts for more than the simplified acquisition threshold must address administrative, contractual, or legal remedies in instances where contractors violate or breach contract terms, and provide for such sanctions and penalties as appropriate.
Termination For Cause And Convenience	All contracts more than \$10,000 must address termination for cause and convenience by the non-Federal entity including how it will be effected and the basis for settlement.
Equal Employment Opportunity (EEO)	All contracts that meet the definition of “federally assisted construction contract” in 41 CFR Part 60-1.3 must include the EEO clause provided under 41 CFR 60-1.4(b).
Davis-Bacon Act	Contractors must be required to pay wages (not less than once a week) to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination. The non-Federal entity must place a copy of the wage determination made by the Secretary of Labor in each solicitation. The decision to award a contract or subcontract must be conditioned upon the acceptance of the wage determination.
Copeland “Anti-Kickback” Act	Each contractor or subrecipient must be prohibited from inducing, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled.
Contract Work Hours & Safety Standards Act	Where applicable, all contracts awarded by the non-Federal entity more than \$100,000 that involve the employment of mechanics or laborers must include a provision for compliance with statutes regarding work hours and safety standards.
Rights to Inventions Made Under a Contract or Agreement	If the Federal award meets the definition of “funding agreement”, the recipient or subrecipient must comply with the requirements of 37 CFR Part 401 and any implementing regulations issued by the awarding agency.
Clean Air & Water Pollution Control Act	Contracts and subgrants of amounts more than \$150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act.
Debarment and Suspension	A contract award must not be made to parties listed on the governmentwide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 and 12689.
Byrd Anti-Lobbying Amendment	Contractors that apply or bid for an award exceeding \$100,000 must file the required certification. Each tier certifies to not use Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award.

Stage 2 NOFO Timing

