Intelligent Transportation Systems (ITS) Cybersecurity Framework Profile

www.its.dot.gov/index.htm

Final Report – July 31, 2023
FHWA-JPO-23-120

U.S. Department of Transportation

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

Notice

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

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

Technical Report Documentation Page

1. Report No.

FHWA-JPO-23-120

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle

Intelligent Transportation Systems (ITS) Cybersecurity Framework Profile

5. Report Date

July 31, 2023

6. Performing Organization Code

7. Author(s)

Hillary Tran, Christina Sames, Carter BF Casey, Julie Nethery Snyder, David Weitzel

8. Performing Organization Report No.

V-337

9. Performing Organization Name and Address

U.S. DOT Volpe National Transportation Systems Center
220 Binney Street
Cambridge MA 02142

10. Work Unit No. (TRAIS)

11. Contract or Grant No.

IAA 693JJ320N300058

12. Sponsoring Agency Name and Address

ITS-Joint Program Office
1200 New Jersey Avenue, S.E.
Washington, DC 20590

13. Type of Report and Period Covered

Final Report August 28, 2020 – August 27, 2023

14. Sponsoring Agency Code

HOIT-1

15. Supplementary Notes

This work was performed in collaboration with the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) and the MITRE Corporation.

16. Abstract

This document is the Intelligent Transportation Systems (ITS) Cybersecurity Framework (CSF) Profile ("ITS Profile") developed for transportation deployers and operators in the ITS ecosystem and those who represent the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) Service Areas and transportation modes. The ITS Profile can be applied to support strengthening the ecosystem against cyber threats and vulnerabilities. The ITS Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to the ITS ecosystem. Practitioners implementing security controls can use the ITS Profile to help focus resources on cybersecurity activities identified as relevant and high priority for the organization or program.

17. Keywords

Intelligent Transportation Systems, Cybersecurity, Profile, NIST

18. Distribution Statement

19. Security Classif. (of this report)

Unclassified

20. Security Classif. (of this page)

Unclassified

21. No. of Pages

88

22. Price

Acknowledgements

This Intelligent Transportation Systems (ITS) Cybersecurity Framework Profile (ITS Profile) was developed in partnership between the United States (U.S.) Department of Transportation (USDOT) Intelligent Transportation Systems Joint Program Office (ITS JPO) and the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE), in collaboration with Volpe National Transportation Center and The MITRE Corporation. The USDOT is responsible for leading collaborative and innovative research, development, and implementation of intelligent transportation systems to improve the safety and mobility of people and goods[1] in partnership with multimodal ITS initiative stakeholders, industry, and USDOT agencies. To ensure cybersecurity is part of the solutions, stakeholder communities (i.e., Traffic Management, Transit, and Commercial Freight and Vehicle) were involved. The collaboration formed the basis for a USDOT ITS Profile, a voluntary tool for managing cybersecurity risk in the ITS ecosystem.

USDOT and the NCCoE would like to thank the following members of the ITS community who provided their time and invaluable insights thus far. This effort could not be successful without contributions from:

- Central Florida Regional Transportation Authority (Lynx) (Orlando)
- Dallas Area Rapid Transit (DART)
- Delaware Dubuque Jackson County Regional Transit Authority (RTA 8) (Iowa)
- Florida Department of Highway Safety and Motor Vehicles
- Florida Department of Transportation/Connected Vehicles, Arterial Management, Managed Lanes
- Idaho State Police
- Massachusetts Department of Transportation, ITS Programs
- MetroLINK (Southern California commuter rail system)
- Metropolitan Atlanta Rapid Transit Authority (MARTA)
- Metropolitan Transit Authority of Harris County
- New Hampshire Department of Safety
- New York City Department of Transportation (NYCDOT) - Bureau of Traffic Operations/Signal Division
- Pace Suburban Bus Service (Suburban Chicago)
- Pierce Transit (Pierce County, Washington)
- Public Service Commission of West Virginia

[1] Intelligent Transportation Systems - ITS Joint Program Office (dot.gov)

- San Diego Association of Governments
- San Jose California Department of Transportation
- Santa Clara Valley Transportation Authority (VTA)
- Skyline Technology Solutions
- Texas Department of Transportation
- Tri-County Metropolitan Transportation District of Oregon (TriMet)
- Valley Metro (Phoenix)
- Washington State Department of Transportation (WSDOT)
- Wyoming Department of Transportation

Table of Contents

List of Tables

List of Figures

Executive Summary

This document is the Intelligent Transportation Systems (ITS) Cybersecurity Framework (CSF) Profile ("ITS Profile") developed for transportation deployers and operators in the ITS ecosystem and those who represent the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) Service Areas and transportation modes. The ITS Profile can be applied to support strengthening the ecosystem against cyber threats and vulnerabilities. The ITS Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to the ITS ecosystem. Practitioners implementing security controls can use the ITS Profile to help focus resources on cybersecurity activities identified as relevant and high priority for the organization or program.

The ITS Profile contains 14 ITS-specific Mission Objectives and prioritized relevant cybersecurity activities (CSF Subcategories) to help organizations or agencies protect the ITS ecosystem. The contents of the ITS Profile can help organizations or agencies prioritize cybersecurity capabilities and inform cybersecurity decisions. This document discusses applying the ITS Profile for stakeholder use, including considerations before adapting the ITS Profile and using Informative References.

The ITS Profile is meant to complement and supplement, but not replace, current cybersecurity standards, regulations, and industry guidelines currently used by the transportation sector. Organizations should consider their unique obligations, operating environment, and high-level mission and business-oriented goals when prioritizing and implementing cybersecurity capabilities.

Chapter 1. Introduction

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides voluntary risk-based standards and best practices designed to help organizations and agencies manage cybersecurity risks. Using a common language, the CSF manages cybersecurity risk in a resource-effective way, based on business needs without imposing additional requirements. The CSF can either serve as a foundation for a new cybersecurity program or complement and improve the operations of an existing program. The CSF focuses on business drivers to guide cybersecurity activities and provides a general set of considerations and processes to assist in expressing cybersecurity requirements to business partners and customers. Multiple sectors and industries have opted to use the CSF to create their own prioritizations, known as CSF Profiles (Profile).

This document is a Profile, an application of the CSF to Intelligent Transportation Systems (ITS). The ITS Profile is the result of collaboration between the United States Department of Transportation (USDOT), NIST National Cybersecurity Center of Excellence (NCCoE), a series of workshops with ITS stakeholders, and analysis of available ITS resources such as the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) and the Cybersecurity Framework Profile for Connected Vehicle Environment (CVE).[2]

This document was developed to provide guidance for State and local transportation agencies with an interest in improving ITS cybersecurity. ITS is a key component of the transportation infrastructure and the Transportation Systems Sector of U.S. critical infrastructure.[3] ITS advances transportation safety and enhances productivity by integrating advanced information technology (IT) with the operational technology (OT) of transportation infrastructure and vehicles. Protecting ITS requires awareness of threats and vulnerabilities of both IT and OT. The ITS Profile can serve as a starting point to better communicate security needs and allocate resources to best help individual organizations or agencies.

1.1 Purpose and Scope

This document is the ITS Profile for the ITS ecosystem. To strengthen the ITS ecosystem against cybersecurity threats and vulnerabilities, this Profile is written around high-level ITS mission and business-oriented goals (Mission Objectives) identified by ITS stakeholders. The ITS Profile is intended to help the ITS ecosystem and its stakeholders focus on those cybersecurity activities and outcomes that support those high-level Mission Objectives (MOs) and are most suitable for ITS stakeholders and their unique environments of operations and risks. The ITS Profile can also help transportation agencies

[2] The CVE Profile is available at: https://www.its.dot.gov/research_areas/cybersecurity/references.htm#Profile

[3] Information from Cybersecurity and Infrastructure Security Agency (CISA) on the Transportation System Sector is available at: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector

identify opportunities for managing cybersecurity risks and engaging in cybersecurity risk management communications internally and externally.

The ITS Profile provides voluntary guidance for ITS implementers/deployers to address cybersecurity implications of ITS ecosystem technologies in an organized and comprehensive way. Additionally, the ITS Profile is intended to:

- Minimize future work by each agency.
- Decrease the chance agencies accidentally omit a requirement.
- Encourage consistent analysis of cyber risk.
- Align industry cybersecurity priorities.
- Facilitate the ongoing dialogue between USDOT and ITS stakeholders regarding cybersecurity priorities.
- Support discussions regarding ITS stakeholder needs with their partners.

The ITS Profile is not intended to replace any existing cybersecurity programs, guidance, or policy State and local transportation agencies may have in place, but rather to complement these as a guide to prioritizing cybersecurity activities and outcomes. The ITS Profile can also serve as a starting point for transportation agencies that do not yet have a cybersecurity program in place. Organizations should consider their unique obligations, operating environment, and high-level mission and business-oriented goals when prioritizing and implementing cybersecurity capabilities.

1.2 Audience

The ITS Profile can be used by the ITS community to communicate and make risk informed decisions regarding cybersecurity across their agencies. The ITS Profile facilitates communicating cybersecurity expectations between agencies and their business partners, suppliers, and other stakeholders (internal or external to the agency). The ITS Profile can be used by roles in leadership positions (e.g., Chief Information Officers [CIOs]), ITS manufacturers and developers, as well as others including those who support the operational aspects of the ITS ecosystem to identify and establish ITS priorities, assess current risk management programs or practices, or to develop a program. Examples of how implementers can apply the ITS Profile include:

- CIOs can use the Profile to identify, decide, and communicate agency priorities and the direction of resources (e.g., people, processes, technologies) for greater assurance or to accept risk.
- Manufacturers and developers can propose and integrate new or modified system and system components that support agency missions, needs, and requirements.
- Operators and operations management can implement the Profile to secure the infrastructure and minimize the potential impact of an incident or the impact of changes to operational systems.

- Traditionally non-cybersecurity agencies or departments (e.g., human resources) can leverage the Profile and additional resources to shape or improve development of their ITS workforce.[4]

Understanding and applying the ITS Profile benefits from practitioners having some experience in ITS or knowledge of cybersecurity concepts, although not required.

1.3 Document Structure

This document consists of the following sections:

- Chapter 2 provides an ITS overview.
- Chapter 3 presents an overview on the NIST CSF and CSF Profiles.
- Chapter 4 discusses applying the ITS Profile.
- Chapter 5 describes the methodology used to produce this Profile.
- Chapter 6 introduces the ITS Profile MOs.
- Chapter 7 details the priority Subcategories for each MO and aligning cybersecurity practices with MOs.
- References cited in this Profile and additional resources.

[4] See Resources under References and Resources in Chapter 8 for supplementary resources for developing an organization's cybersecurity workforce.

Chapter 2. Intelligent Transportation Systems

ITS is an operational system of various technologies which consists of electronics, communications, or information processing systems or devices that interact and share information through wireless and wireline communication technology.[5] The broad range of equipment and systems necessary for ITS deployment or integration in the transportation infrastructure requires coordination across the various transportation sector stakeholders.

As part of multimodal coordination, ITS Joint Program Office (ITS JPO) of the USDOT considers ITS to include assets of the Highway and Motor Carrier subsector, including: roadways, bridges, tunnels, vehicles, licensing systems, traffic management systems, and systems for operations management.[6] Additionally, ITS includes elements of the Mass Transit and Passenger Rail subsector, including: transit terminals, operational systems, and supporting infrastructure for passenger services by transit buses, trolleybuses, monorail, subways, light rail, passenger rail, and vanpool/rideshare services.[7] However, the transportation systems and information exchanges that support ITS are not limited to these subsectors.

[5] See ARC-IT glossary for ITS terminology: https://www.arc-it.net/html/glossary/glossary-i.html

[6] For more information on the Transportation System Sector, see: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector

[7] For more information on the Transportation System Sector, see: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector

ITS is involved across many transportation-specific services (e.g., electronic payment, traveler information, maintenance and construction, freight rail)[8] and provides benefits to the following ITS Areas:

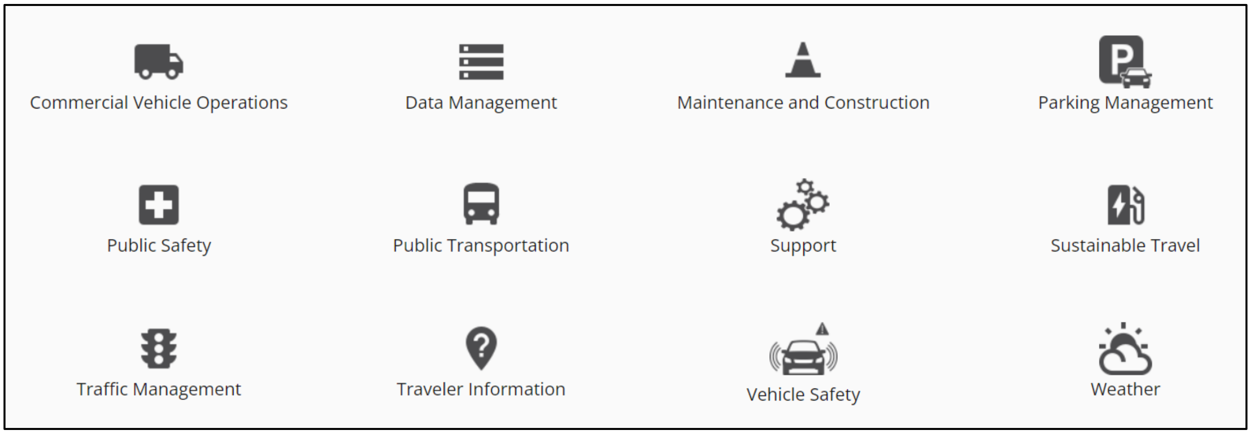


Figure 1. ITS Areas and Benefits Topics[9]

ITS encompasses a broad range of wireless and wireline communications-based information and electronics technologies deployed to improve transportation safety and mobility and enhance American productivity through integrating advanced communications technologies into the transportation infrastructure and in vehicles.[10] These technologies will be integrated directly into the transportation infrastructure, whether through updates to existing infrastructure such as traffic lights, new technologies such as ITS roadside devices, or direct changes to vehicles themselves, with the intent of improving the operating capabilities of the overall system. Integration of ITS can benefit driver, pedestrian, and roadway worker safety through improved traffic management and signaling techniques. Integration can also provide more efficient use of existing roadways and transit systems through techniques such as signal prioritization, real-time information for travelers, variable speed limits, and reversible lanes. Furthermore, improvements in efficiency can result in environmental benefits.

2.1 Industry Priorities

ITS is increasingly becoming a more critical component of improving safety and mobility in the transportation sector by providing and sharing critical information to all users. With increased integration and advancements in technologies and applications, agencies face challenges in implementing the emerging technology and applying appropriate safeguards to existing legacy infrastructure and devices. Across the sector, agencies have common gaps they seek to address to enhance the ITS ecosystem and improve ITS integration and use. The following priorities are observed in the ITS JPO Strategic Plan

[8] The Metropolitan Transportation Commission provides a list of transportation areas supported by ITS Architecture, available at: https://mtc.ca.gov/operations/programs-projects/intelligent-transportation-systems/its-architecture

[9] For more information, see: https://www.itskrs.its.dot.gov/benefits

[10] See ITS Frequently Asked Questions: https://its.dot.gov/about/faqs.htm#deploy

2020-2025,[11] as well as demonstrated across the sector in their strategies and planning activities. The ITS Profile MOs and Subcategory Priority Chart emphasize those areas and aid in indicating where resources should be devoted. Industry priorities include, but are not limited to:[12]

- **Safety** – Agencies aim to promote safety by working towards limiting damage, injuries, or deaths in the ecosystem. Personal safety and user security (e.g., workers, riders, patrons) is closely connected to cybersecurity. Innovations in technology look to maintain and improve human safety. Implementing these innovations identify and communicate safety implications.[13] The highest priority MO (MO 1 "Improve physical safety in the of the transportation ecosystem") in the Profile represents the importance of physical safety in the ecosystem and prioritized cybersecurity activities and outcomes, emphasize actions contributing to physical and human safety.
- **Social Equity** – Stakeholders look to improve access to services and opportunities and remove barriers for underserved communities. Social equity in transportation is a multimodal effort. It is necessary to provide travel for all modes regardless of location, income, or disability to ensure "complete trips".[14] Furthermore, increasing equity needs to extend beyond availability of transportation modes, to increasing equity and diversity in workforce and contracts.
- **Leadership and Stakeholder Coordination** – Agencies and government entities have the tools they need to make better decisions. Research, development, and ITS deployment are available to multiple stakeholders. Cross collaboration and communication of investments or deployments benefit awareness/understanding of implementations at the leadership level. Using plain language to explain technologies helps facilitate communication between stakeholders. The MOs and Subcategory priorities focus on stakeholder engagement and governance measures required to achieve successful stakeholder coordination.
- **Interoperability** – Services need to be interoperable with physical assets as resources or technologies shift to the digital infrastructure. Interoperability can allow for centers and services to aggregate data for improved situational awareness in the ITS ecosystem. Agencies emphasize coordination on standard development and guidance on interoperability for ITS users. Standards with knowledge and technology transfers help enable ongoing interoperable integration.[15] Several MOs place emphases on cybersecurity outcomes in the Identify and Protect Functions to ensure interoperability among IT and OT assets.
- **Workforce** – Agencies maintain strong relationships within the workforce through trust and transparency. Staff skills and opportunities are modernized and aligned to technology systems, with training opportunities available to develops skills and knowledge necessary. Cybersecurity and data privacy are integrated as a function of job roles and responsibilities. Subcategory

[11] See: https://its.dot.gov/stratplan2020/ITSJPO_StrategicPlan_2020-2025.pdf

[12] See: https://www.transit.dot.gov/sites/fta.dot.gov/files/tro3_strategic_plan.pdf

[13] See: https://www.transit.dot.gov/sites/fta.dot.gov/files/tro3_strategic_plan.pdf

[14] See: https://its.dot.gov/stratplan2020/ITSJPO_StrategicPlan_2020-2025.pdf

[15] See: https://its.dot.gov/stratplan2020/ITSJPO_StrategicPlan_2020-2025.pdf

priorities reflect the awareness and training and knowledge skills required to enable workforce development within an agency.

- **Resiliency** – Emphasis placed on operational resilience aids in response and recovery efforts. Resiliency of agency assets through technical safeguards (e.g., server redundancy, network segmentation) helps minimize interruptions of ITS and transportation business processes.[16] Subcategories are prioritized to place focus on response and recovery activities, as well as steps necessary to strengthen agency assets to reduce the impact of a cyber incident.
- **Response and Recovery Efforts** – Focus on developing and maintaining a cyber incident response and recovery plan through an established operation's agency structure and defining roles and responsibilities.
- **Natural Environment and Sustainability** – Focusing on improvements to congestion and traffic flow will help reduce fuel consumption and greenhouse gas emissions. Existing transportation operations are sustained with minimal impacts to the environment.[17]

[16] See: https://wsdot.wa.gov/about/secretary-transportation/strategic-plan

[17] See: https://www.transit.dot.gov/sites/fta.dot.gov/files/tro3_strategic_plan.pdf

Chapter 3. NIST Cybersecurity Framework v1.1 Overview

Created through collaboration between industry and government, the NIST CSF provides flexible, risk-based, and voluntary guidance based on existing standards, guidelines, and practices to help organizations better understand, manage, reduce, and communicate cybersecurity risks. Although originally designed for organizations part of the U.S. critical infrastructure, many other organizations in the private and public sectors use the CSF for managing cybersecurity risk. The CSF enables organizations and agencies—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving security and resilience. It provides a common language for understanding, managing, and expressing cybersecurity risk and cybersecurity management communications among internal and external stakeholders and across an organization or agency, regardless of cybersecurity expertise.

The NIST CSF consists of three main components: the Core, Profiles, and Implementation Tiers.[18] The Core is a catalog of desired cybersecurity activities and outcomes using easily understood, common language. The Core guides organizations in managing and reducing their cybersecurity risks to complement an organization's existing cybersecurity and risk management processes. A CSF Profile is a customized alignment of organizational or agency requirements, mission/business requirements, risk appetite, and resources against the desired outcomes of the CSF Core. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity in an organization or agency. Implementation Tiers guide organizations and agencies to consider the appropriate level of rigor for their cybersecurity program and are often used as a communication tool to discuss risk appetite, mission priority, and budget. The Tiers help organizations understand whether they have a functioning and repeatable cybersecurity risk management process and the extent to which cybersecurity risk management is integrated with broader organizational risk management decisions. (While part of the NIST CSF, for the purposes of this Profile, further discussion on Implementation Tiers is not included.)

3.1 Cybersecurity Framework Core v1.1

The CSF articulates cybersecurity activities and outcomes using common language so all levels of an organization or agency, from the executive level to the individuals with operational roles, can be in alignment on cybersecurity priorities and next steps. It also provides examples of existing standards to help organizations achieve those outcomes. The CSF Core consists of five concurrent and continuous Functions that, when considered together, provide a high-level, strategic view of an organization's management of cybersecurity risk.

[18] CSF-specific terms such as Core, Implementation Tiers, Profile, Function, Category, and Subcategory are normally capitalized and will be capitalized throughout this document.

The five Functions of the Framework Core are:

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the CSF. Understanding the business context, the resources that support critical functions and the related cybersecurity risks, enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The activities in the Protect Function support the ability to limit or contain the impact of a potential cybersecurity event.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The activities in the Detect Function enable timely discovery of cybersecurity events.
- **Respond** – Develop and implement the appropriate activities to act regarding a detected cybersecurity event. The activities in the Respond Function support the ability to contain the impact of a potential cybersecurity event.
- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations to reduce the impact from a cybersecurity event.

For each Function, the CSF Core includes underlying Categories and Subcategories. **Table 1** depicts the five Functions and the 23 Categories of cybersecurity outcomes such as “Asset Management” (ID.AM) and “Protective Technology” (PR.PT).

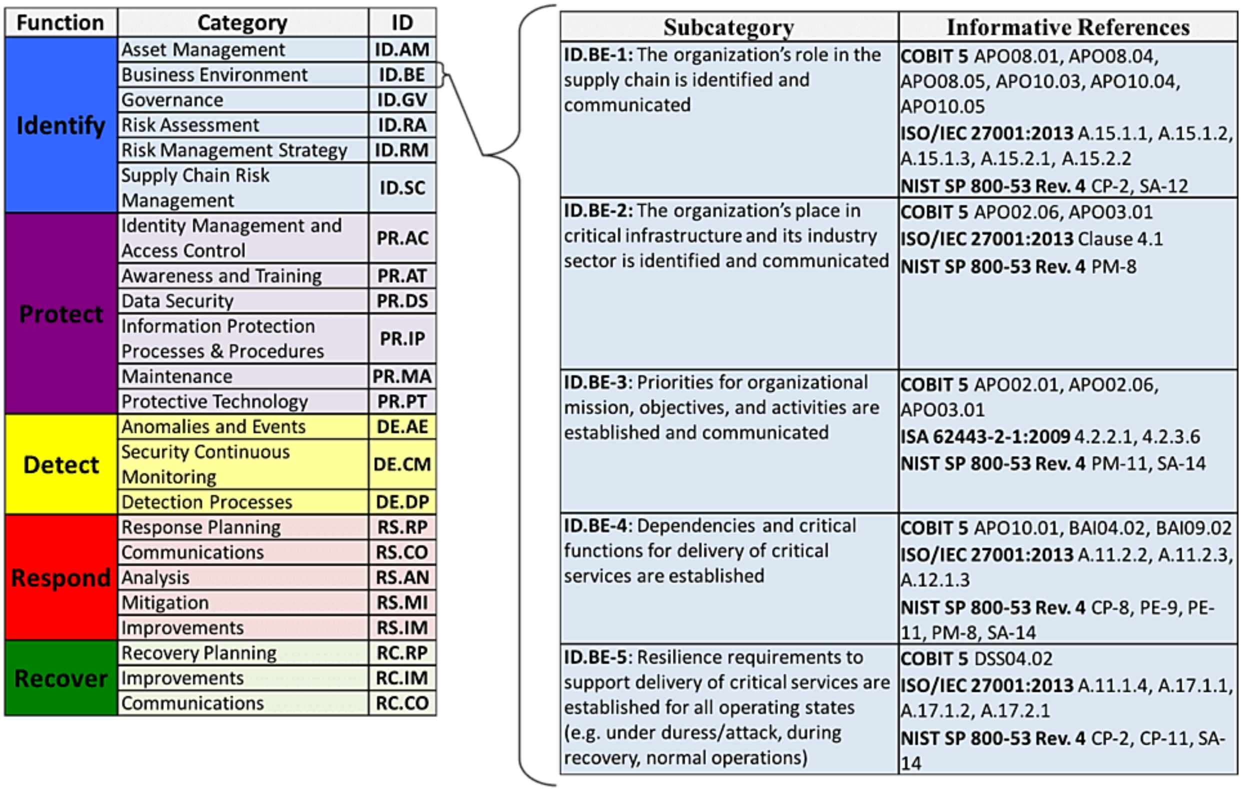
Table 1: Cybersecurity Framework v1.1 Functions and Categories

Function	Function Identifier	Category Unique Identifier	Category
IDENTIFY	ID	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PROTECT	PR	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DETECT	DE	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes

Function	Function Identifier	Category Unique Identifier	Category
RESPOND	RS	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RECOVER	RC	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

The 23 Categories are further divided into 108 Subcategories of specific technical or management activities. The Core also includes Informative References (i.e., existing standards, guidelines, and best practices) that provide practical guidance to help an organization achieve the desired outcome of each Subcategory. The Informative References are now maintained in the NIST Cybersecurity and Privacy Reference Tool (CPRT),[19] which offer a consistent format for accessing the reference data of NIST cybersecurity and privacy standards, guidelines, and frameworks. **Figure 2** provides an example of Subcategories and Informative References within the CSF Category "Business Environment" (ID.BE).

[19] See: https://csrc.nist.gov/Projects/cprt



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figure 2: NIST CSF Core Subcategory and Informative References Example[20]

3.2 CSF Profiles

The CSF and CSF Profiles (Profiles) serve as a flexible, customizable tool for implementers, deployers, and leadership to address cybersecurity implications of their environment or sector in an organized and comprehensive way. Profiles identify and prioritize opportunities for improving cybersecurity at an agency or within an industry. Profiles align CSF Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of an organization or agency.[21] Profiles are oriented around an organization's or agency's business drivers (i.e., MOs) which serve as concise, high-level goals that must be achieved for the organization to succeed in meeting its primary mission. MOs provide the necessary context for an organization or agency to manage its cybersecurity risk and guide cybersecurity activities as it relates to a specific mission need. Profiles note the CSF Subcategories especially relevant to each MO and suggest how those CSF Subcategories should be prioritized to fit the needs of the organization.

[20] Adapted from: *The Framework for Improving Critical Infrastructure Cybersecurity Presentation:* https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview

[21] NIST Cybersecurity Framework, Section 2.3 "Framework Profile."

Profiles can be a “Current Profile” (an existing state) or a “Target Profile” (a “to be” state). A Current Profile reflects the current state of a cybersecurity program and implementation of people, process, and technology to reduce or eliminate certain cybersecurity risks. A Target Profile describes the desired future state cybersecurity program and where an organization wants to be in its future state, given its risk posture. Within an organization or agency, Target Profiles offer a consistent way to communicate cybersecurity objectives across organizational or agency roles—from senior leadership to technical implementors—using common terminology.

An organization or agency can also use a sector or industry-developed profile as a Target Profile (e.g., ITS Profile). Profile users can leverage a sector or industry Target Profile as-is or alter the Profile to meet their specific cybersecurity needs and requirements based on factors such as risk tolerance, input from partners, legal or regulatory requirements, and available resources. A sector or industry Target Profile offers a prioritization of NIST CSF Subcategories based on priority mission and operational considerations for a specific community, industry, or group of stakeholders, such as the ITS ecosystem. These Target Profiles serve as a useful starting point for identifying and engaging in discussions about cybersecurity activities and outcomes important to the Profile’s user community.

Both Current and Target Profiles use the Core to help determine the state of an organization’s cybersecurity program. A comparison between Current and Target Profiles can provide a gap analysis that can be used as a decision support tool for identifying opportunities to improve their cybersecurity posture and risk management efforts. Individuals within an organization or agency can use the gap analysis to evaluate their cybersecurity program, prioritize allocating resources for cybersecurity improvements or to areas of particular concern, and progress towards the desired state in the Target Profile.

For agencies that require a starting point for leveraging the CSF, NIST’s *Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide* provides and an overview and explanation of each of the CSF Functions.[22]

[22] See: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271.pdf

Chapter 4. Applying the ITS Profile

Agencies with ITS operations can adapt and use the ITS Profile to establish or improve their cybersecurity risk governance process, practices, and activities and align with other risk management priorities. When applying the ITS Profile, State and local transportation agencies should consider the unique needs of their environment (e.g., applicable state laws, policies, standards), risks, challenges, threats, and other influencing factors adapting it for their use. This may include adjusting the prioritization of Subcategories under an MO or developing a new MO and determining its prioritized Subcategories along with relevant rationale to support informed risk management decision making and communications. Categories and Subcategories which may not initially be prioritized by the agency, nevertheless, are important to an organization and warrant further review or consideration in accordance with organizational priorities and resources.

To develop a robust cybersecurity risk management program, implementers of the Profile should review Categories and Subcategories outside what they have determined as a priority and determine whether to elevate the prioritization of specific Subcategories. Prioritized Subcategories reflect cybersecurity outcomes that may warrant more immediate attention in relation to the general ITS ecosystem. Agencies benefit from reviewing and implementing all CSF Subcategories in the context of their cybersecurity risk management program. As a starting point, the ITS Profile includes prioritized CSF Subcategories designed to help an agency protect the ITS ecosystem.

To apply the ITS Profile, State and local transportation agencies may use the following activities:

- Analyze the ITS Profile MOs and identify gaps in existing operations, processes, or plans:
    - Review MOs not currently addressed and determine applicability within the agency environment.
    - Determine next steps or develop an action plan to incorporate the MOs into the agency's existing cybersecurity risk management program.
- Review the ITS Profile MOs and Subcategory priorities for applicability within a specific agency environment:
    - Designate MOs as “N/A” or “Not Applicable” that are not relevant to the program’s deployment plans.
    - Adapt existing MOs and Subcategory priorities, if needed, to reflect the operating environments, risk tolerances, and available resources.
    - Develop additional MOs to support individual implementation, if needed, and adjust the relative priority of MOs or Subcategories accordingly. Any additional agency-specific MO(s) should be relevant to that agency’s specific ITS operating environment.
- Map the agency’s applicable policies, standards, and other implementation resources where available (these may be used in addition to or instead of the Informative References the CSF provides for each Subcategory).

- Tie to Existing and Emerging Risk Governance Programs
- Tie to the budget/resource allocation for ITS.
- Use the ITS Profile as a tool to aid with cybersecurity risk management and strategic communications:
    - Internally (i.e., between stakeholders from those in Executive-level roles to line-level implementers)
    - Externally (i.e., between agency stakeholders and other agencies, partners, suppliers, and regulators)
    - Between cybersecurity experts and experts in other fields.
- Explore how CSF efforts integrate with other ITS risk management efforts, including integrating the NIST Privacy Framework into the ITS Profile and integrating with previous privacy engineering guidance.
- Conduct a gap analysis, which will consider an agency's cybersecurity posture relative to the ITS Profile and any agency-specific Target Profile.
    - A high-level assessment against the Target Profile may reveal which cybersecurity capabilities are fully executed, as well as those not fully addressed.
    - Gaps can be prioritized based on impact and relative importance to cybersecurity, and how those gaps affect an agency's ability to achieve its MOs.

      Prioritized gaps form the basis for an action plan, which should also consider the specific steps, resources, and timeline required to close or address gaps.

Ultimately, ITS-focused agencies can apply and adapt the Profile to identify the cybersecurity activities and outcomes they need to achieve for their own operations and when sharing resources with other ITS-focused agencies to manage cybersecurity risks to critical mission and business endeavors.

Chapter 5. ITS Profile Development Methodology

Developing a CSF Profile is a collaborative, stakeholder-driven process. To align the Profile with cybersecurity outcomes and mission requirements, input from ITS stakeholders and experts from ITS Areas (see **Figure 1**) was critical. This methodology lays out how NCCoE gathered input and garnered consensus from a group of stakeholders to produce this Profile.

5.1 Inputs to the ITS Profile

Sections 5.1.1, **5.1.2**, and **5.1.3** provide information on the inputs, listed alphabetically, used to inform the development of the ITS Profile.

5.1.1 ARC-IT Goals

To provide a national blueprint for planning and deploying ITS, ITS JPO released ARC-IT v9.1.[23] ARC-IT provides a common framework for designing ITS. Planners, engineers, and other ITS stakeholders can use ARC-IT to inform ITS planning and integration.

ARC-IT provides over 150 sample ITS implementations planners and engineers can reference and adapt to their specific needs. These sample implementations, called service packages, provide goals and objectives. ARC-IT Goals[24] offer a list of generalized statements which broadly relate the physical environment to goals and desired outcomes present across the ITS ecosystem.[25] ARC-IT Goals are supported by one or more ARC-IT Objectives[26] that define what needs to occur to accomplish the Goal and identify strategies and investments that will be included in project plans. ARC-IT Goals and ARC-IT Objectives serve as input for developing ITS architecture and help planners identify which components of the ecosystem support each ARC-IT Objective. ARC-IT Goals, like MOs in a Profile, aid in transportation planning desired outcomes and “are closely tied to the planning factors required by 23 CFR 450 [Planning

[23] See: https://www.arc-it.net/index.html

[24] The USDOT ARC-IT Goals, which reflect the desired outcomes and the transportation vision for a region to support transportation planning by metropolitan and statewide areas, are available at: https://www.arc-it.net/html/archuse/goals.html. The Goals are intended to ultimately support ARC-IT Service Packages and Areas.

[25] See: https://www.arc-it.net/html/archuse/goals.html

[26] An ARC-IT Objective defines what needs to occur to accomplish an ARC-IT Goal. Each goal is supported by one or more objectives. For more information and a list of Objective Categories and Objectives, see: https://www.arc-it.net/html/archuse/objectives.html

Assistance and Standards]."[27] Considering ARC-IT Goals, Objectives, and ITS Architecture, ITS planners and stakeholders can inform development of their operational objectives with resources available.

Service packages showcase how a set of interconnected components (i.e., Views), which focus on four different architecture perspectives, contribute to meeting ARC-IT Goals and Objectives:

- **Enterprise** – Addresses the relationships between agencies and users, and their roles in the delivery or consumption of ITS services.
- **Functional** – Functions and interfaces foundational to the Physical view.
- **Physical** – Can be viewed further through service packages that represent specific services in the Physical View (e.g., Public Transportation, Traffic Management, Vehicle Safety). A service package will detail physical objects (systems and devices), functional objects, and information flows relevant to the specified ITS Service Area.
- **Communications** – Linked to services packages and provides Source, Data Flow, and Destination.

5.1.2 Connected Vehicle Environment (CVE) Profile

Connected Vehicle (CV) technologies integrate communication technologies with transportation infrastructure to improve safety and efficiency. Innovations in CV technologies and applications allow for more reaction time to prevent accidents. CV technologies do not limit drivers to "line of sight" communications; it provides notifications or alerts on traffic and potential hazards prior to the incident being in view, enhancing situational awareness.[28] Application of CV capabilities are dependent on leveraging ITS and communication technologies. By enabling communication and information sharing among various transportation infrastructure devices and components, CV is an important component of the ITS ecosystem. The ITS Profile considers risks and requirements associated with CV technologies as a component of the ITS ecosystem's priorities.

Development of the ITS Profile is rooted in the ITS JPO sponsored project to develop a limited-scope Profile based on engagements with the University of Michigan Transportation Research Institute and the Connected Vehicle Pilot Programs with the New York City Department of Transportation, the Tampa Hillsborough Expressway Authority, and the Wyoming Department of Transportation.[29] The result of this work was released as a CSF Profile for the CVE. This Profile was developed to support the emergence of connected vehicle deployments across the United States and manage the associated cybersecurity risks. Because connected vehicle environments impact the ITS ecosystem, the CVE Profile was analyzed for its relationship to and impact on the ITS Profile. The CVE Profile served as a proof of concept for use of Profiles in the ITS industry and development of the ITS Profile. The ITS Profile development methodology

[27] Federal Highway Administration, Department of Transportation requirement for Statewide and Nonmetropolitan Transportation Planning and Programming See: https://www.ecfr.gov/current/title-23/chapter-I/subchapter-E/part-450/subpart-B

[28] For more information on CV technologies and ITS JPO CV Program activities see: https://www.its.dot.gov/research_archives/connected_vehicle/connected_vehicle.htm

[29] Background and Program Overview of the ITS JPO Connected Vehicle Pilot Program is available at: https://www.its.dot.gov/pilots/overview.htm

is based upon the process used when developing the CVE Profile and has been updated to reflect facilitating workshops virtually.

5.1.3 ITS Stakeholder Groups

ITS stakeholder groups were identified and engaged with to gain perspective on current and future sector operations and priorities. Members of these groups participated in workshops and provided comments during development of the Profile. Three workshops were conducted with stakeholders from three areas of ITS-related infrastructure: Traffic Management, Transit, and Commercial Vehicle and Freight. These stakeholder communities were identified for workshops because they deploy ITS infrastructure. The following definitions are taken from the relevant Service Areas under ARC-IT:

- **Traffic Management**: "This area addresses the management of the movement of all types of vehicles, travelers, and pedestrians throughout the transportation network. It deals with information collection, dissemination, and processing for the surface transportation system. It covers both automated monitoring and control activities as well as decision-making processes (both automated and manual) that address real-time incidents and other disturbances on the transportation network, as well as managing travel demand as needed to maintain overall mobility."[30, 31]
- **Transit**: "This area addresses the management, operations, maintenance, and security of public transportation to enable them to provide transit services that operate in a timely and efficient manner, delivering operational information, including multimodal information to the operators and users. This area covers both fixed route and demand response systems, as well as those passenger rail systems operated by transit agencies."[32]
- **Commercial Vehicle and Freight**: "This area addresses the management of the efficiency, safety, and operation of commercial vehicle fleets and the movement of freight. It includes activities that expedite the authorization process for freight to move across national and other jurisdictional boundaries, activities that expedite inter-modal transfers of freight and the operation of freight vehicles that exchange information on the motor carrier, the vehicle, the driver, and, in some cases, the cargo to enhance freight operations and management."[33]

5.2 Stakeholder Workshops

Between September 2021-October 2022, the USDOT hosted virtual workshops for the three major areas of ITS identified in **5.1.3**. In this capacity as infrastructure owner/operators, the workshop participants represent the community that will use the ITS Profile to manage cybersecurity risk for their infrastructure.

[30] See: https://www.arc-it.net/html/archuse/goals.html

[31] See: https://www.arc-it.net/html/servicepackages/sa1.html

[32] See: https://www.arc-it.net/html/servicepackages/sa3.html

[33] See: https://www.arc-it.net/html/servicepackages/sa5.html

The workshops sought to gather information from participants to form the basis for developing a greater ITS Profile including other ITS-supported ARC-IT Areas and Service Packages and the CVE CSF Profile.

Each workshop (i.e., traffic management, transit, and commercial freight and vehicle) was a series of virtual working sessions and activities to introduce participants to the CSF, the methodology used during the working sessions to gather stakeholder input for this Profile, and workshop activities. Workshop activities included brainstorming, focused discussion, and participant session preparation between sessions. All sessions were facilitated by the NCCoE team.

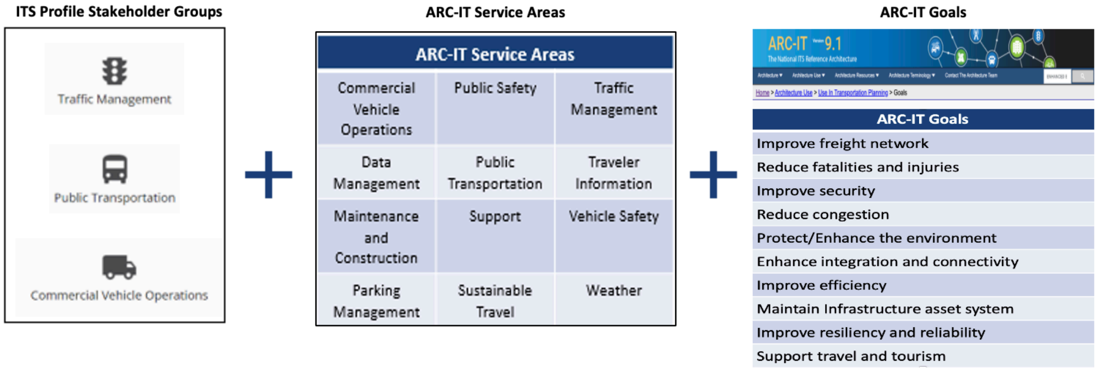
The goal of each workshop was for the participants to:

- Identify and describe high-level candidate MOs for managing and maintaining operations specific to their ITS area.
- Engage in an activity to determine candidate MO's importance and criticality to ITS.
- Engage in an activity to prioritize the type of cybersecurity activities, using the Categories in the CSF Core, for each MO identified during their stakeholder workshop.

This work forms the basis for developing a greater ITS Profile that includes other ITS-supported service areas found in USDOT's ARC-IT.

5.3 Post Workshop Activities

Following the workshops, the NCCoE team of subject matter experts (with expertise in the Transportation sector, ITS, cybersecurity, and privacy) needed to develop general Mission Objectives and cybersecurity outcomes and activities that reflect the broad ITS ecosystem. The NCCoE team analyzed the participants' inputs received throughout the workshop activities alongside the other sources listed in **5.1** to inform development of the ITS Profile. During Mission Objective development and Subcategory prioritization, the NCCoE team established Mission Objectives and determine priority cybersecurity outcomes, and activities that would apply to stakeholders in the broad ecosystem by reviewing the complete list of ARC-IT Service Areas and their respective service packages. The NCCoE team documented general rationales for why an organization would prioritize a Subcategory, along with specific rationale for prioritizing Subcategories for MOs where appropriate. This analysis is contained in **Chapter 7** and **Appendix C**.



ARC-IT Service Areas		
Commercial Vehicle Operations	Public Safety	Traffic Management
Data Management	Public Transportation	Traveler Information
Maintenance and Construction	Support	Vehicle Safety
Parking Management	Sustainable Travel	Weather

ARC-IT Goals
Improve freight network
Reduce fatalities and injuries
Improve security
Reduce congestion
Protect/Enhance the environment
Enhance integration and connectivity
Improve efficiency
Maintain Infrastructure asset system
Improve resiliency and reliability
Support travel and tourism

Figure 3. ITS Ecosystem Stakeholder Areas Reviewed for the ITS Profile

5.3.1 Mission Objective Development

Candidate MOs from each of the three virtual workshops varied in scope, scale, and number. The number of candidate MOs identified during the workshop discussions with each stakeholder area ranged from 12 to 25. USDOT and NCCoE used input from those discussions, as a component of the analysis, in conjunction with the ARC-IT Goals[34] and the CVE Profile. Using the ARC-IT Goals and CVE Profile ensured aspects of ITS not captured during the stakeholder workshop are represented in the ITS Profile MOs. The analysis resulted in a combined set of ITS ecosystem MOs.

NCCoE analyzed the three sets of candidate MOs from the workshops to identify areas of commonality and emergent themes. For example, all three ITS stakeholder workshops identified candidate MOs related to efficient use of transportation modes and services. Furthermore, the CVE Profile contains two MOs that speak to using warning, alerts, and traffic data for improving efficiency in "Providing transportation efficiency for commercial vehicles and fleets" and "Improve mobility for passenger vehicles." To ensure the ITS MOs applied to the broader ITS ecosystem, the theme was analyzed against ARC-IT Goals. Efficiency was noted in two ARC-IT Goals: 1) Reduce congestion (Achieve a significant reduction in congestion) and 2) Improve efficiency (Improve the efficiency of the surface transportation system). The theme of efficiency became MO 2, "Increase the efficiency of the transportation system." While the goals and scope of each ITS area differ, USDOT and NCCoE determined there are broadly applicable MOs and cybersecurity priorities between these environments applicable to the ITS ecosystem. The consolidated set of ITS MOs incorporates the concepts and feedback provided by the participants, yet the objectives are broader than many of the inputs provided so they can be used across the ITS areas, services, and stakeholders who may vary widely in scope, goals, and priorities.

Once the consolidated list of MOs was determined, inputs from the original candidate MOs were used to calculate relative priorities among them and draft a description for each. The consolidated and ranked MOs, along with their draft descriptions, are provided in **Table 2**.

5.3.2 Category Prioritization

For each consolidated MO, the NCCoE team analyzed the prioritized Categories identified by stakeholders to inform which Categories were important or supportive of each consolidated MO. The priority Categories identified from each workshop's Category scoring activities and the facilitated discussion were critical input to determine priority Categories for the consolidated list of MOs and understand what cybersecurity activities and outcomes were significant to a given consolidated MO's success. These prioritized Categories, as determined by the workshops' stakeholders, served as MO priority Categories and acted as a guide for Subcategory prioritization discussions.

5.3.3 Subcategory Priorities

The NCCoE team used Category prioritizations and outputs from facilitated discussions during the stakeholder workshops as a guide to determine priority CSF Subcategories for each consolidated MO.

[34] The USDOT ARC-IT Goals, which reflect the desired outcomes and the transportation vision for a region to support transportation planning by metropolitan and statewide areas, are available at: https://www.arc-it.net/html/archuse/goals.html. The Goals are intended to ultimately support ARC-IT Service Packages and Areas.

Transportation sector SME knowledge contributed to identifying additional Subcategories for discussion to ensure Subcategory priorities reflect current and future developments in the ITS environment.

For each MO, the NCCoE team discussed and identified the priority of a Subcategory for that specific MO. All other Subcategories not identified as critical or significant to an MO were noted as important to the overall cybersecurity of the MO but did not require the same level of urgency as higher priority Subcategories. This process was repeated for all consolidated MOs. Subcategory priorities are in **Chapter 7**.

For MOs that potentially involve user data or other privacy concerns (e.g., collection of Protected Health Information (PHI),[35] maintaining traveler privacy, data minimization) an expert on privacy and the NIST Privacy Framework[36] was consulted during the Subcategory discussions. The focus of the ITS Profile is cybersecurity and it only references privacy where the two areas share some overlap. Although the ITS Profile does not include a NIST Privacy Framework Profile, Privacy Framework Subcategories that are mapped to CSF Subcategories informed and sometimes increased the priority of a Subcategory given the potential for privacy risks. **Appendix B** provides a description of the relationship between cybersecurity and privacy.

[35] PHI is a subset of information that is protected in certain healthcare-related contexts under the Health Insurance Portability and Accountability Act (HIPAA) and its regulations. Not all health-related data is PHI under HIPAA, but when HIPAA applies, ITS programs may also need to follow the HIPAA Security and Privacy Rules.

[36] See https://www.nist.gov/privacy-framework

Chapter 6. ITS Profile Mission Objectives

The ITS Profile serves as a voluntary, community-wide Target Profile that ITS stakeholders can use as a starting point to create their own program's Target Profile that meets their goals and priorities. The elements of the Profile align the agency's mission/business needs and requirements with the prioritized CSF Categories and Subcategories in achieving the MOs. Using the ITS Profile, an organization can identify gaps to be addressed to meet cybersecurity risk management objectives. An organization can adapt the ITS Profile (i.e., MOs priority order, application of Categories and Subcategories) to specific agency needs.

6.1 Mission Objectives

As a result of the post-workshop activities described in Section **5.1.3**, 14 MOs were identified for the ITS ecosystem. Their descriptions are formed from workshop participant input and NCCoE team expertise. The MOs are prioritized based off inputs from the virtual workshops, and their prioritization is meant to be informative rather than prescriptive.

Below each MO description are priority Categories. These are informed by stakeholders' Category selections during workshops and post-workshop analysis of consolidated MOs. The listed Categories offer implementers of the Profile a view of Categories considered significant to achieving each MO. The Categories are listed by their order in the NIST CSF Core and do not reflect the Category's importance relative to the MO. Each agency should consider its own mission/business requirements, goals, and priorities when consulting this Profile and adjust how the agency may apply guidance accordingly.

Table 2: Prioritized Mission Objectives and Mission Objective Descriptions

Mission Objective and Priority	Mission Objective Description
1. Improve physical safety of the transportation ecosystem	A safe and resilient transportation ecosystem is foundational to keeping the public safe, regardless of mobility mode (e.g., pedestrians, bicycles, cars, public transportation, emergency vehicles and first responder's movement). Physical safety considerations may include providing safe and dependable services to the public, providing commercial freight drivers with resources (e.g., roadside awareness interactions such as traffic stops with law enforcement officials, training opportunities for commercial freight drivers), and ensuring those enforcing regulations have access to data needed for inspections and violation identification. Additionally, it may be possible to reduce crashes through efficiency measures such as optimizing the flow of traffic and accommodating emergency response activities. Physical security measures need to be implemented in a consistent and reliable manner.

Mission Objective and Priority	Mission Objective Description
	Priority Categories: *ID.AM, ID.BE, ID.GV, ID.RA, ID.RM, PR.AT, PR.MA, PR.DS, PR.PT, DE.CM, DE.DP, RS.RP, RS.CO*
2. Increase the efficiency of the transportation ecosystem	ITS provides an opportunity to optimize, regulate, and coordinate surface transportation in a technology-driven, efficient manner. ITS operations can manage congestion and introduce efficiencies for vehicles and the traveling public by providing real time information to and from vehicles and regional/local transportation systems, as well as transit riders. Note: MO 12 "Promote and provide equitable service and communications to the public" speaks to engagement necessary to facilitate efficiency measures. *Priority Categories: ID.AM, ID.BE, ID.GV, PR.AT, PR.IP, DE.AE, RS.AN, RS.CO*
3. Collect, manage, use, and disseminate data	An "intelligent" transportation system is one that incorporates data (e.g., vehicles, sensors in municipal equipment such as roadside equipment and toll transponders, individuals) to provide situational awareness and inform decision making. The key high-level activities involving data are: 1) collecting data from outside and within the transportation system, 2) managing data by storing, transmitting, and otherwise controlling it, 3) using data within ITS tools and environments, and 4) disseminating data between State and local departments of transportation that may also have a purpose for it. Disseminating data can also include communications with the public, such as traffic information dissemination through roadway equipment or providing transit traveler information. *Priority Categories: ID.GV, ID.RA, PR.DS, PR.IP, PR.PT, RS.RP, RS.CO, RC.RP, RC.IM*
4. Improve ITS infrastructure and its condition through maintenance and supply chain management	Providing safety and reliability to the public is dependent on maintaining and improving the condition of the ITS infrastructure (e.g., service area infrastructure, fleet, facility operations). This includes preserving the ability of installed technologies to operate effectively (i.e., upkeep of physical devices and software updates) deploying new technologies or capabilities, and often integrating new technologies with legacy infrastructure. Newer technologies often require additional maintenance and management capabilities, and updates to ensure they maintain functionality and connectivity. ITS operations can further facilitate these processes by engaging with members of the supply chain to shape development of the ITS infrastructure and manage risks. *Priority Categories: ID.AM, ID.BE, ID.SC, PR.MA, DE.AE, DE.CM, RS.RP, RS.IM, RC.RP, RC.IM*
5. Coordinate policy and standards	Standards promote consistent application and interoperability of ITS technologies, effective and efficient information exchange with administrative processes, and licensing. The development and distribution of ITS policy and standards benefit from coordination. New or evolved technologies and capabilities require new policies and standards. Coordination is necessary for transportation activities that have a regional,

Mission Objective and Priority	Mission Objective Description
	national, or international impact (e.g., movement of vehicles across borders, travel, and tourism), and to be an effective participant, ITS stakeholders actively engage in standards activities. Note: Coordination with stakeholders is addressed in MO 13 "Engage with the community and relevant stakeholders." *Priority Categories: ID.AM, ID.RA, PR.AT, PR.IP, RS.RP*
6. Enable workforce development	ITS and connected systems require a workforce that understands how evolving technology can make transportation safer, more reliable, and more efficient. Efforts to develop an ITS workforce include providing existing staff opportunities to maintain and enhance their current skills, recruiting the additional talent needed to fill any gaps in capabilities, maintaining high employee morale, and offering opportunities for education, training, and continuous learning. Agencies develop and deliver training curricula consistent with regulations and requirements, real-world scenarios, and current technology. Opportunities are provided to develop or strengthen technical skills. Many types of roles support effective ITS operations, such as transit operators, commercial freight drivers, weigh station inspectors, IT administrators, and many other types of technical, administrative, and operational roles. Ensuring high quality, well-treated staff is essential to ITS operations and personnel retention. *Priority Categories: ID.AM, ID.BE, ID.GV, PR.AT, RC.CO, RC.IM, DE.AE, DE.CM*
7. Enhance the integration and connectivity of the transportation system through technology	The evolving nature of ITS capabilities and technology is dependent upon continuous improvements to technology to support safety and efficiency. This may include introducing new technologies to existing infrastructure. ITS operations deploying new technologies must consider interoperability requirements (whenever possible) to ensure existing and new technologies can effectively communicate. Successful integration improves the speed and availability of real-time notifications and communications. Once integrated, technologies should be maintained on an ongoing basis and measures should be put in place to ensure communications remain secure. *Priority Categories: ID.AM, ID.BE, ID.RA, ID.SC, PR.MA, PR.IP, PR.PT, DE.AE, DE.CM, RS.RP, RS.CO, RC.RP, RC.IM*
8. Build privacy protections into ITS operations[37]	ITS data can reveal travel patterns, health and mobility conditions, demographics, financial information, and other sensitive information about individuals. Agencies identify their role and the impacts of their data processing activities in the ITS ecosystem. ITS operations manage privacy risk to individuals as an integrated component of risk management throughout all aspects of the ITS and consider the needs of individuals, as

[37] See Appendix B for discussion regarding the relationship between cybersecurity and privacy and examples of privacy concepts that are relevant to ITS.

Mission Objective and Priority	Mission Objective Description
	well as the safeguards and limitations of individual informed consent, when performing ITS functions. Prioritizing privacy while developing ITS operations can help mitigate risks to individuals, manage reputational and financial risk for ITS operations, and help set expectations for vendors, operators, and customers for processing ITS data. Effectively managing risk maintains trust and facilities continued participation in ITS operations. *Priority Categories: ID.GV, PR.DS, DE.CM, RS.MI*
9. Prepare for and manage environmental risks to ITS operations	An effective transportation ecosystem balances mobility and safety with the environment. In ITS operations, efficiency and managing environmental risks are complementary objectives as ITS evolves to promote sustainable travel measures (e.g., eco-traffic signal timing/metering, management of HOT/HOV lanes, emissions monitoring) and minimize harm to safety or environmental impacts. Complying with environmental laws and regulations when performing activities (e.g., traffic management maintenance, using transit modes to move goods or people, building infrastructure or facilities) and coordination with environmental experts is part of understanding applicable requirements which, in addition to helping mitigate potential harms, can also minimize project delays or additional costs. During adverse conditions or events, ITS operations can reduce potential harm by incorporating environmental considerations in their incident management and response capabilities (e.g., HAZMAT tracking). *Priority Categories: ID.AM, ID.BE, ID.GV, ID.RA, ID.RM, PR.AT, RS.RP, RC.RP, RC.IM*
10. Maintain secure technology (IT/OT) and communications	ITS is an integrated system of IT and OT designed to provide safe and secure infrastructure. Because of the safety-critical nature of ITS, all IT, OT, and data must be secured using available security features (technologically and resource-wise) while providing timely information. Communications security must use the latest recommended security features. *Priority Categories: ID.AM, PR.IP, PR.DS, PR.MA, PR.PT, DE.CM, RS.RP, RS.MI, RC.RP, RC.IM*
11. Enhance telecommunications and networking to facilitate emerging ITS capabilities	Distribution of ITS information may depend on communications through wired and wireless telecommunications systems and networks (e.g., Wi-Fi, Vehicle to Everything [V2X], Fiber-Optic). Due to the safety-critical and sensitive nature of certain ITS information, it is important to implement safeguards as new attack vectors arise. These telecommunications systems should use currently recommended communications security at the device and network level for vehicle and transit-based systems. *Priority Categories: ID.AM, PR.IP, PR.PT, RS.RP, RC.RP, RC.IM*
12. Promote and provide equitable and accessible services	Transportation services must be accessible and available for all communities, regardless of geography, income level, language proficiencies, disabilities, or race, to receive predictable and reliable services in an equitable manner. Public transportation must be cost-

Mission Objective and Priority	Mission Objective Description
	effective to the public with various payment methods available to support the payment types and needs of all customers. Equitable access includes providing the public with statuses of transportation modes, costs, and scheduling that may inform their travel decisions. Providing equitable and accessible services allows for economic growth, helps mitigate social disadvantage, and enables efficient use of transportation services. *Priority Categories: ID.AM, ID.BE, ID.GV, PR.AT, PR.MA, DE.AE, DE.CM, RC.CO, RC.IM*
13. Engage with the community and relevant stakeholders	To facilitate the broadest cooperation, information dissemination, and feedback between users and providers, it is important ITS providers be engaged with the community (e.g., users of transportation) and stakeholders. This may also provide opportunities to engage a diverse range of people and communities to be involved and represented in decisions that impact them. Stakeholder cooperation may be local, regional, national, or international. Effectively and consistently communicating with communities and stakeholders may be helpful to understand ongoing demands and address barriers to ITS capabilities and information. *Priority Categories: ID.BE. ID.GV, PR.AT, PR.PT, DE.CM, RS.CO, RC.IM, RC.CO*
14. Facilitate and secure financial transactions[38]	Financial transactions and fare payments can occur directly from vehicles and end user devices (e.g., real-time authorizations, mobile payments). Because financial transactions can present significant privacy and cybersecurity risks, deliberate steps are needed to protect personal information, financial information, and locational information during these transactions. Agencies must work to ensure these transactions are secure to maintain trust and avoid negative operational impact (e.g., theft, attacks on the financial system, reduced ridership, fare evasion). Securing financial transactions and managing fare payments can rely on factors such as: supply chain needs, contractual agreements with third-party partners, or privacy-preserving architecture. *Priority Categories: ID.AM, ID.GV, ID.SC, PR.DS, RS.MI, RC.IM*
This CSF Profile only addresses cybersecurity aspects of these 14 Mission Objectives. ITS programs can use the Privacy Framework to address the privacy aspects of these same Mission Objectives. For discussion regarding the relationship between cybersecurity and privacy and examples of privacy concepts that are relevant to ITS, see Appendix B.	

[38] Organizations that handle financial transactions and fare payments may find use in the Cyber Risk Institute (CRI) Profile v1.2.1, which provides a benchmark for cybersecurity and resiliency for the Financial Services industry. The v.1.2.1 Diagnostics tab may offer guidance by providing Financial Service References to help with implementation. Please note that Diagnostic Statements, though similar, do not completely align to CSF v1.1 Subcategories. See: https://cyberriskinstitute.org/the-profile/

Chapter 7. ITS Profile: Priority Subcategories by Mission Objective

Users of the ITS Profile working to improve the security of the ITS ecosystem should conduct activities in support of all applicable NIST CSF Subcategories. This Profile recognizes and specifies a subset of those CSF Subcategories to help agencies prioritize cybersecurity risk mitigations and identify gaps. The NCCoE team reviewed inputs from the stakeholder workshops (e.g., prioritized and supporting Categories, Category selection discussions) to inform Subcategory Prioritization.

This Profile is intended to serve most of the transportation sector's needs and, as such, can be adapted by ITS agencies or programs to fit their capabilities and priorities. Those consulting this document should, as appropriate or necessary, emphasize the importance of Subcategories reflecting the unique needs of their agencies.

7.1 Subcategory Priority Chart

This section presents the results of analyzing stakeholders' Category prioritization and related discussions and applying their input to prioritize the selection of the CSF Subcategories for each Mission Objective. **Table 3** through **Table 7** summarize the information, providing the relative importance of each Subcategory to each MO, to demonstrate the criticality of certain Subcategories in supporting an MO's cybersecurity needs.

A Subcategory's priority is indicated in each Table by:

- **Three dots (●●●) for High Priority:** These represent the most critical Subcategories for enabling an MO that should be addressed most immediately given available resources.
- **Two dots (●●) for Moderate Priority:** The MO has a dependency on the Subcategory, but it is not as critical as High Priority Subcategories. They should be the next priority after implementing High Priority Subcategories and may become a higher priority in certain contexts or environments.
- **One dot (●) for Other Priority:** Subcategories important to the overall cybersecurity of an MO but may not require the same level of urgency as higher priority Subcategories. Note that "Other Priority" does not equate to low priority. All CSF Subcategories should receive consideration by an organization.

Although organizations should develop cybersecurity strategies that address all CSF Subcategories, the prioritization provides adaptable guidance suggesting cybersecurity capabilities that will provide the greatest impact toward meeting Mission Objectives for organizations in the ITS ecosystem.

Some ITS activities can introduce privacy risks that must be considered and are not addressed by implementing cybersecurity Subcategories. The following MOs have additional privacy risks ITS programs will need to consider:

- **MO 3: Collect, manage, use, and disseminate data:** Management of privacy risks to the individual is critical given the types of data (e.g., names, vehicle information, financial information, login identification, and general location information) processed across the ecosystem.
- **MO 8: Build privacy protections into ITS operations:** ITS operations can strengthen their risk management processes and activities, as well as relationships with their stakeholders (e.g., customers, vendors) by accounting for and addressing privacy risks in their operations.[39]
- **MO 13: Engage with the community and relevant stakeholders:** Customer service and engagement activities require processing data about individuals and customers. Agencies need to consider privacy risks throughout all data processing activities, such as managing data use or retention periods with respect to the individual's consent or preference.
- **MO 14: Facilitate and secure financial transactions:** Financial transactions and fare payments present privacy risks due to the information collected and used between end-users' devices and vehicles.

Reviewing the NIST Privacy Framework Subcategories and identifying those that support these MOs, as well as other organization-specific MOs that may warrant privacy considerations, is beneficial to enhancing an agency's cybersecurity and privacy posture. [40] Cybersecurity and privacy practitioners should coordinate when determining how to best apply this Profile within their organization.

[39] See Appendix B for a discussion on ITS programs and privacy risk management.

[40] See Appendix B for a discussion regarding the relationship between cybersecurity and privacy.

Table 3: Identify (ID) Function Subcategory Priorities

IDENTIFY (ID) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	**Subcategory**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	●●●	●●●	●●	●●●	●	●	●●●	●●	●●●	●●●	●●●	●●●	●	●●●
	ID.AM-2: Software platforms and applications within the organization are inventoried	●●●	●●●	●●	●●●	●●	●	●●●	●●	●●●	●●●	●●●	●●●	●	●●●
	ID.AM-3: Organizational communication and data flows are mapped	●●	●●●	●●●	●●	●	●●	●●	●	●	●●●	●●●	●●●	●	●●
	ID.AM-4: External information systems are catalogued	●	●●	●●	●●	●●	●	●●●	●●●	●	●●	●●●	●	●	●●●
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	●●	●●	●●	●●●	●●	●●●	●●●	●	●●●	●●●	●●●	●●●	●	●●
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	●●	●●	●●	●●	●●	●●●	●●	●●●	●●	●●●	●●●	●	●	●●●
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	●	●	●●	●●	●	●	●●●	●●●	●	●	●	●	●●	●
	ID.BE-2: The organization's place in critical infrastructure and its	●●	●●	●	●	●●	●	●●	●	●●	●	●	●	●●	●

IDENTIFY (ID) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	**Subcategory**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	industry sector is identified and communicated														
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	●●●	●	●	●●●	●●	●●●	●●●	●●	●●●	●●	●	●●	●●●	●
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	●●●	●●	●	●●●	●	●●	●●●	●	●●	●●	●	●●●	●●	●
	ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)	●●●	●●●	●	●●●	●	●●	●●	●	●	●●●	●	●●●	●●	●
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information cybersecurity policy is established and communicated	●●	●	●●	●	●●	●●	●	●●●	●	●●●	●	●●	●●	●●
	ID.GV-2: Cybersecurity roles & responsibilities are coordinated and aligned with internal roles and external partners	●●	●●	●●	●	●●●	●●●	●	●●●	●●	●	●	●	●●●	●●●
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	●●	●●●	●●●	●	●●●	●●●	●	●●●	●●●	●●	●	●●●	●●●	●●●

IDENTIFY (ID) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	**Subcategory**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
	ID.GV-4: Governance and risk management processes address cybersecurity risks	●●	●●	●●●	●	●●●	●	●	●●●	●	●●●	●	●	●	●●
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	●●	●	●●●	●	●●	●	●●●	●	●●●	●	●	●	●	●
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	●	●	●●	●	●●	●	●●	●	●	●	●	●	●	●
	ID.RA-3: Threats, both internal and external, are identified and documented	●●	●	●●	●	●	●	●●●	●	●●●	●	●	●	●	●
	ID.RA-4: Potential business impacts and likelihoods are identified	●●●	●●	●●●	●	●●	●	●●●	●●●	●●●	●	●	●●	●●	●
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	●●●	●●	●●●	●	●●	●	●●●	●●●	●●●	●	●	●●	●	●
	ID.RA-6: Risk responses are identified and prioritized	●●●	●	●●	●	●●	●	●●	●●●	●●●	●	●	●●	●	●
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	●●●	●	●	●	●	●	●	●	●●	●	●	●●●	●●	●
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	●●	●	●	●	●	●	●	●	●●	●	●	●	●	●
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical	●●	●	●●	●	●●	●	●	●●	●●●	●	●	●●●	●	●

IDENTIFY (ID) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	**Subcategory**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
	infrastructure and sector specific risk analysis														
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	●●●	●	●●●	●●●	●	●	●●●	●●	●	●	●	●	●	●●●
	ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	●●●	●	●●●	●●●	●	●	●●	●●	●	●	●	●	●	●●●
	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan	●●●	●	●●●	●●●	●	●	●●	●●	●	●	●	●	●	●●●
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations	●●●	●	●●	●●	●	●	●●	●	●	●	●	●	●	●●
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	●●	●	●●	●●	●	●	●	●	●	●	●	●	●	●●

Table 4: Protect (PR) Function Subcategory Priorities

PROTECT (PR) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	**Subcategory**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices users, and processes	●●	●	●●●	●	●	●	●●●	●●●	●	●●●	●	●	●	●●●
	PR.AC-2: Physical access to assets is managed and protected	●●	●	●●	●	●	●	●	●	●	●●●	●	●	●	●●●
	PR.AC-3: Remote access is managed	●	●	●●●	●	●	●	●●●	●●	●	●●	●	●	●	●●●
	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	●	●	●●●	●	●	●	●●●	●●●	●	●	●	●	●	●●●
	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	●●	●	●●●	●	●	●	●●●	●●●	●	●●●	●	●	●	●●●
	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	●	●	●●	●	●	●	●●	●●	●	●	●●	●	●	●●
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks, and	●	●	●●	●	●	●	●●●	●●●	●	●●●	●	●	●	●●●

PROTECT (PR) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	Subcategory	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	other organizational risks)														
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	●●●	●●●	●	●	●●	●●●	●	●●●	●●●	●	●	●●●	●●	●
	PR.AT-2: Privileged users understand roles and responsibilities	●	●	●	●	●●	●●●	●	●	●	●	●	●	●	●
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities	●●●	●●●	●●	●	●●	●●	●	●●	●●●	●	●	●●	●●	●
	PR.AT-4: Senior executives understand roles and responsibilities	●●	●●●	●	●	●●	●●	●	●●	●●●	●	●	●●●	●●●	●
	PR.AT-5: Physical and information security personnel understand roles and responsibilities	●	●	●	●	●●	●●●	●	●	●	●	●	●●	●	●
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	●	●	●●●	●	●	●	●	●●●	●	●●●	●●●	●	●	●●●
	PR.DS-2: Data-in-transit is protected	●	●	●●●	●	●	●	●	●●●	●	●●●	●●●	●	●	●●●
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	●	●	●	●	●	●	●	●●●	●	●	●	●	●	●●
	PR.DS-4: Adequate capacity to ensure availability is maintained	●●●	●	●●	●	●	●	●	●●	●	●●	●●	●	●	●●●
	PR.DS-5: Protections against data leaks are implemented	●	●	●●	●	●	●	●	●●●	●	●	●	●	●	●●
	PR.DS-6: Integrity checking mechanisms are used to verify	●●	●	●●	●	●	●	●	●●	●	●●	●●●	●	●	●●

PROTECT (PR) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	**Subcategory**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
	software, firmware, and information integrity														
	PR.DS-7: The development and testing environment(s) are separate from the production environment	●	●	●	●	●	●	●	●●	●	●	●●	●	●	●●
	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	●●	●	●	●	●	●	●	●●	●	●●	●●	●	●	●●
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	●●	●●	●●	●	●	●	●●●	●	●	●●●	●●●	●	●	●
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	●	●	●●	●	●	●	●●●	●●	●	●●	●●	●	●	●
	PR.IP-3: Configuration change control processes are in place	●	●●	●	●	●●	●	●●●	●	●	●●●	●●●	●	●	●
	PR.IP-4: Backups of information are conducted, maintained, and tested	●	●●	●●●	●	●	●	●	●	●	●	●●	●	●	●
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	●●	●●	●	●	●●	●	●●	●	●	●●	●	●	●	●
	PR.IP-6: Data is destroyed according to policy	●	●	●●	●	●	●	●	●●	●	●	●	●	●	●

PROTECT (PR) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	**Subcategory**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
	PR.IP-7: Protection processes are improved	●●	●	●	●	●●●	●	●●	●	●	●●	●●	●	●	●
	PR.IP-8: Effectiveness of protection technologies is shared	●	●	●	●	●●	●	●	●	●	●	●	●	●	●
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	●●●	●●●	●●	●	●●	●	●●●	●	●	●●	●●●	●	●	●
	PR.IP-10: Response and recovery plans are tested	●●●	●●●	●●	●	●	●	●	●	●	●	●●	●	●	●
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	●	●	●	●	●	●	●	●	●	●	●●	●	●	●
	PR.IP-12: A vulnerability management plan is developed and implemented	●●	●	●●	●	●	●	●●	●	●	●●	●●	●	●	●
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	●●●	●●●	●	●●●	●	●	●●●	●	●	●●●	●	●●●	●	●
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	●	●	●	●●●	●	●	●●	●	●	●●●	●	●	●	●

PROTECT (PR) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	**Subcategory**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, are consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	●●	●	●●●	●	●	●	●●	●	●	●●	●●●	●	●	●
	PR.PT-2: Removable media is protected and its use restricted according to policy	●	●	●●	●	●	●	●●	●	●	●	●●●	●	●	●
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	●	●	●●	●	●	●	●●	●	●	●	●●	●	●	●
	PR.PT-4: Communications and control networks are protected	●●	●●●	●●●	●	●	●	●●●	●	●	●●●	●●●	●	●●●	●
	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	●●●	●●●	●●●	●	●	●	●●●	●	●	●●	●●●	●	●●	●

Table 5: Detect (DE) Function Subcategory Priorities

DETECT (DE) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	Subcategory	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	●●	●●●	●	●●●	●	●●	●●●	●	●	●	●	●●	●	●
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	●	●	●	●●	●	●●	●●	●	●	●	●	●	●	●
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors	●	●	●	●●	●	●	●●	●	●	●	●	●●●	●	●
	DE.AE-4: Impact of events is determined	●●●	●●	●	●●●	●	●●	●●	●	●	●	●	●●●	●	●
	DE.AE-5: Incident alert thresholds are established	●●	●●	●	●●	●	●	●●	●	●	●	●	●●	●	●
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	●●●	●●	●	●●●	●	●●	●●●	●●●	●	●●●	●	●●	●	●
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	●●	●●	●	●●●	●	●	●●	●●	●	●●	●	●●	●	●
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	●	●	●	●●●	●	●●	●●	●●	●	●●	●	●	●	●
	DE.CM-4: Malicious code is detected	●●	●	●	●●	●	●	●●	●	●●●	●	●	●	●	●
	DE.CM-5: Unauthorized mobile code is detected	●	●	●	●	●	●	●	●	●	●	●	●	●	●

DETECT (DE) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	**Subcategory**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	●	●	●	●●	●	●●	●●●	●●●	●●	●	●	●	●	●
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	●●	●	●	●●	●	●	●●●	●●●	●●	●	●	●	●	●
	DE.CM-8: Vulnerability scans are performed	●●	●	●	●●	●	●	●●	●●●	●●	●	●	●●	●	●
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	●●	●	●	●	●	●	●	●	●	●	●	●	●	●
	DE.DP-2: Detection activities comply with all applicable requirements	●●	●	●	●	●	●	●	●	●	●	●	●	●	●
	DE.DP-3: Detection processes are tested	●●	●	●	●	●	●	●	●	●	●	●	●	●	●
	DE.DP-4: Event detection information is communicated	●●	●	●	●	●	●	●	●●	●	●	●	●	●	●
	DE.DP-5: Detection processes are continuously improved	●●	●	●	●	●	●	●	●	●	●	●	●	●	●

Table 6: Respond (RS) Function Subcategory Priorities

RESPOND (RS) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	**Subcategory**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	●●●	●	●●●	●●●	●●	●●	●●●	●	●●●	●●●	●●●	●	●	●
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	●●●	●●●	●●●	●	●	●	●●●	●	●●●	●●●	●	●	●●●	●
	RS.CO-2: Incidents are reported consistent with established criteria	●●●	●●	●●	●	●	●	●●	●	●●	●●●	●	●	●●	●
	RS.CO-3: Information is shared, consistent with response plans	●●	●●	●●	●	●	●	●●	●●	●●	●●	●	●	●●●	●
	RS.CO-4: Coordination with stakeholders occurs, consistent with response plans	●●●	●●●	●●●	●	●●	●	●●●	●●	●●●	●●●	●	●	●●●	●
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	●●	●	●●	●	●●	●	●	●	●	●●	●	●●	●●●	●
Analysis (RS.AN): Analysis is conducted to ensure adequate response	**RS.AN-1:** Notifications from detection systems are investigated	●●●	●●●	●	●	●	●	●	●	●	●	●	●	●	●
	RS.AN-2: The impact of the incident is understood	●●●	●●●	●	●	●	●	●	●	●	●	●	●	●	●

RESPOND (RS) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	**Subcategory**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
and support recovery activities.	**RS.AN-3:** Forensics are performed	●●	●	●	●	●	●	●	●	●	●	●	●	●	●
	RS.AN-4: Incidents are categorized, consistent with response plans	●●	●●	●	●	●	●	●	●	●	●	●	●	●	●
	RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers)	●●●	●	●	●	●	●	●	●	●	●	●	●	●	●
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	●●●	●	●	●	●	●	●	●●●	●	●●●	●	●	●	●●●
	RS.MI-2: Incidents are mitigated	●●●	●	●	●	●	●	●	●●●	●	●●●	●	●	●	●●●
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	●●●	●	●	●	●●	●	●	●●	●	●●	●	●	●	●●●
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	●●●	●	●	●●●	●●	●	●	●	●	●●	●	●	●	●
	RS.IM-2: Response strategies are updated	●●	●	●	●●	●	●	●	●	●	●	●	●	●	●

Table 7: Recover (RC) Function Subcategory Priorities

RECOVER (RC) Function		Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Priorities													
Category	Subcategory	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after cybersecurity incident	●●●	●	●●●	●●●	●●	●	●●●	●	●●●	●●●	●●●	●	●	●
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	●●●	●	●●●	●●●	●●	●●	●	●	●●	●●	●●	●	●	●
	RC.IM-2: Recovery strategies are updated	●●	●	●●	●●	●	●	●	●	●●●	●●	●	●●	●	●
Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	●●	●	●	●	●	●●●	●	●●●	●●	●	●	●	●●●	●
	RC.CO-2: Reputation after an event is repaired	●●	●	●	●	●	●●●	●	●	●●	●	●	●●●	●●●	●
	RC.CO-3: Recovery activities are communicated to internal and external stakeholders and executive and management teams	●●●	●●	●	●	●	●	●	●	●●●	●	●	●●●	●●●	●

Chapter 8. References and Resources

8.1 References

Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT):

https://www.arc-it.net/index.html

ARC-IT Objectives:

https://www.arc-it.net/html/archuse/objectives.html

Connected Vehicle Environments CSF Profile:

https://www.its.dot.gov/research_areas/cybersecurity/docs/1_How_to_Use_the_CSF_Profile_for_CVE.pdf

Cyber Risk Institute Profile:

https://cyberriskinstitute.org/the-profile/

Cybersecurity & Infrastructure Security Agency Transportation Systems Infrastructure:

https://www.cisa.gov/transportation-systems-sector

History of Intelligent Transportation Systems (2021 Update):

https://its.dot.gov/history/pdf/HistoryofITS_book.pdfv

Intelligent Transportation Systems Joint Program Office: Connected Vehicle Pilot Deployment Program:

https://www.its.dot.gov/pilots/overview.htm

Intelligent Transportation Systems Joint Program Office: ITS Frequently Asked Questions:

https://its.dot.gov/about/faqs.htm#deploy

Intelligent Transportation Systems Joint Program Office: ITS Research 2015-2019 Connected Vehicles:

https://www.its.dot.gov/research_archives/connected_vehicle/connected_vehicle.htm

Intelligent Transportation Systems Joint Program Office Strategic Plan 2020-2025:

https://its.dot.gov/stratplan2020/ITSJPO_StrategicPlan_2020-2025.pdf

ITS America 2023-2026 Strategic Plan:

https://itsa.org/wp-content/uploads/2023/01/2026-ITS-America-Strategic-Plan.pdf

ITS Deployment Evaluation: Benefits Areas:

http://www.itskrs.its.dot.gov/benefits

National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*:

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST Catalog of Problematic Data Actions and Problems:

https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM/catalog-PDAP.md

NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*:

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST Special Publication 1271, *Getting Started with the NIST Cybersecurity Framework*:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271.pdf

The Framework for Improving Critical Infrastructure Cybersecurity Presentation:

https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview

U.S. Department of Transportation History of Intelligent Transportation Systems 2021 Update (Publication Number: FHWA-JPO-16-329):

https://its.dot.gov/history/pdf/HistoryofITS_book.pdf

U.S. Department of Transportation Strategic Plan:

https://www.transit.dot.gov/sites/fta.dot.gov/files/tro3_strategic_plan.pdf

23 CFR 450:

https://www.ecfr.gov/current/title-23/chapter-I/subchapter-E/part-450/subpart-B

Washington State Department of Transportation Strategic Plan:

https://wsdot.wa.gov/about/secretary-transportation/strategic-plan

8.2 Resources

Cyber Risk Institute Profile v1.2.1:

The Cyber Risk Institute (CRI) Profile provides the financial services industry (e.g., financial institutions, financial services companies, financial firms) with a benchmark for cybersecurity and resiliency through Diagnostic Statements. Organizations managing financial transactions or handling financial data may find guidance in the v.1.2.1 Diagnostics tab of the Profile (with Financial Services References) and accompanying Profile Workbook for interpretive guidance of the Diagnostic Statements. Please note the CRI Profile does not completely map to the CSF v1.1 used for the ITS Profile. Diagnostic Statements for implementation may not fully align to the Subcategories prioritized in the ITS Profile. The CRI Profile reviews seven over-arching functions in comparison to the CSF's five. Therefore, using the CRI Profile spreadsheet will differ from implementing the ITS Profile.

https://cyberriskinstitute.org/the-profile/

ITS JPO Resources:

The ITS JPO site provides additional resources to provide context on ITS, ITS deployment, and other relevant information. In general, the ITS JPO site offers information that can benefit the ITS community seeking information on the latest ITS research, development, and implementation news.

https://www.its.dot.gov/resources.htm

NIST CSF Risk Management Resources:

The NIST CSF site offers a listing of publicly available Framework resources to assist in Risk Management activities. Resources include, but are not limited to approaches, methodologies, implementation guides, mappings to the Framework, case studies, educational materials, Internet resource centers (e.g., blogs, document stores), example profiles, and other Framework document templates.

https://www.nist.gov/cyberframework/resources/risk-management-resources

Privacy Workforce Public Working Group:

The Privacy Workforce Public Working Group provides a forum for participants to contribute to the development of the NIST Privacy Workforce taxonomy. The Working Group will create Task, Knowledge, and Skill Statements aligned with the NIST Privacy Framework and the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.

https://niccs.cisa.gov/workforce-development/nice-framework

Workforce Framework for Cybersecurity (NICE Framework):

The NICE Framework help employers develop their cybersecurity workforce by providing a common language to describe common cybersecurity functions (Categories), distinct areas of cybersecurity work (Specialty Areas), and groupings of requirements to perform a Work Role (Work Roles).

https://niccs.cisa.gov/workforce-development/nice-framework

Appendix A. Acronyms and Abbreviations

ARC-IT	**Architecture Reference for Cooperative and Intelligent Transportation**
C2C	**Center-to-Center**
C2F	**Center-to-Field**
CIO	**Chief Information Officer**
CPRT	**NIST Cybersecurity and Privacy Reference Tool**
CRI	**Cyber Risk Institute**
CV	**Connected Vehicle**
CVE Profile	**Connected Vehicle Environment Profile**
CSF	**Cybersecurity Framework**
HAZMAT	**Hazardous Material**
HIPAA	**Health Insurance Portability and Accountability Act**
ISAC	**Information Sharing and Analysis Centers**
IT	**Information Technology**
ITS	**Intelligent Transportation Systems**
ITS JPO	**Intelligent Transportation Systems Joint Program Office**
MO	**Mission Objective**
NCCoE	**National Cybersecurity Center of Excellence**
NICE	**National Initiative for Cybersecurity Education**
NIST	**National Institute of Standards and Technology**
NTCIP	**National Transportation Communications for ITS Protocol**
OT	**Operational Technology**

PHI	**Protected Health Information**
TIC	**Traffic Information Center**
TMC	**Traffic Management Center**
TMDD	**Traffic Management Data Dictionary**
USDOT	**United States Department of Transportation**
V2X	**Vehicle to Everything**

Appendix B. Cybersecurity and Privacy Risk Relationship

Relationship Between Cybersecurity and Privacy Risk Management

Cybersecurity and privacy are independent and separate disciplines. However, as shown by the Venn diagram in **Figure 4,** some of their objectives overlap and are complementary. Cybersecurity programs are responsible for protecting information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized system activity or behavior) to provide confidentiality, integrity, and availability, as well as ensuring organizations comply with applicable cybersecurity requirements. Privacy programs are responsible for managing the risks to individuals associated with data processing throughout the information lifecycle[41] to provide predictability, manageability, and disassociability[42] as well as ensuring agencies comply with applicable privacy requirements. **Figure 4**, from the NIST Privacy Framework, illustrates this relationship between cybersecurity and privacy risks, showing both where they overlap and where they are distinct.

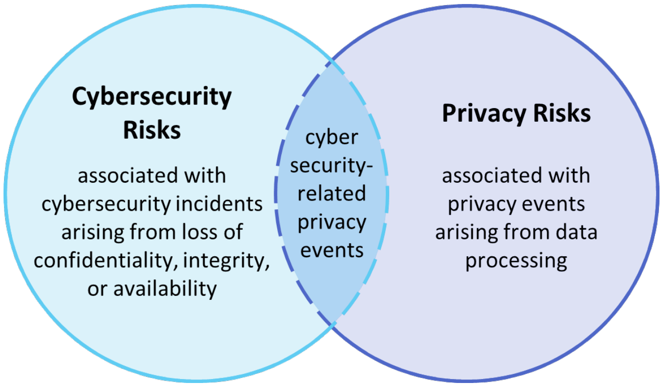

Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing

Figure 4: Cybersecurity and Privacy Risk Relationship

While the overlap between cybersecurity and privacy risk management is important, the distinction between the two is critical to understand. Managing cybersecurity risk contributes to managing privacy

[41] The information lifecycle includes creation, collection, use, processing, dissemination, storage, maintenance, disclosure, or disposal (collectively referred to as "processing") of data that may impact privacy.

[42] Definitions for predictability, manageability, and disassociability, which are privacy engineering objectives, can be found in the NIST Privacy Framework.

risk (i.e., controlling access to data protects against privacy breaches by limiting who can access the data and the actions they can perform), but managing cybersecurity risk alone is not sufficient, as permitted data processing activities can introduce privacy risks unrelated to cybersecurity incidents. Some data processing activities and technologies inherently introduce privacy risk but may be necessary for valid business purposes. These privacy risks must be managed when they arise. For example, some transportation agencies transport individuals from their home to medical appointments. While this is a critical service for individuals who need help traveling to receive healthcare, there is a degree of exposure regarding individuals' health condition. This does not mean the service should not be provided, rather, it means when this capability is provided, agencies must be aware of and manage the privacy risk introduced accordingly.

This Profile only addresses privacy considerations in the overlap section of the **Figure 4** Venn diagram. There are many privacy activities and outcomes in the remainder of the privacy circle outside of the scope of the CSF. For example, considering contextual factors that influence data processing in systems, products, and services. Understanding the different origins of cybersecurity and privacy risks enables ITS programs to effectively manage privacy risks in the ITS systems and services they design. NIST developed both the Cybersecurity Framework and the NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0 ("Privacy Framework") to help organizations, including ITS operations, manage cybersecurity and privacy risk. These two frameworks work together and share some content where the needs of cybersecurity and privacy overlap.

In addition to the cybersecurity focused ITS Profile, practitioners should also review the NIST Privacy Framework for additional Subcategories which may benefit their programs and the individuals they serve.

Privacy Risk Management Overview

Privacy risk can impact individuals and organizations, including ITS programs. Managing privacy risks requires ITS operations to understand and apply privacy risk management concepts. Members of the ITS community in roles that can impact privacy, should also have a clear understanding of how to identify and address privacy risk that may arise during the performance of their role(s).

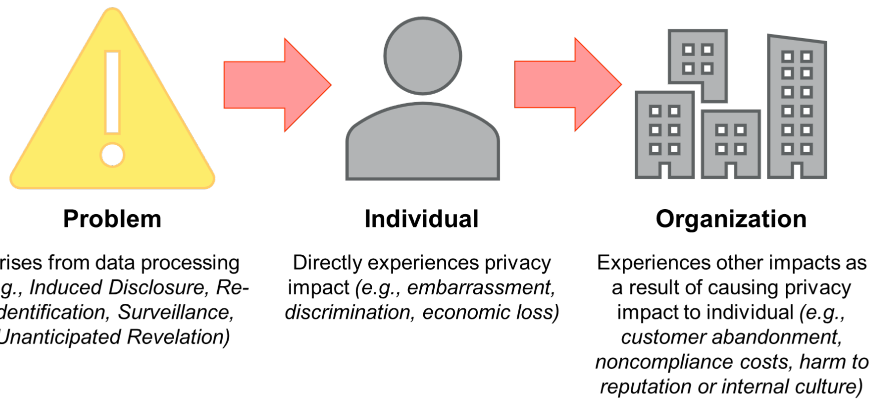
The NIST Privacy Framework is a tool to help organizations manage privacy risk. Just as ITS programs consider the risks associated with cybersecurity incidents, they should also consider privacy events (i.e., the occurrence or potential occurrence of problematic data actions[43]). Privacy events can occur at any point throughout the information lifecycle from data collection to data disposal. Privacy events that occur at an organization or in a system can lead to a variety of potential privacy problems individuals experience. The NIST Privacy Framework describes privacy problems as ranging from dignity type effects (e.g., embarrassment or stigmas) to more tangible harms (e.g., discrimination, economic loss, or physical harm).[44] Privacy problems can arise from an individual's direct use of an ITS capability. Some problems

[43] A problematic data action is a data action or data processing activity that could cause an adverse effect for individuals.

[44] NIST published the Catalog of Problematic Data Actions and Problems to provide that help practitioners understand and label the ways data processing activities can impact privacy ("problematic data actions") and examples of problems that individuals could experience as the result. The Catalog is available at: https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM/catalog-PDAP.md

can also arise simply from individuals’ interactions with ITS systems, products, and services, even when the data being processed is not directly linked to identifiable individuals.

ITS operations may experience impacts that are a result of its role in contributing to privacy risks to individuals, such as noncompliance costs, revenue loss arising from customer abandonment of products and services, or harm to its external reputation or internal culture because of the privacy problems individuals experience. Organizations and programs typically manage these types of program impacts at the enterprise risk management level; by connecting problems individuals experience to these well-understood organizational impacts, organizations can bring privacy risk into parity with other risks they manage in their broader portfolio and drive more informed decision-making about resource allocation to strengthen privacy programs. **Figure 5** illustrates this relationship between privacy risk and organizational risk.



Problem

Arises from data processing *(e.g., Induced Disclosure, Re-identification, Surveillance, Unanticipated Revelation)*

Individual

Directly experiences privacy impact *(e.g., embarrassment, discrimination, economic loss)*

Organization

Experiences other impacts as a result of causing privacy impact to individual *(e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)*

Figure 5: Relationship Between Privacy Risk and Organizational Risk[45]

Cybersecurity and Privacy Risk Management for ITS Data

Understanding the different origins of cybersecurity and privacy risks enables ITS programs to effectively manage both areas of risks in the systems and services they design. NIST developed both the Cybersecurity Framework and the Privacy Framework to help organizations manage cybersecurity and privacy risk. These two frameworks work together and share some content where cybersecurity and privacy needs overlap.

In addition to applying the cybersecurity-focused ITS Profile, ITS practitioners should review the NIST Privacy Framework for additional Subcategories that may benefit their programs and the individuals they serve.

[45] Adapted from NIST Privacy Framework, Figure 3, Catalog of Problematic Data Actions and Problems.

Additional Considerations for Mission Objective 8

To be most effective, privacy should be part of ITS operations from inception. Mission Objective 8, “Build privacy protections into ITS operations,” encourages this.

Privacy is implemented through policy, processes, system design, and implemented components, leading to trust (actual and perceived) in the systems and services offered, which ultimately supports continued participation. While appropriate security safeguards are implemented to protect against loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of ITS data, ITS programs consider the full scope of privacy risks (see **Figure 4**). Privacy risks are considered throughout the data processing lifecycle. System functions and data processing activities are aligned for operating ITS systems. Privacy practices are thoroughly documented and understood by all agencies involved in operating ITS systems and processing the data generated by them. Effectively managing privacy risk maintains trust and facilitates continued participation in ITS programs.

Appendix C. Subcategory Priority Considerations

This appendix provides implementation considerations derived from the Subcategory priority discussions that produced the dot charts (see **Chapter 7.1 Table 3** through **Table 7**). Implementation considerations offer industry context and guidance about how a Subcategory and its respective priority applies in the ITS ecosystem. The considerations in **Table 8** summarize the discussion across all Mission Objectives that prioritized a Subcategory as High Priority (represented as 3 dots ●●● in **Table 3** through **Table 7** above) or Moderate Priority (represented as 2 dots ●● in **Table 3** through **Table 7** above). All other Subcategories are notated with "Not identified as High or Moderate. Agencies should review for considerations specific to their operating environment."

For MOs with a unique rationale for a Subcategory, in comparison to the generalized rationale for all Mission Objectives, a separate line item is included and labeled with the related MO(s). Subcategories mapped to NIST Privacy Framework Subcategories are referenced in certain MO Specific Considerations. Implementers can review the NIST CSF to NIST Privacy Framework crosswalk to identify Privacy Subcategories referenced and potential Privacy Subcategories to implement.[46] This information is provided to support Profile implementers in understanding the drivers behind prioritized Subcategories to inform their agency's use and any adaptations of the ITS Profile. As with dot priority assignments, Subcategory considerations captured reflect the ITS ecosystem at large. Those applying the Profile may find different systems, standards, or dependencies to consider depending on the agency's service area, resources, or priorities.

Table 8: Subcategory Priority Considerations

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
Identify	ID.AM-1	ITS assets, devices, and systems are involved in disseminating and collecting information. It is important to understand what physical and software assets present, what data exist on or are	1,2,3 – Can include sensors, roadside equipment (e.g., sensors, work zone systems, barrier and lane

[46] See the Cybersecurity Framework crosswalk (XLSX): https://www.nist.gov/privacy-framework/resource-repository/browse/crosswalks/cybersecurity-framework-crosswalk

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
		output from relevant systems, and who is involved in data handling and communications.	management systems), and emergency related equipment. 3,8 – Understanding where sensitive data exists is needed to know where to place protections. 4,9,10,11,12 – Aids in understanding maintenance and protections required or awareness if damage were to occur to systems.
	ID.AM-2	An inventory of software and applications supports managing those assets (e.g., applying updates, acquiring new systems, integration) as well as using and managing data (which can be sensitive).	1,2,3 – Often implemented as a web application service, Traffic Management Center (TMC) and Traffic Information Center (TIC) are responsible for consistent and reliable data dissemination. 5,6,7 – Can include systems that manage administrative processes (e.g., electronic driver logs, international border registration, human resource systems) or support consistent operations and interoperability.
	ID.AM-3	Understanding communication and data flows help agencies know where issues are in their operational systems if communication lapses occur.	1,9 – Public safety service areas are dependent on the availability of communication systems to respond to emergencies, incidents, or disasters. Communication systems are critical for interactions between emergency operation centers and public safety agencies.

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
			3,8,14 – Mapped Privacy Framework Subcategory, ID.IM-P8,[47] references data processing and roles, and interactions of individuals or third parties. Communication and data flows are critical to understanding the data processing environment and how ITS data is moving and changing state throughout the information lifecycle. 7 – Center-to-Center (C2C), Center-to-Field (C2F), and Services-to-Services need to be interoperable to aggregate data for situational awareness. C2C Standards and Protocols (e.g., Traffic Management Data Dictionary [TMDD], an information standard, and the National Transportation Communications for ITS Protocol [NTCIP]) can be leveraged to exchange meaningful ITS information.
	ID.AM-4	ITS operations can use many external equipment or systems. Cataloguing these systems facilitates an understanding of service and interoperability requirements, dependencies, and risks.	3 – Some systems of the TMC or Roadside equipment collecting information may be external. 6 – Systems that support human resource services, personnel, or administrative processes may be outsourced. 3,8,14 – There are additional privacy risks to consider when sensitive data is sent outside the agency. 11 – External systems (e.g., Google, Waze), and are systems that can provide real-time information for traffic,

[47] NIST Privacy Framework Subcategory ID.IM-P8 is “Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.” under the NIST Privacy Framework Category “Inventory and Mapping.” See NIST Privacy Framework at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
			weather, and payment processing systems. The responsibility to catalogue such systems can be shared with third-party providers or suppliers. 14 – Financial services may come from third party providers and ITS operations will need to know who is providing external financial transactions.
	ID.AM-5	Prioritizing assets supplements coordination required for addressing issues that may impact operations. Agencies will have a better understanding of critical systems, operations, and dependencies for supporting response.	
	ID.AM-6	Conducting ITS operations requires the coordination of many different agencies or stakeholders. Personnel need to be aware of their roles and responsibilities, and the impact on operations. Consider applying ID.GV-2 consistent with this Subcategory.	6 – Roles may need to be fulfilled by different technicians for each discipline (e.g., servers, networks, application, infrastructure). Technicians may not have experience writing security documentation or policy. Their role may be to manage assets and meet installation guidance provided. Consider dedicating roles for documentation and policy or providing additional training.
	ID.BE-1	An agency's role in the supply chain impacts the supply chain management, maintenance, and improvements required. This enhances the understanding of roles, risks, dependencies.	3,8,13 – Maps to the privacy notion of an agency knowing its role in the data processing ecosystem. An agency should consider what is happening before and after them during the data processing lifecycle and data supply chain. 13 – Managing data privacy (e.g., data minimization, retention) can be linked to customer service.

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
			7 – Can impact resiliency requirements in ID.BE-5. ID.BE-4 may be dependent on implementing this Subcategory.
	ID.BE-2	An agency's place in critical infrastructure needs to be identified and communicated within the agency and with stakeholders. Application of ID.RM-3 may be similar.	
	ID.BE-3	Prioritizing critical systems that support the organization sets the standard for what will be required of implementers and the community. ITS being integrated or used will seek to not only maintain but improve operations.	
	ID.BE-4	It is important to understand which systems or technologies are responsible for delivering critical services, their functions, and dependencies that may exist. Understanding dependencies and critical functions can inform resiliency requirements that should be established for ID.BE-5.	6 – Helps inform workforce training and ensuring those responsible for managing critical functions have the appropriate training and understand all requirements (e.g., licensing requirements to operate commercial vehicles, safety requirements for hazardous material [HAZMAT] transport). 7 – Can include understanding the new dependencies created by integrating new ITS and understanding potential loss or degradation of functions and their impacts.
	ID.BE-5	Improving resiliency of ITS is a priority within the industry and community due to the communications necessary among ITS stakeholders and real-time notification often	

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
		required. This Subcategory helps support providing the critical services established in ID.BE-4.	
	ID.GV-1	This Subcategory establishes what may need to be in place to support assets in place across the ITS ecosystem. Systems must remain up to date and cyber-aware to be able to respond to any issues or threats and have policies in place for maintenance of assets.	
	ID.GV-3	Agencies and personnel are aware and trained to communicate and adhere to the requirements and standards of regulations that exist to enhance ITS operations.	2 – Can include the laws and regulations around operator safety, speed limits, or movement of goods. Can factor into or have an impact on increasing efficiency or providing multiple modes to provide information (i.e., through connected means). 3,8,12,13,14 – Can include statutes and regulations related to data collection and privacy obligations. Requirements around handling data are evolving due to increasing complexity and interconnectedness. This Subcategory supports ITS programs with meeting minimum compliance requirements so they can continue to operate, which is part of an overall privacy risk management program.

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
	ID.GV-4	It is important organizations know and understand their risk tolerance and the risks within their assets or processes that could harm ITS operations.	3,8 – Maps to GV.PO-P6[48] in the NIST Privacy Framework. Addressing privacy risks requires understanding what data exists on ITS and addressing cybersecurity risks through governance and risk management policies, processes, and procedures.
	ID.RA-1	Vulnerabilities in inventoried assets under ID.AM increases risks to ITS operations (e.g., functionality of ITS, data). Identification of vulnerabilities can help determine impact to systems with dependencies. Supports implementation of ID.RA-5.	1 – Should be aware of potential vulnerabilities to safety critical systems to minimize impact. 3 – Increases risks to exposure of sensitive data, delays in disseminating data, control messages that are corrupted or modified. 9 – Consider physical assets such as vehicles using CV technologies that support low emissions zone management, HAZMAT vehicles. Also consider impacts of environmental conditions (e.g., natural disasters) that can affect assets.
	ID.RA-2, ID.RA-3	Supports implementation of ID.RA-5.	3 – Understand threats and impact to data - the more sources available, the more robust data protection can be. 5 – Controls may be based on Cyber Threat Intelligence from Information Sharing and Analysis Centers (ISAC). Infrastructure Owner Operators who run ITS products and Original Equipment Manufacturers who make ITS products may rely on this information. Source may come

[48] NIST Privacy Framework Subcategory GV.PO-P6 is "Governance and risk management policies, processes, and procedures address privacy risks." under the NIST Privacy Framework Category "Governance Policies, Processes, and Procedures." See NIST Privacy Framework at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
			from international border coordination and sharing information between agencies to support expedited clearance, customs processing, and inspections
	ID.RA-4	Supports implementation of ID.RA-5.	1,13 – Understand what could impact physical safety, as response to incidents can have an impact on the agency's image or reputation. If people in the ecosystem do not feel safe, this could have impact to transportation (e.g., usage, ridership, mobility). 3,8 – Critical to understanding how data use and dissemination may be impacted, as well as impact to the individual. Maps to ID.RA-P4[49] in the NIST Privacy Framework.
	ID.RA-5	Risks to operations should be informed by threats, vulnerabilities, and likelihood. This Subcategory is supported by implementing ID.RA-1, ID.RA-3, and ID.RA-4.	
	ID.RA-6	Once risks are determined, agencies should know how to respond to risks to limit harmful impact to assets and individuals.	8 – Corresponds to the risk processes outlined in ID.GV-6, informed by ID.RA-4 and ID.RA-5. Mapped Privacy Framework Subcategory indicates implementation of the risk responses. 9 – HAZMAT responses, climate risks and impacts are important to understanding responses.

[49] NIST Privacy Framework Subcategory ID.RA-P4 is "Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk." under the NIST Privacy Framework Category "Risk Assessment."

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
	ID.RM-1	Establishing and managing risk management processes allows agencies to balance risk management decisions with agency or operational needs, stakeholder needs and regulatory requirements.	1 – An established risk management process and risk tolerance is critical for physical safety and determining emergency or disaster response.
	ID.RM-2, ID.RM-3	Understanding agency risk tolerance and thresholds helps support prioritizing resources needed, and allocation required for the services provided to the public.	3,8 – Privacy link to agencies knowing their role in the data processing ecosystem (and data supply chain) and contributes to understanding and handling privacy risks. 12 – Strengthening security may weaken accessibility. Agencies need to consider accessibility when hardening systems and implementing cybersecurity safeguards. Risk responses ideally address both.
	ID.SC-1	The ITS and transportation ecosystem requires sourcing systems, parts, components, etc. from various suppliers. Cyber supply chain risk management helps protect the devices, systems, and assets.	3,8,14 – Consider data as part of the supply chain as it is an integral part of ensuring the ITS ecosystem is operational. It is important for an agency to understand their and others' roles in the supply chain, the data processing ecosystem, and the risks associated. 7 – Foundational best practice when integrating new technologies. There may also be additional risks to consider with cloud use.
	ID.SC-2	Similar and in support of ID.SC-1, given the presence of third-party partners and suppliers in the ecosystem, these parties will be assessed using a cyber supply chain assessment process.	3,8,14 – Can include those that provide the data or couriers between delivery of data. 7 – Important due to multistakeholder integrated systems.

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
	ID.SC-3	Helps enforce supply chain risk management processes and assessment processes established in ID.SC-1 and ID.SC-2. Contracts can be the primary way of addressing risks to data shared with third parties. Suppliers and third-party partners are expected to meet applicable standards, regulations, and requirements.	1 – Contracts can help implement appropriate measures to mitigate harmful impacts to physical safety. 3,8,14 – Consider incorporating how to address privacy risks as part of contracts.
	ID.SC-4	Audits and testing may be outlined in the contracts established in ID.SC-3. Contracts can be ineffective without testing. Testing can support verification that contract provisions are being upheld.	1,3,5,8 – Related to physical and human safety, if third party systems are not functioning and that information needs to be disseminated to users. 7 – Testing processes can help manage risks and verify partners are conforming and complying with standards.
	ID.SC-5	Response and recovery planning and testing with suppliers can be part of contracts established in ID.SC-3, processes established in ID.SC-1, or incorporated in response and recovery plans established in PR.IP-9.	3,8,14 – If handling data that may introduce privacy risk, response and recovery testing across the supply chain is best practice. 4 – Response and recovery planning and testing allows for trust that systems and services will be reliable and resilient in the event of an attack.
Protect	PR.AC-1	Service areas in the ITS ecosystem depend on various systems, networks, and other assets that require protection. Having a robust management system to handle identities and credentials for users will help protect these assets from cyber threats.	7,10 – Can help secure communication channels within integrated IT/OT assets. This can help mitigate risks if group accounts are used for user access. This is needed for PR.IP-7 and implementation of digital certificates or Public Key Infrastructure.

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
	PR.AC-2	Managing physical access to assets can help agencies identify and manage threats to facilities or hardware exposed to the public to any mobility mode.	10 – Electronic locks, though cost-intensive, are available as an option to protect physical assets and inform if there has been a breach.
	PR.AC-3, PR.AC-4	Not identified as a High or Moderate Priority Subcategory. Agencies should review for considerations specific to their operating environment.	
	PR.AC-5	Implementing this Subcategory should be consistent with protection of communication and control networks in PR.PT-4.	3,8,14 – Management centers (e.g., TIC, emergency) may have critical data. A lack of network integrity can impact systems disseminating the information involved. This supports integrity of data on network, especially any data shared with other parties. 10 – There may be varying degrees of risk and importance for ITS assets. Segregation of devices (i.e., assets by security zone) may be needed.
	PR.AC-6, PR.AC-7	Not identified as a High or Moderate Priority Subcategory. Agencies should review for considerations specific to their operating environment.	
	PR.AT-1, PR.AT-2, PR.AT-3, PR.AT-4	Users and operators of assets in the ITS ecosystem need to understand their role and impacts to ITS operations. Specifically, those in executive-level roles need to understand their roles and responsibilities as they are in the position to communicate resource prioritization. Applying these Subcategories should be consistent with and informed by ID.AM-6, ID.GV-1, and ID.GV-2.	5 – Standards development should acknowledge users. Users need to understand the standards and policies in place and related to their roles. Senior executives need to understand the importance of standards and coordination and be aware of new technologies to facilitate proper allocation of agency resources. 6 – Workforce development is largely driven by training available and solidifying an understanding of regulations and requirements. Consider providing additional training

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
			for personnel who do not have an IT or network security background for better understanding of agency ITS operations and cybersecurity risks. Senior leaders need to understand the vision for workforce development, their own roles and responsibilities, and the vision for what those are for the rest of the workforce. Workforce levels and workflows may need to be determined to address minimum staffing levels needed for operations and cybersecurity as well as identifying work that needs to be completed.
	PR.DS-1, PR.DS-2	Protecting data-at-rest and data-in-transit is foundational to keeping ITS infrastructure safe and secure, and protecting data residing in and traveling through systems.	3,8 – Location-based services or car-to-service communications (e.g., Waze, Google Maps) and fleet administration systems that handle pre-hiring checks and performance monitoring for drivers, use data that can have harmful privacy impacts if not protected. 14 – Financial transactions may rely on both data-at-rest (e.g., storing credit card or car information) and real-time data flows.
	PR.DS-3	Formally managing assets through transfer, removal, and disposition is critical during the data processing lifecycle.	8 – Promotes protection of any asset containing ITS data, including systems, products, or services, through end-of-life of the asset and facilitates proper handling of information when assets are no longer needed or are transferred to another agency. 14 – Consider ID.AM Subcategory implementations when applying PR.DS-3. Third-party providers and all tools (e.g., cards, applications) that might contain information needing to be disposed of properly.

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
	PR.DS-4	Adequate capacity to ensure availability is necessary for stakeholders of ITS operations to disseminate and receive information.	1 – Capacity increase may be required if there is an event that causes congestion or impacts physical safety, as the public will need notification of status, alternative routes, etc. 3,8 – There should be mechanisms to ensure control messages or information is received. For disseminating data, those who need it should have real-time access to incident response information. When determining who receives access to disseminated information, privacy is considered. This may be implemented during the system design and engineering process. 8,14 – ITS data is available when needed for making decisions regarding ITS services (e.g., financial data is available during a transaction, receiving transportation to health facilities) while minimizing the degree of availability of privacy information. 10 – Telecommunication and networks are a critical component for information availability.
	PR.DS-5	Data leaks are a primary cause of privacy incidents and breaches, which can harm both individuals (e.g., embarrassment) and ITS operations (e.g., erosion of trust).	3,14 – Incident information, device data, financial information etc. can contain data about the device capabilities and location, including information that introduces privacy risk to individuals. 8 – Protective measures should be put in place throughout engineering and data management processes to prevent data leaks. Information being collected needs to be minimized and protected.

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
	PR.DS-6	Software integrity checking mechanisms reduce the likelihood of tampering of agency assets and supports protection and integrity of data. Integrity checking can help prevent system failure or exposure to risks. This Subcategory supports the integrity of assets from ID.AM-1 and ID.AM-2, respectively.	
	PR.DS-7	Non-production environments may not be as well-secured as production environments, leaving ITS data vulnerable to inappropriate access and unnecessary exposure. Development and testing environments do not have final, fully vetted products, which can introduce risk to production environments when not separated. It is important to keep developing and testing environments separate when possible; some agencies outsource developing and testing.	8 – Supports minimizing privacy risks to individuals while developing ITS operations.
	PR.DS-8	Hardware integrity checking mechanisms reduce the likelihood of tampering with agency assets and supports protection and integrity of data. Integrity checking can help prevent hardware failure or risk exposure. This Subcategory supports the integrity of assets from ID.AM-1 and ID.AM-2, respectively.	
	PR.IP-1	Having and maintaining a baseline sets a foundation for other protective measures, and detection and monitoring activities.	

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
	PR.IP-2	The Software Development Lifecycle should cover testing, integration, deployment, maintenance, termination, or end of life (disposal).	3,8 – Includes the data lifecycle and risk management of data. It is important to understand risks throughout and be aware of what privacy engineering concepts should be integrated.
	PR.IP--3	Configuration change control processes are important in a safety critical environment and helps track changes and who made changes to the baseline.	5 – As standards are implemented, adapting systems and requirements to applicable standards are factored into configuration change control processes and reviewed for compliance. 7 – If changing configuration to adopt new technologies, changes need to be logged.
	PR.IP-4	Collect backups as necessary for the agency's ITS operations. When a cyber incident occurs, backups are needed to recover data and return to normal operations.	2 – Backups may be less critical for real-time data.
	PR.IP-5	Given the presence of ITS, roadway devices, and facilities in the physical operating environment, agencies should meet policies and regulations.	5 – Coordinating policy and standards can involve policy and regulations for the physical operating environment (e.g., facilities, weigh stations).
	PR.IP-6	Data destruction or data retention policies are applied to data collected.	3,8 – Important for privacy principle of minimization and related to retention schedules.
	PR.IP-7	Improving protection processes enhances the security of assets and data and strengthens the agency's protection capabilities.	5 – Evolving standards lead to improved protection processes. 7 – When integrating technologies, protection processes will need to evolve and improve with such integrations.

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
	PR.IP-9	Serves as the foundation for Response and Recovery activities and needs to be implemented as a prerequisite for RS.RP and RC.RP.	2 – Coordination needed for services such as emergency management, maintenance, and incident response if needed, and to manage surface transportation needs or crises. 7,10,11 – Account for system interdependencies due to component integration and consider needs for real-time communications.
	PR.IP-10	An untested plan may signify the plan is not ready for operational use. Testing Response and Recovery plans supports PR.IP-9 and identifying gaps.	
	PR.IP-11	Not identified as a High or Moderate Priority Subcategory. Agencies should review for considerations specific to their operating environment.	
	PR.IP-12	Helps in understanding vulnerabilities and how to manage them. A vulnerability management plan should be regularly updated to deal with new threats and capabilities.	
	PR.MA-1	Having the correct personnel in place to address maintenance or repair of ITS infrastructure, and in a timely manner, can minimize or eliminate negative impacts to operations.	2,7 – System and software assets will require software updates to address identified vulnerabilities. Regular maintenance helps integrating new technologies and identifies if assets need replacing to improve operations.
	PR.MA-2	Similar to PR.MA-1, to maintain ITS operations but may require additional measures due to the inherent risks with conducting maintenance remotely.	7,10 – Proper procedures are in place for new assets that allow remote maintenance. Due to the risks remote maintenance introduces, it should typically be discouraged. If remote maintenance is required, it should

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
			be done as minimally as feasible (and only when necessary).
	PR.PT.-1	The ability to review audit logs can help determine the cause of the event and how to respond. PR.PT-1 supports implementation of Detection Subcategories	3 – A common privacy requirement is to be able to tell people what was done with their information and who it was shared with. Audit logs (audits and logs are both data) help piece together that history and are helpful when investigating privacy incidents/breaches or cybersecurity event.
	PR.PT-2	Consider disabling removable media as part of policy if not needed as it can introduce risk. If not, personnel should be aware of potential risks before usage.	
	PR.PT-3	To reduce risk, minimize the functions and services a system or its capabilities is expected to permit. Access to information and system services and capabilities are in accordance with agency access control policies.	3 – Supports data minimization.
	PR.PT-4	Critical to protecting ITS, as communications and control networks are a common attack vector.	1,2,13 – Necessary to keeping the public safe while providing reliable resources and traveler information. 3 – Helps minimize exposure of data or information.
	PR.PT-5	Systems that carry out ITS operations need to function under or be resilient to adverse conditions	1,3 – Supports disseminating information on travel conditions, real-time information, and alerts and advisories (e.g., emergency evacuations) despite adverse situations.

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
			5,10 – TMDD and NTCIP can be applied to the system engineering process to enable C2C communications and address cybersecurity.
Detect	DE.AE-1	Establishing a baseline of network operations and expected data flows is foundational to detecting anomalous activities or potential cyber events. The baseline can help with network monitoring activities to identify cyber threats.	
	DE.AE-2	Understanding your attack vectors helps inform improvements to the reliability of the systems and devices deployed.	6 – Can inform whether an agency is a target of ransomware and how to train the workforce to respond accordingly. 7 – Understand and analyze detected events or indications of adversaries' activity particularly as it relates to a TMC.
	DE.AE-3	Should collect event data, as possible, from all sources (e.g., roadside equipment, sensors, internal systems) to know when an anomalous event has occurred.	
	DE.AE-4	Understanding the impact helps inform what improvement measures need to take place and determine priority for mitigation activities.	6 – Should understand impact especially for events that involves human resources or sensitive information. Training (e.g., response to ransomware) may need to be updated or provided. For physical events, trained personnel are on scene and equipped to respond.
	DE.AE-5	Establishing alert thresholds inform agencies of when systems or services are unavailable.	

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
		Agencies can determine how and when to respond to events.	
	DE.CM-1	Monitoring the network is foundational to detecting anomalous activities. Unusual network activity can indicate ongoing cybersecurity events.	3,8 – Consider privacy risks and secure networks that manage data flows. 6 – Workforce is trained and understands how to monitor and what activities to look for. 7 – Integration and connectivity is based off trust with other systems. Monitoring allows determination of whether to trust connections/integration of systems.
	DE.CM-2	ITS and roadway equipment can be accessible in the physical environment and should be detected for potential cybersecurity events.	2 – Can include monitoring for traffic and road conditions, and environmental conditions that may affect traffic flow. Physical evidence, such as downed traffic lights across a broad area, can indicate a cyber or physical event.
	DE.CM-3	Not identified as a High or Moderate Priority Subcategory. Agencies should review for considerations specific to their operating environment.	
	DE.CM-4		7 – Code can be pushed over connections. Monitoring push over connections can aid enhancing the integration of systems. New technologies likely to be susceptible to supply chain attacks, by which malicious code may be introduced. 10 – Applications from various vendors running on ITS devices should be monitored for malicious code.
	DE.CM-5	Not identified as a High or Moderate Priority Subcategory. Agencies should review for considerations specific to their operating environment.	

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
	DE.CM-6	Integration of cloud technologies introduces additional cybersecurity risks. Agencies should be aware of threats to systems and data that can be introduced by using services by external providers.	
	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software helps prevent potential threats to devices and software such as attackers trying to disrupt information through the TIC.	3,8 – Measures need to be in place so personnel who do not need access to data do not obtain unauthorized access.
	DE.CM-8	Scans should be performed since using technologies increases risks. Acts as a form of monitoring and determining if enhancements are needed. Results of scans may inform execution can be informed by the plan established in PR.IP-12.	4 – Perform scans to know when maintenance or measures need to be taken with regards to an agency's systems and capabilities. 8 – Needed to protect on backend systems that hold sensitive information.
	DE.DP-1	Established detection roles and responsibilities supports the ability for an agency to detect events and respond as appropriately.	
	DE.DP-2	Detection activities may support and have requirements outlined in the vulnerability management plan in PR.IP-12.	
	DE.DP-3	Testing detection processes helps with efficacy of existing processes and can inform necessary improvements DE.DP-5.	

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
🟨	DE.DP-4	Communicating detected information coincides with any communication required in Response and Recovery Function activities.	5 – Standards such as TMDD can be used to help enable C2C communications and manage regional sharing of data and incident management capabilities. 8 – Supports coordination with third-party partners and suppliers in the event of a privacy incident or breach.
	DE.DP-5	Improving detection processes helps account for new threats or vulnerabilities identified and how to respond	
Respond	RS.RP-1	Executing a response plan considers factors such as stakeholder coordination required to maintain operations, protection of data, functionality and capabilities of technologies deployed, and existing standards and policies.	6 – Understand access control requirements such as who needs access to critical systems and services in a physical or cyber event. Personnel should know how to access and execute a response plan.
	RS.CO-1	Implementation should be consistent with ID.AM-6. This supports response efforts and minimizing harmful impacts if safety critical systems are down.	6 – If operational infrastructure or systems (e.g., servers, networks infrastructure) are managed by different technicians, personnel managing these areas coordinate on how to execute the response plan. 9 – Consider HAZMAT material transport and coordination between emergency management centers and freight administration. Disaster response and recovery includes providing enhanced access for response personnel and resources. 13 – Roles and responsibilities during a response to an event are necessary when conducting engagement and

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
🟥			coordination and communications (e.g., with first responders, law enforcement).
	RS.CO-2, RS.CO-3, RS.CO-4, RS.CO-5	Given the multistakeholder environment of ITS, crisis coordination is critical. All stakeholders involved are communicated with (e.g., information sharing, coordination) during an incident and in alignment with an agency's response plan.	3 – Transportation, transit, and rail agencies can communicate with the public, share information, and leverage crowd-sourced data from mobile navigation applications (e.g., Waze). Consider the additional security risks from this type of information sharing. 5 – Voluntary sharing to ISACs, trade associations, or bodies dedicated to standards development can help improve existing standards, polices, and best practices. Standards such as TMDD can be used to help enable C2C communications and manage regional sharing of data and incident management capabilities. 8 – Information sharing and coordination is in alignment with application of DE.DP-4. There are common reporting requirements to individuals when a privacy incident or breach has occurred. 9 – Disaster recovery and response includes various stakeholders such as Emergency Operations Centers, Incident Commands, traffic operations, and drivers. Stakeholders need to be informed for situational awareness and effective recovery efforts. Disaster traveler information like evacuation or reentry is shared with the public.
	RS.MI-1, RS.MI-2, RS.MI-3	When an incident occurs, containing and mitigating the incident and potential damages is critical. In accordance with risk tolerances and thresholds, newly identified vulnerabilities not mitigated are documented as accepted risks. Accepted risks may	3,8,14 – Consider vulnerabilities or incidents that impact privacy and the coordination that requires (e.g., notifying those impacted).

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
		still need minimum safeguards or mitigation measures.	5 – Documentation of newly identified vulnerabilities and after-actions can inform development or updates to policies and standards.
	RS.IM-1, RS.IM-2	Updating response plans and recovery strategies with lessons learned allows for effective collaboration between all stakeholders in the transportation ecosystem (e.g., law enforcement, drivers, agencies).	4 – Lessons learned may impact updates to the ITS infrastructure and how operations respond to an incident in the future. Strategies or acquisition and procurement of new technologies or capabilities could be determined by response activities.
Recover	RC.RP-1	Similar to RS.RP-1, executing a recovery plan enables getting back to normal state and minimizing disruptions to operations.	4 – During this phase, operators will start applying intended updates or maintenance to ITS. 9 – Recovery to a prior state may not be possible given environmental damage. It is important to understand what environmentally can be recovered and efforts that can support that recovery. Plans may need to consider coordination required for transporting HAZMAT.
	RC.IM-1, RC.IM-2	Incorporating lessons learned allows for improvements to services and better alignment of resources. This contributes to efforts to enhance resiliency of ITS and operations. Similarly, updates made to recovery strategies may include lessons learned and will support recovery capabilities.	3 – Allows for agencies to reconsider how data is being handled and can support improving transportation-related recovery efforts. 5,6 – New policies, standards, or training and education can be informed by lessons learned. 10 – Beyond recovery plans, lessons learned may be applied to broader ITS infrastructure or design architecture.
	RC.CO-1, RC.CO-2	Following incidents, managing public relations and reputation is critical to foster public trust. The public should understand restoration activities and be	6 – Building a solid workforce and attracting talent is dependent on public perception and reputation.

Function	Subcategory	General Implementation Considerations	MO Specific Considerations
🟩		aware of when their chosen mobility mode is back to a normal state.	8,13 – Handling incidents or breaches (including privacy incidents) is critical to trust with the public and community. 9 – Handling environmentally related events impacts public perception.
	RC.CO-3	Stakeholders of the ecosystem need to understand recovery activities taking place and their roles in those activities to maintain ITS operations and verify measures are implemented correctly.	2, 12 – Communication of recovery activities can include notifying the public and applicable communities when transportation services are available for normal operations.

Appendix D. Relationship between ITS Profile and ITS Control Sets

The ITS Profile's prioritized Subcategories (represented by the dot chart in **Table 3** through **Table 7**) serve as a foundation of cybersecurity outcomes to be achieved to address cybersecurity risks. Based on their business drivers and an agency risk assessment, an organization can determine which Subcategories are most important to them. All CSF Subcategories are matched to existing standards, guidelines, and practices in the Informative References section of the CSF Core. The Informative References include a mapping of NIST Special Publication 800-53 security controls[50] to Subcategories,[51] which allows a community of interest (e.g., the ITS community) to understand how those controls support the ITS community's objectives and progress toward the ITS Profile.

Prioritized Subcategories can enable program/system owners to know which cybersecurity activities and outcomes are most important to leadership for a given MO, guiding efforts to select, tailor, implement, and manage controls over time at the system/program level, especially given limited resources. Prioritized Subcategories can assist with identifying any NIST SP 800-53[52] controls relevant to the overall MO's success, which can assist with control set activities and prioritizing control implementation. Prioritized Subcategories in the ITS Profile enable the community to focus efforts at the highest level and broad actions, not at the system level with precise actions.

In comparison to the ITS Profile, ITS control sets are implemented at the system/physical object level to provide detailed controls and implementation specifics, which are narrower contexts than those for which the ITS Profile provides. ITS control sets are specifications of selected controls from NIST SP 800-53 needed to mitigate the risk of operating ITS physical objects. Control sets can help protect ITS assets and integrated systems containing those assets against threats and manage the risks of disruptions to agency operations by considering the threats and vulnerabilities specific to the technology and environment of operation. Control set development and implementation are best when informed by the ITS Profile. Doing so contributes to overall enterprise risk management and informed risk management decisions throughout an organization.

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

[51] Reference Table 2, Framework Core, for this mapping from the: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[52] See NIST Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

As seen in **Figure 6**, the ITS Profile consists of input from ITS stakeholders and ARC-IT to reflect what is important to the ITS community's leadership. The ITS Profile documents those priorities in the developed Mission Objectives and Profile dot chart. Developers of ITS control sets can examine the ITS Profile to understand which Mission Objectives are supported by the physical object of the control set. Once that is understood, the developers of control sets can examine a Subcategory's priority and review the controls mapped to the Subcategory in the NIST CSF Informative References. Implementers of the ITS control set can then determine which mapped controls may be a priority for a physical device based on priority Subcategories within the ITS Profile compared to the selected controls within an ITS control set for that physical device.

Control sets address more specific circumstances beyond those reflected in a Cybersecurity Framework Profile. For this reason, control sets typically do not influence the content of the ITS Profile, but the two work as complementary cybersecurity risk management tools within the ITS community.

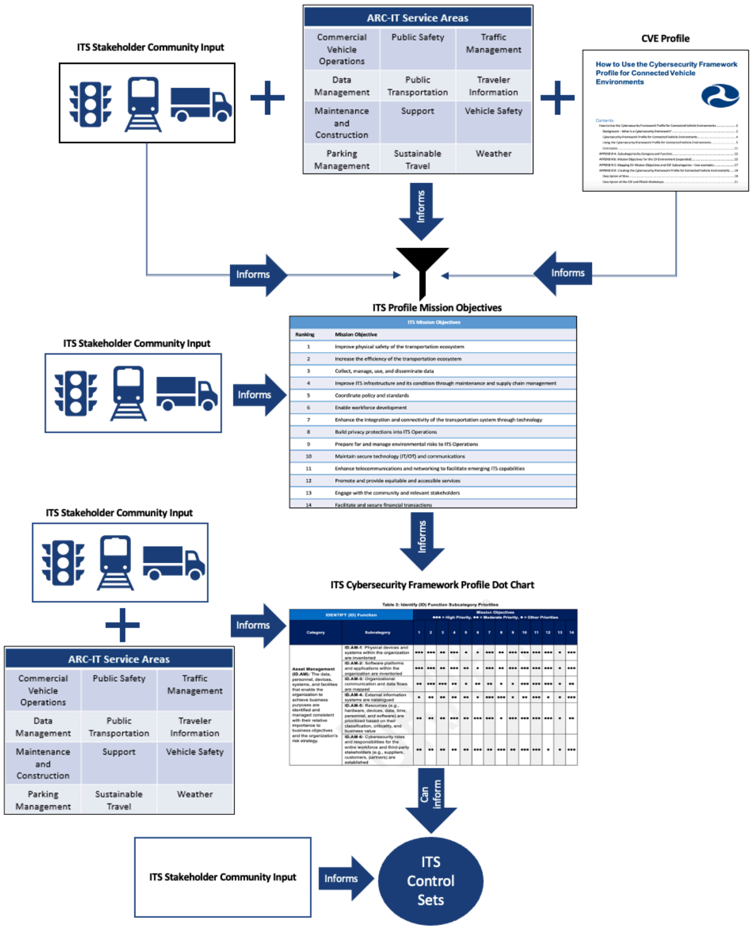

ITS Stakeholder Community Input
+
ARC-IT Service Areas
Commercial Vehicle Operations
Public Safety
Traffic Management
Data Management
Public Transportation
Traveler Information
Maintenance and Construction
Support
Vehicle Safety
Parking Management
Sustainable Travel
Weather
+
CVE Profile
How to Use the Cybersecurity Framework Profile for Connected Vehicle Environments
Informs
Informs
Informs
ITS Profile Mission Objectives
ITS Mission Objectives
Ranking
Mission Objective
1 Improve physical safety of the transportation ecosystem
2 Increase the efficiency of the transportation ecosystem
3 Collect, manage, use, and disseminate data
4 Improve ITS infrastructure and its condition through maintenance and supply chain management
5 Coordinate policy and standards
6 Enable workforce development
7 Enhance the integration and connectivity of the transportation system through technology
8 Build privacy protections into ITS Operations
9 Prepare for and manage environmental risks to ITS Operations
10 Maintain secure technology (IT/OT) and communications
11 Enhance telecommunications and networking to facilitate emerging ITS capabilities
12 Promote and provide equitable and accessible services
13 Engage with the community and relevant stakeholders
14 Facilitate and secure financial transactions
ITS Stakeholder Community Input
Informs
Informs
ITS Stakeholder Community Input
+
ARC-IT Service Areas
Commercial Vehicle Operations
Public Safety
Traffic Management
Data Management
Public Transportation
Traveler Information
Maintenance and Construction
Support
Vehicle Safety
Parking Management
Sustainable Travel
Weather
Informs
ITS Cybersecurity Framework Profile Dot Chart
Table 3: Identify (ID) Function Subcategory Priorities
IDENTIFY (ID) Function
Mission Objectives
Can inform
ITS Stakeholder Community Input
Informs
ITS Control Sets

Figure 6: Relationship Between the ITS Profile and ITS Control Sets

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

Toll-Free “Help Line” 866-367-7487

www.its.dot.gov

[FHWA Document Number]

U.S. Department of Transportation