How to Use the Cybersecurity Framework Profile for Connected Vehicle Environments

Contents

How to Use the Cybersecurity Framework Profile for Connected Vehicle Environments

Connected Vehicle (CV) technologies are an emerging area of innovation that integrates communication technologies with transportation infrastructure to improve the safety and efficiency of the American transportation system. However, increased connectivity of the transportation system brings potential new cybersecurity and privacy risks. To protect travelers and to preserve the integrity of CV technologies, the Intelligent Transportation Systems Joint Program Office (ITS JPO) of the US Department of Transportation (USDOT) asked the National Institute of Standards and Technology's (NIST) National Cybersecurity Center of Excellence (NCCoE) to help create a Cybersecurity Framework (CSF) Profile for the CV Environment (CVE). This document provides background on this effort. It introduces the NIST Cybersecurity Framework, but focuses on the CSF Profile for CVE, and discusses how organizations can use it to manage cybersecurity risk.

Background – What is a Cybersecurity Framework?

The NIST Cybersecurity Framework

The NIST CSF provides a common framework for strengthening cybersecurity defenses across critical infrastructure in any industry or organization that creates, processes, and stores information. The CSF provides a methodology and outlines activities that users can customize to assess risk, identify cybersecurity gaps, and select appropriate controls. It offers one way organizations can approach cybersecurity. The steps in the CSF process allow an organization to identify and prioritize risk in a systematic way and leads to a risk-based catalog of desired cybersecurity outcomes, but the results do not mandate what or how much cybersecurity is appropriate for an organization. Each organization determines appropriate cybersecurity actions based on their priorities, resources, and risk tolerance.

The CSF is also a communication tool. It provides a common language for discussing cybersecurity activities within an organization (e.g., between a chief information security officer and the board of directors) and between organizations (e.g., organizations that rely on cybersecurity capabilities provided by other partnering organizations and/or supply chain partners). It can also provide a way for organizations to measure the progress of their cybersecurity activities over time and to benchmark against or evaluate their organizations' cybersecurity choices. It serves as a tool to communicate cybersecurity capabilities to auditors, regulators, and other types of assessors as well as to partners and vendors.

The basic components of the CSF include the Framework Core, the Framework Implementation Tiers, and the Framework Profile. For more in-depth information about these components, visit NIST's website https://www.nist.gov/cyberframework. This document will refer to the Framework Core and drill down into the Cybersecurity Profile for Connected Vehicle Environments developed by USDOT. The Framework Implementation Tiers are not used in this document.

The CSF Core

The CSF Core is a framework upon which to base a cybersecurity risk analysis. It guides users through a process to answer five key questions about their organization:

1. What processes and assets need protection?
2. What safeguards are available?
3. What techniques can identify incidents?
4. What techniques can contain impacts from incidents?
5. What techniques can restore capabilities?

Each question addresses a different Function (see Table 1, below). The CSF defines Categories common to most organizations under each Function as a starting point. Each Category specifies Subcategories. The Subcategories are linked to Informative References that provide specific control options. The CSF is a flexible, customizable tool: Not all Subcategories may be relevant for every application, but clear justification is necessary before omitting one. Appendix A provides a table of Subcategories by Category and Function.

Table 1 The CSF Five Functions

Function	Identify	Protect	Detect	Respond	Recover
	What processes and assets need protection?	What safeguards are available?	What techniques can identify incidents?	What techniques can contain impacts from incidents?	What techniques can restore capabilities?
Description	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

Categories					
	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Supply Chain Risk Management	• Access Control • Awareness and Training • Data Security • Information Protection and procedures • Maintenance • Protective Technology	• Anomalies and Events • Security Continuous Monitoring • Detection Process	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvements • Communication

CSF Profile

A CSF Profile is a customized tool for identifying, prioritizing, and addressing the cybersecurity needs of a particular organization or industry, based on factors such as Mission Objectives, risk tolerance, and available resources. Profiles identify and prioritize opportunities for improving cybersecurity at an organization or within an industry.

Organizations, industries, or any interested entities can create profiles at any time. Usually, the first time an organization creates a profile, its purpose is to assess the current state of its cybersecurity approach. After developing an Initial Profile (depicting its current state) an organization can create a Target Profile(depicting its desired state) to provide a roadmap for improving risk management. A gap analysis can then be performed to support prioritization and progress towards the desired state in the Target Profile. Frequently, the first step in creating a profile is to articulate and define the Mission Objectives for the industry or organization. Next, an organization can then review each Subcategory from the CSF Core to determine its relevance to each Mission Objective. The Subcategory may be applicable as is, it may need tailoring to the specific system, or it may not apply. If a Subcategory is relevant, an analysis determines whether the desired outcomes are achievable and, if so, using which controls. If not, that fact is an input to the gap analysis.

By creating the CSF Profile for CVE, USDOT did some of the preliminary work of creating a template for an initial CSF Profile. The information that follows and the corresponding "CSF Profile for CVE DOT Chart" workbook can be used and adapted by Connected Vehicle technology deployers as they see fit to apply to the specifics of their deployments, resources and priorities.

Cybersecurity Framework Profile for Connected Vehicle Environments

The CSF Profile for CVE is an industry profile developed by USDOT that CV programs can use as a starting point when developing a more customized profile and analysis for their own unique environment. State and local organizations and departments that implement connected vehicle technology often share similar Mission Objectives and face similar risks. Therefore, USDOT conducted guided workshops with the University of Michigan Transportation Research Institute (UMTRI), and pilot sites in New York City,

Tampa, and Wyoming to develop a CSF profile specific to the CV environment. The workshops resulted in an initial set of 12 mission objectives and prioritizations that provide a baseline for building a more customized profile and cybersecurity program. CV programs can use their profile as a tool to develop, refine, or validate their cybersecurity strategy.

Mission Objectives are specific outcomes that support universal objectives of an industry or industry subsector, in this case CV environments. The Mission Objectives developed specifically for the CV environment allow users to identify relevant high and moderate cybersecurity outcomes for each one in a targeted, systematic, and comprehensive way. The Mission Objective for CV environments are summarized in Table 2 in the next section, with more detailed descriptions provided in Appendix B.

The ability of CV environments to meet their Mission Objectives is dependent on the success of cybersecurity activities and outcomes, which correspond to CSF Subcategories. Generally, multiple relevant Subcategories are prioritized in support of each specific Mission Objective. Assigning priority (high, moderate, low) to each Mission Objective with respect to each CSF Subcategory (see Appendix C: Mapping CV Mission Objectives and CSF Subcategories) and tabulating them, allows users to formulate customized high and moderate priority cybersecurity outcomes for each Mission Objective.

The CSF for CVE was developed early in the lifecycle for deploying CV technologies. The number of CV applications being deployed is low in comparison to the many applications envisioned in the future. As CV technologies mature and evolve, organizations may need to adjust this profile to address the specific needs of their program.

Using the Cybersecurity Framework Profile for Connected Vehicle Environments

How an organization uses the CSF Profile for CVE will depend on many factors including how an organization manages risk, its current cybersecurity program, its institutional context, and the stakeholders involved. This industry profile is only a starting point and should be tailored and supplemented as needed to address areas where an organization's scope or objectives may differ from the hypothetical baseline case. In general, working with any CSF Profile requires input from different departments, individuals and functions within an organization. For example, individuals from Information Technology, Cybersecurity, Legal, Risk Management, Finance and the Executive Suite would all have different information and perspectives to contribute to the discussion and development of a robust profile and implementation process. Each organization is different, so determining who within an organization can or should contribute will vary.

The profile is a flexible tool for CV implementers/deployers to address cybersecurity and privacy implications of connected vehicle technologies in an organized and comprehensive way. The NCCoE has described one way in which an organization can use or adapt a profile[1] (See Figure 1.) USDOT has adapted and annotated this process below.

[1] NCCoE, How To: Develop a Cybersecurity Framework Profile, NIST Cybersecurity Risk Management Conference 2018

Figure 1 NCCoE CSF Profile Use Process

As mentioned, this is just one example of how an organization can create a profile using the CSF for CVE as a starting point and/or Target Profile. Below are some steps an organization may employ in using the profile to develop a more comprehensive cybersecurity program, based on NIST's *"Framework for Improving Critical Infrastructure Cybersecurity," version 1.1*. USDOT has also developed a worksheet tool, *CSF Profile for CVE Dot Chart*, to enable organizations to manipulate and customize both the Mission Objectives and prioritization.

1. Identify Mission Objectives

Since Mission Objectives link business risk to cybersecurity risk, an organization must identify its Mission Objectives and high-level priorities, as well as the scope of systems and assets that support the process. The Mission Objectives developed for the CV environment, and described in the Table 2 below, can serve as a starting point. Each organization may:

- Determine which are relevant for their environment and remove any that do not apply to the program's deployment plans;
- Adjust descriptions of existing Mission Objectives, if needed, and adjust priority Subcategories accordingly;
- Identify the need for any additional Mission Objectives that should be considered a priority for the program and identify priority Subcategories for each new objective; and
- Adjust the relative priority of Mission Objectives accordingly.

What is a Mission Objective?

Mission Objectives are specific actions for achieving an organization's goals. To be most effective, Mission Objectives should be concise and action oriented. The action verb selected influences each objective's relative priority within the set of Mission Objectives as well as the Subcategories prioritized for it. It may take several attempts at drawing candidate lists of objectives to achieve an appropriate level of functional abstraction. They should not simply be lists of 'what we do' and they should not be so abstract that subject matter experts would not understand why the functionality is listed. People with experience in enterprise architecture and architectural frameworks typically understand how to identify objectives that strike the desired balance. CV programs can use the existing Mission Objectives in the CV Environment CSF Profile as examples of what constitutes a useful Mission Objective.

Extending the Categories and Subcategories in the CSF is also an option for organizations. Before adding new Subcategories, CV programs should carefully evaluate whether existing Subcategories can meet their needs with additional supporting narrative in their profile to maintain interoperability of their profiles with other CV programs and partners as well as future versions of the CSF.

NIST's National Cybersecurity Center of Excellence (NCCoE) has found that implementing profiles is most manageable when there are no more than 8-12 Mission Objectives. Once identified, the CV programs

can rank or prioritize the Mission Objectives, indicating why and by how much one is ranked over another. The CSF for CV provides an initial ranking, however, the nature of CV environments may vary widely, and so programs may want to customize the Mission Objectives relevant to them and/or the relative priority between Mission Objectives.

Table 2 Baseline Mission Objectives Developed for the CV Environment

Mission Objective	Description
Ensure secure and timely communications	Messages and other system data move freely about the CV system; trusted messages are given with adequate time to react and safety-related messages are given priority
Plan, deploy, and operate network	Through a continuous improvement process, CV environments can build on legacy infrastructure and plan for the future without redundancy and fail-over
Manage data collection and storage	Collect and maintain the right data through governance structure and adequate protections to enable trust in the system
Build privacy into CV program	Create requirements relevant to the collection and use of personally identifiable information (PII), including options for consent and the ability for users to control information about themselves
Improve mobility for passenger vehicles	Use timely warnings and alerts, as well traffic data on future projects, to increase efficiency
Provide transportation efficiency for commercial vehicles and fleets	Allow commercial entities to improve efficiency of routing around issues
Manage users	Provide the necessary level of customer service to support users
Assure asset security and operational viability	Assets are monitored for expected capabilities, system health, and security
Conduct data analyses	Conduct data analyses to evaluate operations and need for maintaining and improving the system
Minimize driver distraction and workload	Design interfaces to assist the driver in operation
Measure and evaluate performance	Deployments must measure and evaluate performance to validate effectiveness and monitor for system degradation
Perform strategic communications to facilitate business and driver adoption	Communication should be tailored to meet the needs of internal and external stakeholders

2. Establish Context for Cybersecurity

The next step in the process is to identify relevant systems and assets, potential regulations or requirements, and overall risk approach, as well as threats to the systems identified. This requires the identification and engagement of stakeholders and key individuals.

Through discussion amongst stakeholders and key individuals, CV programs should consider the unique needs of their environment in terms of requirements (e.g., applicable laws, policies, standards); risks and challenges (e.g., known threats); and any other influencing factors deemed relevant.

3. Create a Current Profile

By creating a Current Profile, organizations can examine the extent to which they are achieving the outcomes described in the Core Categories and Subcategories, aligned with the five high-level Functions: Identify, Protect, Detect, Respond, and Recover. The CSF for CVE provides an initial alignment and prioritization scheme that can be found in the spreadsheet *CSF CVE Profile Dot Chart* or in Appendix C of this document. It is up to each organization to review and determine its relative prioritization and customize the spreadsheet as necessary.

Whether creating or customizing an existing profile, an organization begins with analyzing each Subcategory from the CSF Core to determine its relevance to each Mission Objective. The Subcategory may be applicable as is, it may need tailoring to the specific system, or it may not apply. Each CV environment scope, technologies and context will influence the Subcategories that are most important for each Mission Objective.

Once relative prioritization is determined, CV programs can then analyze and document their current level of execution for each of the outcomes described in the Categories and Subcategories; and focus on those that are most impactful to meeting each Mission Objective. As needed, narrative in the Target Profile (explained below) can describe the reasons behind the prioritization and the relative state of implementation.

The Current Profile is a compilation of the Subcategory outcomes from the CSF Core that are being achieved. Outcomes that are not achieved, or only partially achieved, will form the basis of a gap analysis in subsequent steps.

4. Conduct Risk Assessment

Risk assessments identify, evaluate, rank, and address potential adverse impacts to organizations. Each organization can analyze its operational environment to identify the likelihood of an event and the impact an event could have, as well as the adequacy of planned or existing security controls.

One method an organization can use is to answer the following questions for each Mission Objective:

- What threats could prevent the successful completion of the objective?
- What damage is caused when the objective is not achieved?
- What assets are most important for achieving the objective?

- Where do physical infrastructure and cybersecurity infrastructure effect each other?

5. Create a Target Profile

As previously stated, organizations, industries, or any interested entities can create profiles at any time. In this case, the purpose of the Target Profile is to create a roadmap for a CV program to achieve its cybersecurity goals, based on the Mission Objectives, cybersecurity context, and the risk analysis. A Target Profile may be part of the design phase for a new program, or part of an evaluation of the cybersecurity status of an existing program.

Whether creating or extending a profile, an organization begins with analyzing each Subcategory to determine its relevance to each Mission Objective. The Subcategory may be applicable as is, it may need tailoring to the specific system, or it may not apply. If an organization or industry believes a CV environment profile's Mission Objective or its mapping to the CSF does not map to their understanding of the business functions or the related cybersecurity risks in their own environment, they can address those differences in their Target Profile(s).[2] This can be part of creating their initial Target Profile or a regular update process, or it can be event-driven due to changing circumstances. The desired cybersecurity outcomes prioritized in a Target Profile can be incorporated when a) developing the system during the build phase and b) purchasing or outsourcing the system during the buy phase. Profiles are not static, but they should be stable enough to support the risk management functions of an organization.

Understanding the relative priority between Mission Objectives will aid programs in strategic planning as they use their completed Target Profile. A CV Target Profile is also a communication tool that can be used both internally (e.g., between stakeholders from the C-suite to line-level implementers) and externally (e.g., between your organization stakeholders such as partners, suppliers, and regulators).

6. Conduct a Gap Analysis: Compare the Current Profile and the Target Profile

The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals[3]. A comparison of the Current and Target Profiles will reveal gaps. Taking into account the relative priorities of Mission Objectives and desired cybersecurity outcomes, a prioritized action plan can be created to address the gaps. Specific controls for each supcategory and/or gap can be found in the informative references section of the CSF Profile for CVE DOT chart.

When the Current Profile was created (in step 3), there may have been Subcategories identified as relevant to the organization that were not yet addressed. This is one kind of gap. Another kind of gap is revealed when the Current Profile and the Target Profile are compared at the Subcategory level. If the

[2] Appendix 4 discusses the methodology for creating the CV Environment Cybersecurity Framework Profile, including discussion of identifying Mission Objectives and priority Subcategories. A similar approach can be used by CV programs when adapting or creating Mission Objectives.

[3] "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, National Institute of Standards and Technology (April 16, 2018), p. 11

cybersecurity outcomes are not fully addressed by the Current Profile, the gaps identified are collected and form the input for a prioritized action plan.

In an action plan, an organization may consider not only the potential controls available to achieve desired outcomes, but also what is both necessary and possible for that organization. This process results in an executable action plan.

7. Implement Action Plan: Address the Identified Gaps

The action plan is the mechanism through which an organization progresses towards its Target Profile. In order for the action plan to be of practical use, it must accurately reflect the resources available to the organization. An organization will need to prioritize each action in the plan by both its importance and the resources required to implement it.

Each organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the CSF identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

Cybersecurity is not static. An organization repeats the steps as needed to continuously assess and improve its cybersecurity. Because technology is constantly changing, new threats and vulnerabilities will arise. The CSF process will need to be repeated regularly in order to for CV programs to continuously adapt to the changing environment[4].

Additionally, as CV deployments evolve, the scope and number of applications used by any one program are likely to increase beyond the current pilot environments, bringing yet greater complexity to CV deployments. In more complex environments, more attention will be required to consider the cybersecurity and privacy implications of how a larger scope of and variety of CV applications interact with each other.

Conclusion

New methods to address the risk introduced by the rapid expansion of communication technologies and their use in in areas such as transportation is needed to protect the safety and security of the Nation's transportation system. The NIST CSF is one such method. By using the CSF as a starting point, and engaging academia and CV pilots to develop strategies to tailor it to the CV environment, ITS JPO developed the CSF for the CVE. This tool will allow the CV industry to protect travelers and preserve the integrity of CV technologies. Using the Cybersecurity Framework Profile is a process. It is not a static document but a customizable framework that can be updated and developed over time as organizations and connected vehicle technologies evolve.

[4] Ibid

APPENDIX A: Functions, Categories and Subcategories

IDENTIFY (ID)	**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 prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**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 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
		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 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

PROTECT (PR)	**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 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 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
		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
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, 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 principles 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

DETECT (DE)	**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
		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
RESPOND (RS)	**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 and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated
		RS.AN-2: The impact of the incident is understood
		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
RECOVER (RC)	**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

APPENDIX B: Mission Objectives for the CV Environment (expanded)

Mission Objective	Description
Ensure Secure and Timely Communications	Messages and other system data move freely about the CV system among vehicles, mobile devices, system components in the field, and back-office systems within expected latency parameters. Trusted messages reach applications and vehicles with adequate time for drivers to react. Priority is given to safety-related messages.
Plan, Deploy, and Operate Network	Providing CV network connectivity requires proper planning, deployment, and operations. This network must operate in a time-critical manner with appropriate redundancy and fail-over. Through a continuous improvement process, CV environments build on legacy infrastructure, incorporate currently envisioned CV capabilities, and plan for the future fully integrated automated vehicle-enabled environment.
Manage Data Collection and Storage	The CV system creates, ingests, and maintains reliable data to support system functions as well as valuable data analyses. Data is a key asset during all lifecycle stages. Identifying and collecting the right data provides insights regarding system performance and health as well as indicators of breaches or other issues that impact system effectiveness and/or participants. Implementing a governance structure and adequate protections enables trust in individual system components and the system over all as well as confidence in information-sharing relationships, research efforts, and analyses.
Build Privacy into CV Program	The CV system manages privacy as an integrated component of risk management throughout all aspects of the system. Privacy is implemented through policy, processes, system design, and implemented components, leading to trust in the system and continued participation by the public. Requirements regarding the collection and use of personally identifiable information (PII) and potential PII are aligned with the purpose for operating the CV system as well as thoroughly documented and understood by all organizations involved in operating the CV system and using from the data generated by it. Participants are informed of privacy practices with understandable notices, are offered options for consent, and provided the ability to control information about themselves, their devices, and their vehicles when practicable. Advanced notice to participants of changes and the choice to opt-in are provided in advance. Adequate controls are built into the CV system to protect user information as well as vehicle information that could lead to identification of and information about a vehicle/device owner or driver.
Improve Mobility for Passenger Vehicles	The CV system provides alerts and historical data that support decision making for efficient vehicular travel. These efficiencies are gained through timely warnings and alerts that allow drivers to make decisions in real-time as well as analyses of traffic data that inform future projects. These efficiencies result in safer driving experiences, improved travel time performance, and improved environmental impacts.

Mission Objective	Description
Provide Transportation Efficiency for Commercial Vehicles and Fleets	Technologies and connectivity adapted for commercial vehicles must be properly integrated into the CV environment. In addition to system wide alerts and warnings, the CV system provides fleet management capabilities that allow commercial entities and transit operators to improve efficiency of routing around issues such as traffic and weather conditions and to receive driving metrics to improve fleet management decisions.
Manage Users	CV deployments provide the necessary level of customer service to support users. During the pilot stage this includes defined business cases to link pilot objectives to necessary participant qualifications (e.g., expectations regarding driving records); clear communications regarding procedures; maintaining ability to communicate with participants, as necessary; procedures for managing pilot incentives; and the ability to determine when issues occur. Procedures address recruitment, enrollment, outfitting of vehicles, informing and gathering participant information, in-study data collection, analysis, unenrollment, and post-study decommissioning. During full deployment this covers the necessary level of customer service for all users of the system to include drivers, pedestrians, infrastructure operators, and service providers.
Assure Asset Security and Operational Viability	Performance of CV system components is monitored for expected capabilities, system health, and security to ensure they are performing within the expected parameters, thereby maintaining the functionality of the CV system. Assets can be remotely monitored, managed, and updated where possible and when needed.
Conduct Data Analyses	Data analyses will be conducted by local and regional agencies to evaluate real-time operations and assess future needs for maintaining and improving the system. Additionally, third parties may conduct research and other analyses. Protocols should be developed to manage access and sharing of the data to support these current and future analyses and to facilitate sharing of results with appropriate parties.
Minimize Driver Distraction and Workload	Driver interfaces should be designed to assist the driver in operation of a safer vehicle due to the addition of CV technology. Alerts and warnings should be delivered in a manner that encourages drivers to react within an appropriate amount of time to avoid an incident and without causing additional incidents.
Measure and Evaluate Performance	Connected vehicle deployments must measure and evaluate performance of CV technology and processes to validate effectiveness, monitor for system degradation, and provide information to support improvements. This includes proper instrumenting, data collection, and data analysis.
Perform Strategic Communications to Facilitate Business and Driver Adoption	Using strategic communications facilitates adoption of CV technologies by providing benefits to participants for safety and efficiency to business for CV and non-CV economic opportunities. Communication methods and messaging should be tailored to meet the needs of internal and external stakeholders, including participants (e.g., commercial and personal vehicle drivers); consumers of CV system data (e.g., researchers, city planners); supporting technology vendors, CV program leadership, and others that support the CV program.

APPENDIX C: Mapping CV Mission Objectives and CSF Subcategories

IDENTIFY (ID)		1 Ensure Secure and Timely Communica-tions	2 Plan, Deploy, and Operate Network	3 Manage Data Collection and Storage	4 Build Privacy into CV Program	5 Improve Mobility for Passenger Vehicles	6 Provide Transporta-tion Efficiency for Commercial Vehicles and Fleets	7 Manage Users	8 Assure Asset Security and Operational Viability	9 Conduct Data Analyses	10 Minimize Driver Distraction and Workload	11 Measure and Evaluate Perfor-mance	12 Perform Strategic Communications to Facilitate Business and Driver Adoption
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 prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**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 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	•	•	•	•••	•••	•••	•••	•	•	•	••	••
	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 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	•••	•••	••	••	•••	•••	•	•••	•	•••	•	•
	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	••	••	••	••	••	••	•	••	•	••	•	•

APPENDIX D: Creating the Cybersecurity Framework Profile for Connected Vehicle Environments

Description of Sites

In order to provide cybersecurity and privacy guidance to broadly support current and future CV environments, ITS JPO consulted with four CV sites that are actively working to meet a diverse set of CV goals with differing applications. The sites included the Ann Arbor Connected Vehicle Test Environment (AACVTE) research implementation in Ann Arbor, Michigan, which is run by the University of Michigan Transportation Research Institute (UMTRI), as well as three of the pilot sites. A brief description of each site follows.

About the AACVTE[5]

The AACVTE aims to be the largest operational, real-world deployment of connected vehicles and infrastructure in the world. The test bed is federally funded, (FHWA), State funded (Michigan Economic Development Corporation), as well as funded by academia, Michigan Mobility Transformation Center (MTC), the City of Ann Arbor, and additional partners. Deployment will include up to 5,000 equipped vehicles covering 45 street locations and 12 freeway sites, and 27 square miles (the City of Ann Arbor). Devices continuously transmit speed and position data from participating vehicles to other, similarly equipped vehicles, as well as into the surrounding environment where this information can be recognized by equipment located along the roadside and at intersections. Information transmission in this study occurs during the participant's usual everyday driving.

About the Pilots

The ITS JPO awarded cooperative agreements to three pilot sites in New York City; Wyoming; and Tampa to implement a suite of connected vehicle applications and technologies tailored to meet their region's unique transportation needs.[6] These pilot sites help connected vehicles make the final leap into real-world deployment so that they can deliver on their promises to increase safety, improve personal mobility, enhance economic productivity, reduce environmental impacts, and transform public agency operations. In early 2019, the pilot sites will move from the installation phase to operations and evaluations. Through evaluations and lessons learned, these sites are laying the groundwork for even more dramatic transformations as other areas follow in their footsteps.

[5] https://www.its.dot.gov/research_archives/safety/aacvte.htm

[6] The DOT continues to fund additional CV technology projects beyond the Wyoming, New York, and Tampa pilots, such as those that are part of the Advanced Transportation and Congestion Management Technologies Deployment (ATCMTD) Program. However, the work discussed in this document was conducted with the three pilots named above.

New York City (NYC) DOT Pilot[7]

The New York City Pilot aims to improve the safety of travelers and pedestrians in the city through the deployment of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) connected vehicle technologies. Approximately 5,800 cabs, 1,250 MTA buses, 400 commercial fleet delivery trucks, and 500 city vehicles that frequent three distinct areas will be fit with CV technology. Using short-range communications, the deployment will include approximately 310 signalized intersections for V2I technology. In addition, NYCDOT will deploy approximately eight roadside units (RSUs) along a higher-speed area to address challenges such as short-radius curves, a weight limit and a minimum bridge clearance and 36 RSUs at other strategic locations throughout the city to support system management functions. As a city bustling with pedestrians, the pilot will also focus on reducing vehicle-pedestrian conflicts through in-vehicle pedestrian warnings and an additional infrastructure-to-vehicle (I2V) project component that will equip approximately 100 pedestrians with personal devices to assist them in safely crossing the street.

Tampa-Hillsborough Expressway Authority (THEA) Pilot[8]

THEA owns and operates the Selmon Reversible Express Lanes (REL), which is a first-of-its-kind facility to address urban congestion. The REL morning commute endpoint intersection is on major routes into and out of the downtown Tampa commercial business district. Drivers experience significant delay during the morning peak hour resulting in, and often caused by, a correspondingly large number of rear-end crashes and red-light-running collisions. Because the lanes are reversible, wrong-way entry is possible. The THEA pilot will deploy a variety of V2V and V2I applications to relieve congestion, reduce collisions, and prevent wrong-way entry at the REL exit. THEA also plans to use CV technology to enhance pedestrian safety, speed bus operations, and reduce conflicts among street cars, pedestrians, and passenger cars at locations with high volumes of mixed traffic.

Wyoming (WY) DOT Pilot[9]

Wyoming is an important freight corridor that plays a critical role in the movement of goods across the country and between the United States, Canada, and Mexico. Interstate 80 (I-80) in southern Wyoming, which is 6,000 feet above sea level, is a major corridor for east/west freight movement and moves more than 32 million tons of freight per year. During winter seasons, crash rates on I-80 have been found to be 3 to 5 times higher than summer crash rates due to increased wind speeds and wind gusts. The Wyoming Department of Transportation (WYDOT) CV Pilot site focuses on the needs of the commercial vehicle operator in the State of Wyoming and will develop applications that use V2I and V2V connectivity to support a flexible range of services and advisories including roadside alerts, parking notifications, and dynamic travel guidance. This WYDOT CV Pilot is expected to reduce the number of blowover incidents and adverse weather-related incidents (including secondary incidents) in the corridor in order to improve safety and reduce incident-related delays.

[7] https://www.its.dot.gov/pilots/pilots_nycdot.htm

[8] https://www.its.dot.gov/pilots/pilots_thea.htm

[9] https://www.its.dot.gov/pilots/pilots_wydot.htm

More information regarding the pilots is available at https://www.its.dot.gov/pilots/.

Description of the CSF and PRAM Workshops

To obtain feedback from each site, ITS JPO and NCCoE visited each site to facilitate discussions to support the development process for both the CSF Profile for CVE and the CVE Privacy Risk Assessment Methodology (PRAM). The workshops followed a common format. Each workshop began with an overview of the project to create this guidance as well as an overview of each site's CV environment. The second phase of the workshop focused on identifying and prioritizing CV Mission Objectives for each site's CV program. Subsequently, each of these Mission Objectives was then reviewed to determine priority Cybersecurity Framework Categories that support each Mission Objective. Through the Cybersecurity Framework related discussions, useful information for the privacy risk assessment process also surfaced. The third phase of each workshop focused on gathering additional information needed to address privacy, including additional discussion regarding the site's approach to privacy and constructing high-level data flows between the CV program's system components.

The UMTRI site focused on the test environment and test processes. The Wyoming site focused on technical aspects of the traffic system, wired and wireless network connectivity, devices, vehicles (passenger, commercial, snowplow, law enforcement/public safety), and messages in a highway-based CV environment. The NYC site identified many potential Mission Objectives focused on urban-based CV environment. The Tampa site identified similar functions to the others but focused on the transition zone from interstate highways and off-ramps to urban surface transportation and related bottlenecks.