Using the Cybersecurity Framework Profile for Connected Vehicle Environments

Executive Summary

In order to support the emergence of Connected Vehicle (CV) deployments across the U.S., the United States Department of Transportation (USDOT) sponsored the creation of a Cybersecurity Framework (CSF) Profile for Connected Vehicle Environments (CVE).

"How to Use the CSF Profile for CVE" discusses how organizations can use the Cybersecurity Framework Profile for CVE to manage cybersecurity risk. It introduces the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), but focuses on the CSF Profile for CVE. A corresponding worksheet tool, *CSF CVE Profile Dot Chart*, is also available to enable organizations to manipulate and customize the Mission Objectives as well as the prioritization of the categories and subcategories of actions within the profile.

This profile is an informative resource for deployers of CV technologies. It is an application of the NIST CSF, which is voluntary and based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. It was designed to help foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

In the context of the Cybersecurity Framework, Mission Objectives are specific outcomes that support common objectives within an industry or industry subsector, in this case CV environments. The Mission Objectives in this profile were developed specifically for the CV environment to allow users to identify relevant high and moderate cybersecurity outcomes for each one in a targeted, systematic, and comprehensive way. 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. Assigning priority (high, moderate, low) to each Mission Objective with respect to each CSF allows users to customize high and moderate priority cybersecurity outcomes for each Mission Objective and make more informed decisions about where to focus their cybersecurity activities.

In general, working with any CSF Profile requires input from different departments, individuals and functions within an organization. For example, individuals from Operational Offices, 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 specific to their organization. Each organization is different, so determining who within an organization can or should contribute will vary.

How an organization chooses to use 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 can be tailored and supplemented as needed to address areas where an organization's scope or objectives may differ from the hypothetical baseline case provided in this CSF Profile for CVE.