NIST Interagency Report
NIST IR 8473

# Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure

Jim McCarthy
Nakia Grayson
Joseph Brule
Tom Cottle
Alan Dinerman
John Dombrowski
Josie Long
Hillary Tran
Karen Quigg
Michael Thompson
Anne Townsend
Nik Urlaub

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8473

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

**NIST Interagency Report**
**NIST IR 8473**

# Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure


Jim McCarthy*
Nakia Grayson
*Applied Cybersecurity Division*
*Information Technology Laboratory*

Joseph Brule
Tom Cottle
Alan Dinerman
John Dombrowski
Josie Long
Hillary Tran
Karen Quigg
Michael Thompson
Anne Townsend
Nik Urlaub
*The MITRE Corporation*
*McLean, VA*

**Former NIST employee; all work for this publication was done while at NIST.*



This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8473

October 2023




U.S. Department of Commerce
*Gina M. Raimondo, Secretary*

National Institute of Standards and Technology
*Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology*

**Publication History**
Approved by the NIST Editorial Review Board on 2023-10-05

**How to Cite this NIST Technical Series Publication:**
McCarthy J, Grayson N, Brule J, Cottle T, Dinerman A, Dombrowski J, Long J, Tran H, Quigg K, Thompson M, Townsend A, Urlaub N (2023) Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8473. https://doi.org/10.6028/NIST.IR.8473

**Author ORCID iDs**
Jim McCarthy: 0000-0002-5559-733X
Nakia Grayson: 0000-0003-1062-4338
Michael Thompson: 0000-0002-0836-244X
John Dombrowski: 0000-0002-9408-1838

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2002) Gaithersburg, MD 20899-2002

## Abstract

This document is the Cybersecurity Framework Profile (Profile) developed for the Electric Vehicle Extreme Fast Charging (EV/XFC) ecosystem, including the four domains that relies on the ecosystem (i) Electric Vehicles (EV); (ii) Extreme Fast Charging (XFC); (iii) XFC Cloud or Third-Party Operations; and (iv) Utility and Building Networks. This Profile utilizes the NIST Cybersecurity Framework Version 1.1 and provides voluntary guidance to help relevant parties develop Profiles specific to their organization to understand, assess, and communicate their cybersecurity posture as a part of their risk management process. The Profile is intended to supplement, not replace, an existing risk management program or cybersecurity standards, regulations, and industry guidelines that are in current use by the EV/XFC industry.

## Keywords

Cybersecurity Framework; electric vehicle, EV/XFC ecosystem; extreme fast charging; Framework; mission objectives; profile; risk management; security controls.

## Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

## Department of Energy Points of Contact

The National Cybersecurity Center of Excellence (NCCoE) would like to thank the following Department of Energy (DOE) colleagues for their collaboration on this profile.

Lee Slezak - DOE, Office of Energy Efficiency and Renewable Energy (EERE)
Jessica Yoo Perry – DOE, Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

## Acknowledgements

The National Cybersecurity Center of Excellence (NCCoE) would like to thank the following individuals for their discussions and insights during the development of this profile.

Nicole K. Bell, NIST Guest Researcher

Dr. Sunil M. Chhaya, Electric Transportation Program (EPRI)

Lovington Dela Cruz, Arcadis
Katya Delak, NIST Office of Weights and Measures
Alexis Diamond, NIST Guest Researcher
Gregory Brian Dindlebeck, Pacific Northwest National Laboratory
Xavier Francia, DER Cybersecurity Program (EPRI)
Dr.-Ing. Fredrich Emanuel Hust, Mercedes-Benz AG
Alexander Irrgang, Mercedes-Benz AG
Pamela K. Isom, IsAdvice & Consulting
Moe Kia, BC Hydro
Ramesh Krishnasagar, Bp
Alanna Quail, Via Motors
Lionel Richard Saposnik, Saiflow
Dor Shmaryahu, SaiFlow
Or Shwartz, SaiFlow
Werner Streich, P3 Group
Mauricio Tavares, Privacy Test Driver
Jennifer Tisdale, GRIMM

## Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: evxfc-nccoe@nist.gov

## Table of Contents

## List of Tables



## List of Figures

# 1. Introduction

To address risks to critical infrastructure, the Cybersecurity Enhancement Act of 2014 [S.1353] assigned responsibility to the National Institute of Standards and Technology (NIST) to identify and develop cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. This formalized NIST's previous work developing Version 1.0 of the Framework under Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, and provided guidance for future Framework evolution [EO.13636]. The NIST Cybersecurity Framework [NIST-CSF] is a voluntary, risk-based assemblage of industry standards and best practices designed to help organizations manage cybersecurity risks. Standards listed in the informative reference section are simply recognized best practices or provide relevant information and are not meant to represent any type of regulatory or compliance mandate from this document. Informative references listed under "Ecosystem" can provide additional information or best practices for any ecosystem member, references listed under specific domains (EV, XFC/EVSE, Cloud/Third-Party, Utility/Building Management Systems) can provide information or best practices for that domain.

The number of electric vehicles (EVs) is projected to be 24.6M by 2030 [EEI-2022]. The EV infrastructure was prominently included in the Infrastructure Investment and Jobs Act and is also expected to grow. As of 2023, there were over 48,000 public charging stations in the US, and a commitment by the Infrastructure Investment and Jobs Act is in place to increase this number to 500,000 by 2030. The U.S. EV charging infrastructure market size was valued at $3.15B in 2022 and is expected to grow to $24B by 2030. [Grandview]

Given the current value, expected growth, potential for cyber-related attacks, and the criticality of the transportation and energy sectors, the Department of Energy (DOE) in collaboration with the Electric Power Research Institute (EPRI) studied the Electric Vehicle/Extreme Fast Charging ecosystem (EV/XFC ecosystem). Recognizing the need for relevant parties to assess their cybersecurity posture as a part of risk management, the DOE commissioned NIST to apply the NIST Cybersecurity Framework (CSF) to the EV/XFC ecosystem.

This document is the result of that effort. The Cybersecurity Framework Profile for Extreme Fast Charging (XFC) Infrastructure (referred to herein as the EV/XFC Cybersecurity Framework Profile) is a sector-level profile. The EV/XFC Cybersecurity Framework Profile is an application of the Framework Categories and Subcategories in the context of the EV/XFC cybersecurity ecosystem identified by the DOE and EPRI and NIST tailored the CSF to apply to ecosystem. The EV/XFC Cybersecurity Framework Profile provides ecosystem-relevant parties a means to assess and communicate their cybersecurity posture, by addressing risks specific to the ecosystem using the structure of the Cybersecurity Framework. The EV/XFC Cybersecurity Framework Profile provides users with an industry-level risk-based approach for managing cybersecurity activities and facilitates cross-collaboration between the various industry relevant parties, vendors, and end users.

**Fig. 1.** Charging an EV

## 1.1. Purpose

The EV/XFC Cybersecurity Framework Profile is designed to be part of an enterprise risk management program to aid organizations in managing threats to systems, networks, and assets within the EV/XFC ecosystem. The EV/XFC Cybersecurity Framework Profile is not intended to serve as the only solution or as a compliance checklist. Users of this profile will understand that its application cannot eliminate the likelihood of disruption or guarantee some level of assurance.

Use of the Profile will help organizations:

- Identify key assets and interfaces in each of the ecosystem domains.
- Address cybersecurity risk in the management and use of EV/XFC services.
- Identify the threats, vulnerabilities, and associated risks to EV/XFC services, equipment, and data.
- Apply protection mechanisms to reduce risk to manageable levels.
- Detect disruptions and manipulation of EV/XFC services.
- Respond to and recover from EV/XFC service anomalies in a timely, effective, and resilient manner.

## 1.2. Scope

The EV/XFC ecosystem relies on multiple connected domains. This Profile addresses the four major domains in the EV/XFC ecosystem:

- **EV**. EVs come in a variety of shapes and sizes—motorcycles, cars, Electric Vehicle Take-Off and Landing (EVTOL) equipment, such as drones or aircraft, and commercial vehicles (e.g., tractor-trailers, construction vehicles, buses). EVs rely on multiple networking systems to communicate internally and with external entities. Internally, there are control systems for batteries, motors, charging, and the vehicle itself that operates through an internal Control Area Network (CAN). The charger and vehicle communicate

through a physical connector. The vehicle communicates with vendor cloud/third-party organizations via Bluetooth, Wi-Fi, or cellular.

- **XFC/EVSE**. Electric Vehicle Supply Equipment (EVSE) consists of systems that provide electric power to the vehicle to recharge the vehicle's batteries. EVSE systems include electrical conductors, related equipment such as Battery Energy Storage Systems (BESS), software, and communications protocols that deliver energy efficiently and safely to the vehicle. Extreme Fast Charging (XFC) is a type of EVSE that is capable of recharging vehicles in a manner of minutes rather than hours. [Energies-2019] In addition to connecting to the EV, the XFC/EVSE and related equipment must connect and communicate with cloud providers and third-party vendors for providing EVSE location information, billing, and other services.
- **Cloud/Third-Party Organizations**. The EV/XFC ecosystem consists of independently owned and operated domains, and most charging stations are operated by a charging network with business models that blend station, electricity, and vehicle charging sales together. Third parties are individuals or entities that facilitate transactions but are not one of the primary parties within the exchange. The EV/XFC ecosystem typically uses cloud service providers for these transactions because they are suitable for sensitive data exchanges that involve financial information, personally identifiable information (PII), and other potentially sensitive data.
- **Utilities/Building Systems**. Utilities provide the power necessary to fuel the EV/XFC ecosystem. Building and facility management systems may be present in installations where energy management is required, such as EVSE installed at shopping centers, as well as where distributed energy resources (DER) may be present or where physical security control is required. Both utilities and building/facility management systems include equipment to monitor power utilization, communicate with networked devices and supervisory systems, and help control on-site energy demands.

The scope of cybersecurity and enterprise risk management includes operational technology (OT) in addition to information technology (IT). While managing cybersecurity risks is equally important to IT and OT processes, there are considerable operational differences between the two, which may impact the implementation of risk management techniques for IT vs OT. Despite these differences, the interdependencies between IT and OT are increasing, which leads to increasing reliance of OT on IT processes and possibly inherited vulnerabilities and risks between the two technologies.

The EV/XFC ecosystem has always relied on a combination of IT and OT processes. Integrated risk management includes a collaboration of IT and OT professionals to generate integrated assessments, mitigations, and recovery plans.

The foundational concepts used to define the EV/XFC Cybersecurity Framework Profile's scope were derived from previous research and documentation developed by the Electric Power Research Institute (EPRI) [EPRI-2023] as illustrated in Fig. 2 below. Power generation and communications within the utility are outside the scope of the EV/XFC Cybersecurity Framework Profile.

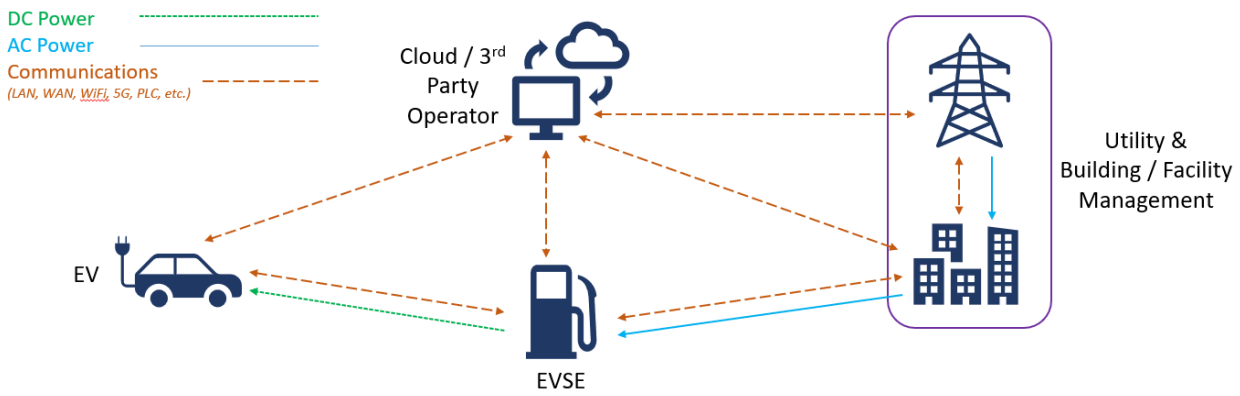


**Fig. 2.** EV/XFC Ecosystem Domains and Profile Scope

## 1.3. Audience

The EV/XFC Cybersecurity Framework Profile may be used by any number of relevant parties within the EV/XFC ecosystem. The relevant parties within the ecosystem are diverse and growing. Members of the ecosystem include:

- EV owners (including individuals in the general public and fleet owners)
- EV manufacturers
- EVSE owners/operators
- EVSE manufacturers
- Cloud/Third-Party providers
- Utility owner/operators
- Building Network Owners/Providers
- Suppliers/Vendors

This document is intended for organizations and relevant parties involved in the EV/XFC industry that use or produce EV/XFC services, systems, and related components such as:

- Public and private organizations that use or provide EV/XFC services
- Managers responsible for the use or provision of EV/XFC services
- Risk managers, cybersecurity professionals, and others with a role in risk management for systems that use or provide EV/XFC services
- Procurement officials responsible for the acquisition of EV/XFC infrastructure or services
- Mission and business process owners responsible for achieving operational outcomes dependent on EV/XFC services

The EV/XFC Cybersecurity Framework Profile is intended for a general audience and is broadly applicable. The Profile applies to organizations that:

- Have already adopted the NIST Cybersecurity Framework to help identify, assess, and manage cybersecurity risks.
- Are familiar with the Framework and want to improve their risk postures.
- Are unfamiliar with the Framework but need to implement risk management frameworks for their organization.

## 2. Intended Use

The EV/XFC Cybersecurity Framework Profile provides a framework that organizations may use to assess their cybersecurity posture (both the "as is" and "to be" states) as a part of their risk management processes and procedures. This profile provides guidance, and its use is voluntary. The Profile provides an assessment methodology for organizations to determine risks and the potential impacts of cyber-based disruptions to the EV/XFC ecosystem. The Profile is intended to help organizations within the EV/XFC community prioritize cybersecurity activities based on their mission objectives.

Additionally, the Profile can be used to help organizations identify areas where standards, practices, and other guidance can help manage risks to systems that use EV/XFC services. An organization can use the Profile in conjunction with its processes for identifying, assessing, and managing risk. The Profile is intended to complement, not replace, the organization's existing risk management processes. This Profile is intended to be used as a foundational profile, and specific organizations can customize the EV/XFC Cybersecurity Framework Profile by considering the following questions:

- What are the mission objectives for the organizations within the ecosystem?
- What processes or assets support the mission objective?
- What processes and assets are vulnerable to disruption or degradation?
- What is the impact to the mission should a process or asset be lost or degraded?
- What are the integrity and availability thresholds of EV/XFC to avoid mission impact?
- What safeguards are available?
- What techniques can be used to detect events of concern?
- What techniques can be used to respond to events of concern?
- What techniques can be used to recover pre-event capabilities?

## 3. EV/XFC Cybersecurity Mission Objectives

The Mission Objective is defined as a high-level goal that must be achieved for an organization to succeed at its primary mission or purpose. Often the development of a Profile starts with the identification of an organization's mission objectives. The EV/XFC Cybersecurity Mission Objectives provide the context for an organization to manage its cybersecurity risk as it relates to

its specific mission needs. To ensure that the Profile aligns cybersecurity outcomes with mission requirements, input from stakeholders and experts in a particular field is critical. CSF Categories and Subcategories especially relevant to each mission objective can then be identified and prioritized to fit the needs of the organization.

Mission objectives identified in this CSF Profile are those that may be common to organizations in the Electric Vehicle Extreme Fast Charging industry but recognizes that individual mission objectives may vary by organization. After identifying the Mission Objectives, an organization can use this information for prioritizing areas of particular concern. Prioritization is meant to be informative rather than prescriptive.

For this profile, between February 2023-May 2023, NCCoE hosted 12 virtual working group sessions for EV/XFC ecosystem and the four major domains in the EV/XFC ecosystem identified above in 1.2 Scope. The working group discussions resulted in four Mission Objectives that characterize high-level critical operational needs to an organization to meet its primary mission in the EV/XFC ecosystem including the four domains. Each organization should consider its own goals and priorities when consulting this Profile and adjust how the organization may apply guidance accordingly. The following Mission Objectives listed in the sections below can serve as a starting point for a particular organization to define their own Mission Objectives but should not be considered an exhaustive list as they do not directly address every technical aspect of the EVSE ecosystem.

## 3.1. Mission Objective 1: Deliver Reliable Performance through Secure Communications

Communicating across the XFC infrastructure is critical to the performance in the EV/XFC ecosystem and the success of the EV industry. Because of this in tandem dependency, the communications should be reliable and secure to fulfill the ecosystem's mission needs. The XFC infrastructure faces many operational and cybersecurity threats and vulnerabilities, especially to its communication infrastructure; therefore, greater attention is needed to secure communications. Secure communications enable fundamental EV/XFC activities, such as charging experience, billing processes, and availability of charging stations.

The rationale for this Mission Objective includes:

- **EV**. Communication between the EV (battery management system) and the charging station is necessary to facilitate the EV battery charging process. The EV connects to cloud/third-party applications to manage the transactions and collect data. EV user systems (e.g., infotainment) also may communicate with other vehicle systems, such as the charge controller and battery management systems. The interface between these applications presents a potential attack surface for malicious actors to cause damage.
- **XFC/EVSE**. The charging station requires secure communication to the cloud to facilitate financial transactions, provide authorization to charge, collect maintenance logs, and receive updates. Additionally, the charging station draws power from the metered utility.
- **Cloud/Third-Party**. Cloud service providers require reliable secure connections to the EV, charging station, and the utility to facilitate the charging process. Secure reliable communications allow for validation of financial transactions, protect personal

information, and allow for maintenance updates and logs to be transmitted quickly and economically.

- **Utility/Building Management Systems**. Utilities and building management systems provide power to the charging station. Coordination between the XFC chargers and utilities is required for various smart grid applications such as peak shaving/load shifting or forecasting. Where this communication exists, it must be reliable and secure.

## 3.2. Mission Objective 2: Maintain Resilience of the XFC Infrastructure

All users in the EV/XFC ecosystem should have reliable access to services. A loss of cybersecurity may impact physical security; therefore, organizations must implement safeguards to ensure the cyber resilience of the EV/XFC ecosystem. All cybersecurity decisions should be balanced with business needs to maintain usability of the system while keeping the ecosystem secure and resilient.

The rationale for this mission objective includes:

- **EV**. EV owners want assurance that their vehicle is protected before they are willing to participate in the charging ecosystem. Batteries are a significant expense, and a compromised XFC ecosystem could potentially lead to physical damage to the battery, EV components, and other nearby equipment. Thus, implemented safeguards will ease the minds of users and encourage them to use the charging stations.
- **XFC/EVSE**. Due to the unique position of charging stations in the ecosystem, geographical dispersion, and general lack of physical security, charging stations have become an appealing target for threat actors. EVSE infrastructures should be protected, both cyber and physical, to prevent attacks like ransomware or damage to the charging infrastructure itself.
- **Cloud/Third-Party**. The cloud/third-party environment facilitates connectivity between domains of the infrastructure. It should be protected to maintain operations.
- **Utility/Building Management Systems**. Utilities and building management systems should have protection systems in place to prevent manipulation of utility components to maintain safe operations.

## 3.3. Mission Objective 3: Build and Maintain Trustworthy Relationships with Partners and Customers

EV/XFC cybersecurity requires collection and use of partner and customer data from many sources. Building and maintaining relationships with relevant parties demands organizations consider and mitigate against risks throughout the information lifecycle. Protecting the confidentiality of sensitive information (e.g., system status information) ensures confidence in the organization and establishes trust among partners and with customers. Personal information should also be protected (e.g., credit card information, individual XFC usage patterns) to ensure that user information is not correlated for inappropriate use, resulting in a loss of trust from users. Cybersecurity disruptions to systems can impact product quality, leading partners, and customers to question the trustworthiness of the organization.

The rationale for this mission objective includes:

- **EV**. EV owners trust that charging stations will be available and operable, will not cause damage to the EV while charging, and will protect their information during transactions.
- **XFC/EVSE**. EVSEs are the most visible representation of the EV/XFC ecosystem, and a cyber incident can have broad impact leaving the public uncertain of the safety, security and reliability of EVs, potentially impacting future sales.
- **Cloud/Third-Party**. Cloud and Third-Party providers capture and maintain sensitive financial information for transactions across the EV/XFC ecosystem. Inadvertent release of this sensitive information can result in a loss of trust from all ecosystem relevant parties as well as result in high costs to the cloud/third-party providers due to fines, civil lawsuits, or compensation to customers.
- **Utility/Building Management Systems**. Disruptions in the power supply may leave EV owners stranded and others in the EV/XFC ecosystem unable to perform their business functions. These types of disruptions erode trust in the EV/XFC ecosystem.

## 3.4. Mission Objective 4: Maintain Continuity of Operations

The EV/XFC ecosystem must sustain operations and ensure the organization's mission continues in the face of adversity. Organizations need to monitor for deviations to identify potential cybersecurity events and detect and respond to anomalous behavior. Cyber supply chain risk management processes should also be identified and agreed to by organizational relevant parties. Moreover, organizations account for disruptions through business continuity/contingency planning and implementation of response and recovery plans. Achieving this objective requires each domain in the EV/XFC ecosystem to work together as expected.

The rationale for this mission objective includes:

- **EV**. Understanding when an EV is compromised or acting outside its normal baseline operation is key to safe and reliable operations of the vehicle.
- **XCF/EVSE**. To detect anomalous behavior, it is necessary to understand the stations' charging cycle profile and power consumption to identify deviations from normal operations, which may indicate malicious behavior. Supply chain issues (e.g., quality, integrity, availability) impact the reliability of EVSE.
- **Cloud/Third-Party**. Cloud/Third-Party entities must be able to identify malicious behaviors that deviate from cybersecurity baselines (e.g., unknown, or new connections and/or transmissions from sources other than the service provider or authorized by the service provider).
- **Utility/Building Management Systems**. Utilities typically have programs in place to detect anomalous activity from external systems that could impact operations.

# 4. Overview of the Cybersecurity Framework

This section was derived from Version 1.1 of the NIST Cybersecurity Framework (CSF), and the reader is advised to consult the CSF and its corresponding quick start guide for additional details

[NIST-CSF] [NIST-SP1271]. The CSF assists organizations in better managing and reducing cybersecurity risk in a way that responds to the industry's unique cybersecurity needs, risks, threats, and/or cyber sophistication (regardless of its size). The Framework provides an approach to analyzing cybersecurity risk, enabling enterprises to understand their cybersecurity challenges, and selecting appropriate mitigation strategies. The Framework emphasizes the risk management process for cybersecurity by stating that "the Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management process" [NIST-CSF].

The Framework presents industry standards, guidelines, and practices in a manner that allows cybersecurity activities and outcomes to be clearly communicated at all levels of an organization, from executives to individuals with operational job roles. Building on those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

- Describe their current cybersecurity posture.
- Describe their target state for cybersecurity.
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
- Assess progress toward the target state.
- Communicate among internal and external relevant parties about cybersecurity risk.

The Framework consists of three main components: the Core, Profiles, and Implementation Tiers. The Core is a catalog of cybersecurity outcomes written in a common language. A Framework profile is an alignment of organizational requirements, objectives, risk appetite, and resources against the desired outcomes of the Framework Core. Implementation Tiers guide organizations to consider the appropriate level of rigor for their cybersecurity program and can be used as a communication tool to discuss risk appetite, mission priority, and budget; further discussion on Implementation Tiers is not included in this profile.

## 4.1. The Framework Core

The Framework Core consists of five Functions [NIST-CSF]:

- **Identify**. The activities in the Identify function are the foundation for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus on and prioritize its efforts, consistent with its risk management strategy and business needs.
- **Protect**. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event.
- **Detect**. The Detect function enables timely discovery of cybersecurity events.
- **Respond**. The Respond function supports the ability to contain the impact of a potential cybersecurity event.
- **Recover**. The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event.

When considered together, these functions provide a high-level, strategic view for managing cybersecurity risk. The Framework further identifies underlying key Categories and Subcategories for each function and matches them with example informative references such as existing standards, guidelines, and practices for each subcategory. As stated previously, the informative references are meant to be used as examples of best practices and to provide relevant information and are by no means any type of regulatory or compliance mandate from the perspective of this guidance **Table 1** illustrates the alignment of Categories to Functions.

**Table 1.** Function and Category Unique Identifiers of NIST CSF 1.1

| Function | Function Unique Identifier | Category | Category Unique Identifier |
|---|---|---|---|
| IDENTIFY | ID | 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 | PR | Access Control | PR.AC |
| | | Awareness and Training | PR.AT |
| | | Data Security | PR.DS |
| | | Information Protection Processes and Procedures | PR.IP |
| | | Maintenance | PR.MA |
| | | Protective Technology | PR.PT |
| DETECT | DE | Anomalies and Events | DE.AE |
| | | Security Continuous Monitoring | DE.CM |
| | | Detection Processes | DE.DP |
| RESPOND | RS | Response Planning | RS.RP |
| | | Communications | RS.CO |
| | | Analysis | RS.AN |
| | | Mitigation | RS.MI |
| | | Improvements | RS.IM |
| RECOVER | RC | Recovery Planning | RC.RP |
| | | Improvements | RC.IM |
| | | Communications | RC.CO |

The Framework Categories decompose into Subcategories that are more detailed cybersecurity activities and specific outcomes of technical and/or management activities. The final components of the Framework Core are informative references. Informative references map the Subcategories and provide the reader with existing standards, guidelines, and practices that can help an organization achieve the desired outcome for each subcategory.

Profile development applies the Cybersecurity Framework in focusing on the cybersecurity areas of particular concern to an industry, organization, or functional area as identified through its risk management processes. By evaluating the elements of the Cybersecurity Framework in the context of a particular mission, organization, or sector, a profile is created that shows the organization's cybersecurity posture based on evaluation of the mission against the Cybersecurity Framework Functions, Categories, and Subcategories.

Profiles are used to identify opportunities for improving an organization's cybersecurity posture by creating and comparing a "current" profile (the "as is" state) with a "target" profile (the "to

be" state). A target profile offers a prioritization of Subcategories based on pressing mission and operational considerations for a specific community, industry, or group of relevant parties. Target profiles are a basis for identifying and engaging in discussions about cybersecurity activities and outcomes that are important to the profile's user community. Within an organization, profiles offer a consistent way to discuss cybersecurity objectives across organizational or agency roles—from senior leadership to technical implementors—using common terminology. Individuals within the organization or agency may use the gaps between the current and target profiles to discuss prioritization and allocation of resources to meet cybersecurity objectives.

## 4.2. Sector-Level Profiles

Sector-level profiles emerged as a concept after the development of the CSF. Sector-level profiles can act as a starting point for members of the sector to develop their organization's "current" or "target" profile. Sector-level profiles provide a basis for sub-sectors and individual organizations to facilitate conversations and discuss security activities using consistent terminology. Sector-level profiles are intended to:

- Provide a foundational profile for organizations to augment or tailor specific to their organizational needs.
- Decrease the chance that organizations overlook a category or subcategory.
- Encourage consistent analysis of cybersecurity-risk in the sector ecosystem/environment.
- Align sector and regulatory cybersecurity requirements or needs.

Developing sector-level profiles can be facilitated through a collaborative, community of interest (COI) driven process. To ensure that a profile aligns cybersecurity outcomes with mission and business needs, input from relevant parties and experts in the targeted field is critical.

# 5. XFC Baseline Profile

The XFC Baseline Profile was created by using the Cybersecurity Framework as described in Sec. 4. The baseline profile consists of tables for each Category that summarize how each associated subcategory applies generally to the EV/XFC ecosystem with informative references for additional guidance. The tables provide domain-specific considerations as appropriate.

By design, the Cybersecurity Framework is flexible to accommodate the unique environments and needs of different organizations. Users of this document will understand that deviations between their enterprise and the assumptions made in this profile may impact the applicability of the Subcategories. ***Therefore, relevant parties are advised to review all the Subcategories in the context of their organization.***

## 5.1. Identify Function

Cybersecurity decisions are not made in a vacuum but within the context of each organization's business goals and objectives. Decision making evaluates alternatives based on their potential impact on the business.

The Identify function is the foundation of the risk assessment process, so risk management practitioners should start there first. Consideration of the organization's mission and business objectives, threat environment, assets, and vulnerabilities will have significant influence on the overall risk management decision and will also impact the other four Functions (i.e., Protect, Detect, Respond, Recover).

The objectives of the Identify function include:

- Identifying the business or operational environment and organization's purpose
- Identifying all assets, including hardware, software, personnel, roles, and responsibilities, and assets' criticality
- Identifying infrastructure that provides EV/XFC functionality
- Identifying the current and trending vulnerabilities, threats, and impacts should the threat be realized to assess the risk.

The Identify function consists of six Categories:

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management
- Supply Chain Risk Management

Each of these Categories and associated Subcategories is summarized in Sec. 5.1.1 through Sec. 5.1.6.

### 5.1.1. Asset Management Category

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistently with their relative importance to organizational objectives and the organization's risk strategy.

In the context of the ecosystem, managing these resources provides the information needed to inform ongoing decision making consistent with the organization's business objectives and risk strategy. The domains within the EV/XFC ecosystem operate independently to achieve common goals. However, to best manage and use their resources, interdependencies and collaborations should be considered among the domains.

**Table 2.** Identify: Asset Management Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AM-1:**<br>Physical devices and systems within the organization are inventoried. | **Ecosystem:** Hardware inventory is a basic function that supports security and management. The inventory's ability to support security and management is dependent on its accuracy and granularity. Factors that contribute to accuracy include how frequently inventories are performed, how thoroughly the inventory is performed (through means such as automation), and the use of physical inspections or other mechanisms for verification. Factors that contribute to granularity of the inventory include information such as the manufacturer, model number, serial number, version, its function, or its enabled (or disabled) capabilities. Consideration should be given to including rented or leased equipment in the inventory in addition to assets that are directly owned and managed by the organization. A comprehensive inventory may define subsystems, components, or subassemblies as distinct physical assets. | **[NIST SP 800-53r5]**<br>CM-8, PM-5<br>**NERC CIP**<br>002-5.1a-R1 |
| **AM-1 \| EV** | No additional domain-specific considerations to EV manufacturers once the vehicle is delivered to the customer; however, manufacturers may catalogue the equipment installed in their vehicles and consider providing that information to EV owners as needed.<br>EV owners may consider being aware of the basic information about their vehicle, such as voltage ratings, rated charging current, charging method (alternating current (AC) or direct current (DC)) and charging connector type. | **[NIST SP 800-53r5]**<br>CM-8, PM-5 |
| **AM-1 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST SP 800-53r5]**<br>CM-8, PM-5<br>**[NIST Handbook 44]**<br>1.10 G-S.1(a)-(c), G-S.2, G-S.6<br>**ISA/IEC 62443-2-1:D4E1**<br>CM 1.1<br>**ISA/IEC 62443-3-3:2013**<br>SR 7.8<br>**OIML D31:2019**<br>6.2.2.1.1<br>**OIML G22:2022**<br>4.1, 5.1 |
| **AM-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST SP 800-53r5]**<br>CM-8, PM-5 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AM-1 \| Utility/Building Management System** | Applicable, but no additional Utility Building/Management System-specific considerations. | **[NIST SP 800-53r5]** CM-8, PM-5<br>**ISA/IEC 62443-2-1:D4E1** CM 1.1<br>**ISA/IEC 62443-3-3:2013** SR 7.8 |
| **AM-2:**<br>Software platforms and applications within the organization are inventoried. | **Ecosystem:** Accurate and current software inventory is considered a basic security function. The software inventory may include developer and version information, associated hardware, update history, and known bugs. The inventory should consider tracking how software is used and updated so that extraneous, outdated, or vulnerable software can be properly managed. Comprehensive software inventories may use a software bill of materials (SBOM) to track any software dependencies that may have an impact on the software's function. | **[NIST SP 800-53r5]** CM-5, CM-8, CA-9, SA-8<br>**NERC CIP** 002-5.1a-R1 |
| **AM-2 \| EV** | EV manufacturers should consider routinely pushing or providing software updates and patches to EV owners and relevant third parties. | **[NIST SP 800-53r5]** SA-8<br>**ISO 24089:20231** |
| **AM-2 \| XFC/EVSE** | EVSE manufacturers should consider routinely pushing and patching software updates and patches to EVSE owners and relevant third parties. | **[NIST Handbook 44]** 1.10 G-S.1(d), G-S.2, G-S.9<br>**[NIST SP 800-53r5]** SA-8<br>**OIML D31:2019** 6.1.1, 6.2.2.2.2, 6.2.8.4<br>**OIML G22:2022** 4.4.2, 4.4.7, 5.1<br>**ISA/IEC 62443-2-1:D4E1** CM 1.1<br>**ISA/IEC 62443-3-3:2013** SR 7.8 |
| **AM-2 \| Cloud/Third-Party** | Cloud/Third-Party owners/operators may consider including any external third-party software hosted on or connected to the systems. | **[NIST SP 800-53r5]** SA-8 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AM-2 \| Utility/Building Management System** | Utility/Building management owners/may consider including external third-party software hosted on their systems in the software inventory. | **[NIST SP 800-53r5]** CM-5, SA-8<br>**ISA/IEC 62443-2-1:D4E1** CM 1.1<br>**ISA/IEC 62443-3-3:2013** SR 7.8 |
| **AM-3:**<br>Organizational communication and data flows are mapped. | **Ecosystem:** Consider all data flows, internal data flows; within systems, between systems within an organization, and any external or third-party flows. Mapped data flows should consider showing how different types of data are communicated, requirements for transmission, and information on path redundancies. Catalogued information may include any communication and encryption protocols used, associated sensors and end points, and any associated connectors or possible connection points. | **[NIST SP 800-53r5]** AC-4, CA-3, CA-6, CA-9, PM-10, PL-8, SA-17, AC-20<br>**NERC CIP** 002-5.1a-R1,011-2-R1 |
| **AM-3 \| EV** | This mapping may include communication and data relating to vehicle identification, system information, battery statistics, payment information, accounts, etc. Data path/flow diagrams should consider including the EV wire harness and each relevant electric control unit (ECU). Diagrams may also show how ECUs are connected to communication buses, sensors, and actuators, the communication protocols they use, physical location of hardware in the EV, any available ports, and the directionality of communications. | **[NIST SP 800-53r5]** CA-3, CA-6, CA-9 |
| **AM-3 \| XFC/EVSE** | XFC/EVSE interfaces should consider ensuring that only necessary data are sent or received to fulfill their task. It may be necessary to consider measures to avoid an indirect exchange of information between the EV and the utility domain. Consider also including EVSE- and EV-specific interfacing, as well as any communication to any cloud/third-party systems or utility/building management systems. | **ISA/IEC 62443-2-1:D4E1** NET 1.01<br>**OIML D31:2019** 7.1.2, 7.3.2.4<br>**OIML G22:2022** 5.1 |
| **AM-3 \| Cloud/Third-Party** | Cloud/Third-Party members should consider including business and operations-specific flows within the organization as well as interactions with external partners and entities, including EVSE, utilities, building/facility management systems, and transaction management systems. Consider paying particular attention to Payment Card Industry (PCI) data flows and data flows to and from data leaks. | **[NIST SP 800-53r5]** CA-3, CA-6, CA-9 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AM-3 \| Utility/Building Management System** | Consider paying particular attention to data leaks. Data path/flow diagrams should consider showing relevant utility/substation Supervisory Control and Data Acquisition (SCADA) system layouts including Programmatic Logic Controllers (PLCs), Human Machine Interfaces (HMIs), and the equipment they control. Diagrams may show how the cloud network communicates information to the utility. The diagrams can show how information flows and the communication protocols they use. | **[NIST SP 800-53r5]** CA-3, CA-6, CA-9<br>**ISA/IEC 62443-2-1:D4E1** NET 1.01 |
| **AM-4:**<br>External information systems are catalogued. | **Ecosystem:** Catalogue external partner connections and level of access to external information systems, establish processes and agreements with all external partners to ensure an understanding of information system usage, and establish a level of trust and security that is consistent with the policies of the organization. | **[NIST SP 800-53r5]** AC-20, PM-5, SA-9<br>**NERC CIP** 011-2-R1 |
| **AM-4 \| EV** | This may include cataloging EVSE connections to EV, processes used to verify EV identity and accounts, and charge profile information (current, capacity, battery health, etc.) communication. EV connections to cloud-based systems, including account, profile, and location information, should consider also being included. | **[NIST SP 800-53r5]** AC-20, PM-5, SA-9 |
| **AM-4 \| XFC/EVSE** | External information systems that EVSE interfaces with may include EV-specific systems as well as any communication to any cloud/third-party operators or utility/building management systems. EVSE functionality may be dependent upon external information systems to support EVSE connections to EV, to the utility (data flow for power metering, account billing, and demand forecasting) and connections to cloud (to support data flow for charge station search and reservation and billing information). | **ISA/IEC 62443-2-1:D4E1** ORG 1.1 |
| **AM-4 \| Cloud/Third-Party** | Cloud/Third-Party owners/operators may include interactions with external partners, systems, and entities, such as EVSE, utilities, building/facility management systems, and transaction management systems. | **[NIST SP 800-53r5]** AC-20, PM-5, SA-9 |
| **AM-4 \| Utility/Building Management System** | Some aspects of utility or building/facility management require external information systems for proper operation and support EVSE connections to utility and cloud-based systems for functions such as demand forecasting. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1 |
| **AM-5:**<br>Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value. | **Ecosystem:** Identification and prioritization of the criticality and business value of assets are pre-requisites for allocation of resources and enable risk management decisions to either reduce or accept the residual risk. Prioritization of assets allows an organization to focus on the most pending needs first. Special consideration should be considered for user safety, financial, and privacy/personally identifiable information security during prioritization. | **[NIST-SP800-37r2]**<br>**[NIST-SP800-53r5]** AC-20, CP-2, CP-8, RA-2, RA-9, SA-20, SC-6 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AM-5 \| EV** | EV manufacturers have an additional concern in that they will be supporting equipment and systems already in the customer's possession and use. In addition to their current assets, manufacturers may consider the importance of resources necessary to support discontinued models. | **[NIST-SP800-53r5]** AC-20, RA-2, RA-9, SA-20, SC-6 |
| **AM-5 \| XFC/EVSE** | The prioritization of resources will be influenced by the XFC/EVSE's ability to support different makes and models of EV. The resource prioritization may be updated as the number and variety of EVs change.<br><br>XFC/EVSE stations are geographically diverse, and the local owners/operators may have different risk tolerances. As such, the evaluations may be adjusted based on local threat assessments, vulnerabilities of local equipment, local risk assessments, and the individual owners' tolerance. EVSE manufacturers may consider supporting equipment and systems already in the customer's possession and use, which would influence the prioritization process. EVSE owners/operators can acknowledge that prioritization may be adjusted based on geographical location in addition to the equipment/system type and model. This may mean defining what types of EVs are eligible to charge during times of decreased availability. For example, emergency response EVs may be prioritized during an emergency to ensure that their missions are upheld. | **ISA/IEC 62443-2-1:D4E1** DATA 1.1<br><br>**OIM D31:2019** 6.2.2.2.4 |
| **AM-5 \| Cloud/Third-Party** | Criticality to customer and partners organizations may be part of the prioritization. | **[NIST-SP800-53r5]** AC-20, RA-2, RA-9, SA-20, SC-6 |
| **AM-5 \| Utility/Building Management System** | Consumers may be elements of the critical infrastructure (such as shipping or disaster recovery). This may mean prioritizing what loads receive power during a time of decreased availability and communicating that prioritization with partners. | **[NIST-SP800-53r5]** AC-20, RA-2, RA-9, SA-20, SC-6<br><br>**ISA/IEC 62443-2-1:D4E1** DATA 1.1 |
| **AM-6:**<br><br>Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established. | **Ecosystem:** Clear definition of roles and responsibilities enables coordination of cybersecurity programs. The roles and responsibilities for external organizations such as customers, partners, third parties, and suppliers may be defined in advance on a case-by-case basis. Consider putting memorandums of understanding or other agreements in place to facilitate tracking a participant's performance and hold them accountable for their responsibilities. Role and responsibility definitions should consider including details about authorities across domains, cover the entire cybersecurity posture of an organization including accounting for external relevant parties, and detail the level of transparency required for accountable and acceptable use, storage, and interaction with intellectual property. | **[NIST-SP800-53r5]** CP-2, PM-2, PM-11 PM-29,PS-2, PS-7<br><br>**NERC CIP** 004-6-R4, 004-6-R2 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AM-6 \| EV** | Additional relevant parties for EV manufacturers include elements of the workforce involved in vehicle design, and pre/post-sales support. EV owners may be made aware of methods and opportunities for good cyber hygiene as it relates to their EV usage, as well as informed on the responsibilities to the customer of their vehicle manufacturer. | **ISO/SAE 21434** RQ-07-04, RQ-07-06 |
| **AM-6 \| XFC/EVSE** | Additional relevant parties for EVSE manufacturers should consider including elements of the workforce involved in equipment design/usage, pre/post-sales support, and those involved during EVSE installation design and construction. | **ISA/IEC 62443-2-1:D4E1** ORG 1.3 |
| **AM-6 \| Cloud/Third-Party** | Extra emphasis may be placed on external partner relationships due to the requirement for externally sourced operational data. | **[NIST-SP800-53r5]** CP-2, PM-2, PM-29 |
| **AM-6 \| Utility/Building Management System** | Utilities and network building should consider defining the roles and responsibilities in context of rules and regulations that apply to the energy sector. Extra emphasis may be placed on physical security personnel to protect the physical operating environment and infrastructure against cybersecurity risks. | **ISA/IEC 62443-2-1:D4E1** ORG 1.3 |

### 5.1.2. Business Environment Category

The organization's mission, objectives, relevant parties, and activities are understood and prioritized by organizations; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

In the context of the EV/XFC ecosystem, organizations will understand the business environment for relevant parties from across domains and how it impacts their specific domain.

**Table 3.** Identify: Business Environment Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **BE-1:** The organization's role in the supply chain is identified and communicated. | **Ecosystem:** Degree of applicability and role in the supply chain is domain specific. In general, identification of the role in the supply chain are pre-requisites for supply risk management and communication of the role facilitates definition of thresholds, service level agreements, memorandums of understanding and other commitments. Identifying and understanding relationships and interfaces with suppliers influences the organization's role in the supply chain. The organization's role in the supply chain is influenced by system interdependencies that may impact supply chain positions and agreements. Subcomponents (e.g., microcontrollers, sensors, electrical wiring, connectors.) critical to the function of onboard controllers and management systems may be considered when identifying how supply chain roles impact goods/services. | **[NIST-SP800-53r5]** SR-1, SR-3 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **BE-1 \| EV** | EV manufacturers' role in the supply chain may include relationships and interfaces with suppliers, customers, EVSE manufacturers/operators, and cloud/third-party operators. | **ISO/SAE 21434** RQ-07-04, WP-07-01 |
| **BE-1 \| XFC/EVSE** | EVSE manufacturers' role in the supply chain may include that of an equipment manufacturer, consumer/holder of data from EV owners, and a developer of tools used for communication within the EV/XFC ecosystem. EVSE owners/operators may consider following a similar path, understanding their position in the supply chain as a user/maintainer of EVSE systems and service provider to EVs. | **ISA/IEC 62443-2-1:D4E1** ORG 1.6 |
| **BE-1 \| Cloud/Third-Party** | Cloud/Third-Party owners/operators' role in the supply chain typically includes a service provider and consumer/holder of data from other EV/XFC entities. Additionally, identified dependencies and requirements may be communicated internally and with impacted business partners. | **[NIST-SP800-53r5]** SR-1, SR-3 |
| **BE-1 \| Utility/Building Management System** | Utility/building management systems' role in the supply chain may include a service provider, and consumer/holder of data. | **[NIST-SP800-53r5]** SR-1, SR-3 |
| **BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated. | **Ecosystem:** Transportation and energy are considered critical infrastructure sectors; however, the degree to which the subcategory applies is domain specific. | **[NIST-SP800-161]** **[NIST-SP800-53r5]** PM-8 |
| **BE-2 \| EV** | EV manufacturers should consider educating/informing their customers about their vehicle's capability to charge from/communicate with various types of infrastructure safely. This may include informing EV owners of which types of charge connectors are compatible with their vehicle, when connector adapters are applicable, what charge station characteristics are required (voltage, current ratings, DC/AC), or more specifically, what EVSE brands/models or third-party apps are compatible with their EV. The EV manufacturer may consider communicating the risks and/or potential consequences of failing to adhere to these recommendations. | **[NIST-SP800-161]** **[NIST-SP800-53r5]** PM-8 **ISO/SAE 21434** RQ-10-03 |
| **BE-2 \| XFC/EVSE** | The EVSE owners/manufacturers can communicate how service/availability to EV owners could be limited and how the EVSE may behave relative to the utility during a period of lost or degraded energy availability or communications. EVSE manufacturers/owners may consider identifying the relationship of industry competitors as alternatives in the event of emergency to ensure the sustainment of critical infrastructure operation. | **[NIST-SP800-161]** **[NIST-SP800-53r5]** PM-8 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **BE-2 \| Cloud/Third-Party** | Identified dependencies and requirements may be communicated internally and with impacted business partners. EVSE reservation and alternative billing options to cloud/third-party use should consider being defined for use in the event of degradation or an outage. | **[NIST-SP800-161]** **[NIST-SP800-53r5]** PM-8 |
| **BE-2 \| Utility/Building Management System** | Identified dependencies and requirements may be communicated internally and with impacted business partners. | **[NIST-SP800-161]** **[NIST-SP800-53r5]** PM-8 |
| **BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated. | **Ecosystem:** Prioritization guides the organization's strategic activities as it operates and interfaces with customers and partners within the EV/XFC ecosystem. Current and future regulations and contractual obligations may influence the organization's priorities. Ecosystem members can consider prioritizing operator safety and personal information security in their organizational missions, objectives, and activities. | **[NIST-SP800-53r5]** PM-11 |
| **BE-3 \| EV** | EV manufacturers may consider emphasizing the cybersecurity and operational requirements of partners in the EV/XFC ecosystem in the prioritization process. | **[NIST-SP800-53r5]** PM-11 |
| **BE-3 \| XFC/EVSE** | EVSE manufacturers and owners/operators should consider emphasizing the cybersecurity and operational requirements of partners within the EV/XFC ecosystem in the prioritization process. | **[NIST-SP800-53r5]** PM-11 |
| **BE-3 \| Cloud/Third-Party** | Cloud/Third-Party owners/operators may consider focusing more on secure communications and operational requirements/dependencies of partner organizations within the EV/XFC ecosystem in the prioritization process. | **[NIST-SP800-53r5]** PM-11 |
| **BE-3 \| Utility/Building Management System** | Utility/Building management owners/operators may consider additional focus on stability and integrity of the grid and the operational requirements/dependencies of partner/customer organizations within the EV/XFC ecosystem in the prioritization process. | **[NIST-SP800-53r5]** PM-11 |
| **BE-4:** Dependencies and critical functions for delivery of critical services are established. | **Ecosystem:** EV/XFC ecosystem members may consider understanding their position within the EV/XFC ecosystem to properly identify dependencies and critical functions, both internal and external, that may impact their delivery of goods and services to customers and partners. For example, communications between the EVSE and other systems could be a critical function for the ecosystem. In the event of primary communication disruption, redundancies or alternative communication avenues could allow operation to continue at some level and insulate downstream functions from failure propagation. | **[NIST-SP800-53r5]** CP-2, CP-8, PE-9, PE-11, PM-8, RA-9, SA-20, SR-2 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **BE-4 \| EV** | Interdependencies may include finding available charging stations, making reservations, billing the transaction, and connecting to/communicating with the charging station. EVs that do not communicate correctly with the EV charger and/or cloud could incorrectly pay for services, leak personal identifiable information (PII), or cause harm to the EV, EVSE, utility/building infrastructure, or user/owner. | **ISO/SAE 21434** RQ-15-01, RQ-15-02 |
| **BE-4 \| XFC/EVSE** | EVSE manufacturers may consider understanding their position in the EV/XFC ecosystem, both as an equipment manufacturer/supplier and provider that others depend upon. EVSE manufacturers may recognize that providing safe and reliable patches as well as support to operators are critical functions. EVSE owners/operators may consider following a similar path, understanding their position in the ecosystem as a service provider with multi-directional dependencies and critical functions. Interdependencies may include receiving utility power to transform for EV, receiving booking requests from the EV via cloud apps, and effective collaboration with third parties to charge EV owners for purchase. | **ISA/IEC 62443-2-1:D4E1** AVAIL 1.2 |
| **BE-4 \| Cloud/Third-Party** | Cloud/Third-Party owners/operators may have layered dependencies due to being a service provider, as well as partner of and consumer/holder of data from other EV/XFC entities. Depending upon organizational and operational designs, the cloud/third-party owners/operators may also provide multiple critical functions within the EV/XFC ecosystem. Interdependencies may include communications with EVSE regarding current status and availability. | **[NIST-SP800-53r5]** CP-2, CP-8, PE-9, PE-11, PM-8 |
| **BE-4 \| Utility/Building Management System** | Depending upon organizational and operational designs, the utility/building management owners/operators may also provide multiple critical functions within the EV/XFC ecosystem. Interdependencies may include proper electricity rate/tariff selection to temper demand and accurate billing for services. Critical functions may include reliable distribution of power to critical loads. | **ISA/IEC 62443-2-1:D4E1** AVAIL 1.2 |
| **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). | **Ecosystem:** EV/XFC ecosystem members may consider defining how they will remain in business during various scenarios, including planning on how to work with partner organizations to address issues and concerns identified in the scenarios. Graceful degradation of operations and operating at reduced capacities are preferrable to complete failure during attack and recovery. Resilience plans may include details for how operating states are defined, operational adjustments in each state, and necessary communications. | **[NIST-SP800-53r5]** CP-2, CP-11, RA-9, SA-8, SA-20<br>**IEC 61850-90-4** 12.2, 14.2.4<br>**NERC CIP** 009-6-R1 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **BE-5 \| EV** | EV manufacturers may consider the potential severity associated with impacts to EV owners. These requirements could include the ability to respond to a malicious EVSE/Third-Party or to protect the EV in the event of EV manufacturers equipment compromise. The EV manufacturer may consider how EV use may change during an ecosystem disruption and how the EV may recommend behavioral changes to the driver. For example, if a cyber-attack limits EVSE operability, the EV may recommend planning to charge at home. | **[NIST-SP800-53r5]** CP-2, CP-11<br>**IEC 61850-90-4** 12.2, 14.2.4 |
| **BE-5 \| XFC/EVSE** | EVSE manufacturers can consider providing designs and support to help EV/XFC partners achieve their resiliency targets. These requirements, for example, could include the ability to respond to malicious EV firmware. The EVSE can consider communicating how operations will continue in the event of decreased power availability. This may include changes to reservations, charge time, and pricing. | **[NIST Handbook 44]** 3.40 S.2.1, S.2.2, S.2.3<br>**ISA/IEC 62443-2-1:D4E1** AVAIL 1.1<br>**OIML D31:2019** 6.2.5.3<br>**OIML G22:2022** 4.4.9.3.1, 4.49.3.2 |
| **BE-5 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CP-2, CP-11<br>**IEC 61850-90-4** 12.2, 14.2.4 |
| **BE-5 \| Utility/Building Management System** | Depending on organizational and operational designs, the utility/building management owners/operators may rely on, as well as provide support to, EV/XFC partners. The utility may consider defining priorities for distribution and planning for decreased service capacity. | **ISA/IEC 62443-2-1:D4E1** AVAIL 1.1 |

### 5.1.3. Governance Category

The policies, procedures, and processes that manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are documented, reviewed, and inform the management of cybersecurity risk.

The EV/XFC ecosystem spans several sectors, and the domains will have unique operational requirements. There is a wide range of legal and regulatory requirements across the ecosystem. A domain may benefit from an awareness of the rest of the ecosystem's constraints and requirements.

**Table 4.** Identify: Governance Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **GV-1:**<br>Organizational cybersecurity policy is established and communicated. | **Ecosystem:** EV/XFC ecosystem may collaborate on policies with external organizations within the domain to ensure consistency and should also consider inputs from partner companies within the ecosystem to ensure interoperability. Additionally, policies may be defined to account for activities, roles, and responsibilities to manage operational systems, regulatory requirements, update and maintenance strategies, or applicable industry standards among other considerations. | **[NIST-SP800-53r5]**<br>AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1<br>**ISO/SAE 21434**<br>**NERC CIP**<br>004-6-R2 |
| **GV-1 \| EV** | Applicable, but no additional EV-specific considerations. | **ISO/SAE 21434**<br>RQ-05-01, RQ-05-02, RQ-05-03, RQ-05-04, RQ-05-05, RQ-05-09.<br>WP-05-01<br>**ISO 24089:2023** |
| **GV-1 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 1.1 |
| **GV-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]**<br>CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1 |
| **GV-1 \| Utility/Building Management System** | Applicable, but no additional Utilities/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 1.1 |
| **GV-2:**<br>Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners. | **Ecosystem:** Agreements with external organizations or partners are typically made in advance and documented in a service-level agreement (SLA), memorandum of understanding (MOU), or other forms of agreement. These agreements clearly define cybersecurity roles and responsibilities to properly define how their cybersecurity programs should function in a coordinated manner and allow for accountability for participant responsibilities. | **[NIST-SP800-53r5]**<br>PM-1, PM-2, PM-29, PS-7, PS-9 |
| **GV-2 \| EV** | Roles and responsibilities may include those involved in vehicle design, pre/post-sales support, software/firmware lifecycle activities, and supporting nominal vehicle operations such as charging, maintenance, and patching. | **ISO/SAE 21434**<br>RQ-07-04, RQ-07-06, WP-07-01 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **GV-2 \| XFC/EVSE** | Roles and responsibilities may include those during EVSE installation design, construction, maintenance, updating, and operation. EVSE manufacturers can also consider defining roles to better support the needs of EV/XFC partners and customers, which may follow established OT or IT processes and methods for equipment, remote services, and capabilities. | **ISA/IEC 62443-2-1:D4E1** ORG 1.3 |
| **GV-2 \| Cloud/Third-Party** | Applicable, no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** PM-1, PM-2, PM-29 |
| **GV-2 \| Utility/Building Management System** | Applicable, no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.3 |
| **GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. | **Ecosystem:** Understanding the cybersecurity legal and regulatory requirements published and planned for their industry sector allows the elements of the ecosystem to comply with the requirements in a manner that is compatible with the organizations other obligations and goals. Requirements may include privacy, customer data security/management, and regulatory obligations. | **[NIST-SP800-53r5]** AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1 |
| **GV-3 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** SA-1, SC-1, SI-1, SR-1 |
| **GV-3 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1 |
| **GV-3 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** SA-1, SC-1, SI-1, SR-1 |
| **GV-3 \| Utility/Building Management System** | Applicable, but no additional Utilities/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1 |
| **GV-4:** Governance and risk management processes address cybersecurity risks. | **Ecosystem:** EV/XFC ecosystem members may consider ensuring that cybersecurity risks are included in processes conducted within organizational governance and risk groups. Management processes may include policies, procedures, lifecycle activities, and contractual or regulatory requirements. | **[NIST-SP800-53r5]** PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, RA-1, RA-2, RA-3, SA-2<br>**[NIST-SP800-160V1]** 3.3.8<br>**ISO/SAE 21434** |
| **GV-4 \| EV** | Applicable, but no additional EV-specific considerations. | **ISO/SAE 21434** RQ-05-01, RQ-05-02, RQ-05-03, RQ-05-04, RQ-05-05, WP-05-01 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **GV-4 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 2.1 |
| **GV-4 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** PM-3, PM-7, PM-9, PM-10, PM-11, PM-28<br>**[NIST-SP800-160V1]** 3.3.8 |
| **GV-4 \| Utility/Building Management System** | Applicable, but no additional Utilities/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 2.1 |

### 5.1.4. Risk Assessment Category

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

There is a high level of interaction and interdependence of OT and IT within the EV/XFC ecosystem, so consideration of a coordinated or hybrid approach of OT and IT risk assessment is warranted.

**Table 5.** Identify: Risk Assessment Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **RA-1:**<br>Asset vulnerabilities are identified and documented. | **Ecosystem:** EV/XFC ecosystem may consider a robust and timely process to identify, document, and report vulnerabilities that exist in their assets. Perform periodic scanning and testing at a frequency consistent with policy and whenever there have been modifications to the system.<br>This ecosystem has custom assets with software performing key functions. These assets can have vulnerabilities that are not detected by typical scanning tools. Special considerations for niche firmware and software are warranted. | **[NIST-SP800-53r5]** CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5<br>**Auto-ISAC**<br>**E-ISAC**<br>**NERC CIP** 007-6-R2 |
| **RA-1 \| EV** | Consider participation in forums such as Auto-ISAC to gain information regarding vulnerabilities. Known asset vulnerabilities may include accessible connector ports, etc. | **ISO/SAE 21434** RQ-08-05, WP-09-01 |
| **RA-1 \| XFC/EVSE** | Known asset vulnerabilities may include accessible connector ports, poor EVSE physical security, EVSE devices running outdated kernels, unsigned firmware, remotely accessible EVSE devices. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.9 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **RA-1 \| Cloud/Third-Party** | Known asset vulnerabilities may include poor password protection, lack of authentication (e.g., client-side validation, unsanitized log-on fields) | **[NIST-SP800-53r5]** CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 |
| **RA-1 \| Utility/Building Management System** | Consider participation in forums such as E-ISAC to gain information regarding vulnerabilities. Known asset vulnerabilities may include poor password protection, outdated control infrastructure software, and poor substation physical security. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.9 |
| **RA-2:** Cyber threat intelligence is received from information sharing forums and sources. | **Ecosystem:** EV/XFC ecosystem members should consider maintaining an awareness of cyber threat intelligence sources along with cyber threat reports that relate to organizational assets. Ecosystem members may routinely review threat reports to compare with equipment catalogues and check for applicable vulnerabilities or actionable information. | **[NIST-SP800-53r5]** PM-15, PM-16, RA-10, SI-5<br>**[NIST-SP800-150]**<br>**NERC CIP** 007-6-R2 |
| **RA-2 \| EV** | EV manufactures may consider participation in Automotive-Information Sharing and Analysis (Auto-ISAC) for industry-specific intelligence. | **ISO/SAE 21434** RQ-08-01, WP-08-01 |
| **RA-2 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1 |
| **RA-2 \| Cloud/Third Party** | Applicable, but no additional Cloud/Third Party-specific considerations. | **[NIST-SP800-53r5]** PM-15, PM-16, RA-10, SI-5<br>**[NIST-SP800-150]** |
| **RA-2 \| Utility/Building Management System** | Utility/Building Management Systems may consider participation in Electricity Information Sharing and Analysis Center (E-ISAC) for industry-specific intelligence. Organizations within the Energy sector may have limited access to intelligence gained by national means through appropriate channels. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1 |
| **RA-3:** Threats, both internal and external, are identified and documented. | **Ecosystem:** Identification can occur from Cyber Threat Intelligence (CTI) sources, cybersecurity assessment/testing activities, or from other sources of information. Organizations can incorporate threat modeling processes to identify and understand existing and future threats specific to their domain. Consider threats such as insider threats, physical threats, cybersecurity threats, etc. Special considerations should consider being made for threats that impact safety, safety-critical systems/components, and financial/transactional systems/components. Threats to critical partners or suppliers may also be considered. Threats may be considered for the organization while in hardware/software design and manufacturing as well as during normal operation and maintenance. Organizations may also consider the threats that can be introduced in legacy equipment or systems. | **[NIST-IR8179]**<br>**[NIST-SP800-37r2]**<br>**[NIST-SP800-53r5]** PM-12, PM-16, RA-3, RA-10, SI-5<br>**[NIST-SP800-154]**<br>**[NIST-SP800-160V1]** 2.3<br>**NERC CIP** 007-6-R4 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **RA-3 \| EV** | Applicable, but no additional EV-specific considerations. | **ISO/SAE 21434** RQ-15-04, RQ-15-06, WP-15-03 |
| **RA-3 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** PM-12, PM-16, RA-3, RA-10, SI-5 |
| **RA-3 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** PM-12, PM-16, RA-3, RA-10, SI-5 |
| **RA-3 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** PM-12, PM-16, RA-3, RA-10, SI-5 |
| **RA-4:** Potential business impacts and likelihoods are identified. | **Ecosystem:** The potential for local attacks/breaches to spread to other domains is a consideration for discussion internal and external to an organization, regarding impacted ecosystem members. This may include risks to interfacing with a compromised external organization within the domain. | **[NIST-SP800-53r5]** CP-2, PM-9, PM-11, RA-2, RA-3, RA-9<br>**NERC CIP** 002-5.1a-R1 |
| **RA-4 \| EV** | Applicable, but no additional EV-specific considerations. | **ISO/SAE 21434** Clause 15 |
| **RA-4 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 2.1 |
| **RA-4 \| Cloud/Third-Party** | Possible impacts on charge station availability and PII should consider being identified. | **[NIST-SP800-53r5]** CP-2, PM-9, PM-11, RA-2, RA-3, RA-9 |
| **RA-4 \| Utility/Building Management System** | Potential impacts to energy availability and PII should consider being identified. | **ISA/IEC 62443-2-1:D4E1** ORG 2.1 |
| **RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. | **Ecosystem:** Historically, the determination and management of IT and OT risk have been treated as separate disciplines. Given the level of IT/ OT interaction and interdependencies within this ecosystem, consider a holistic risk determination that includes IT and OT. | **[NIST-SP800-30r1]**<br>**[NIST-SP800-53r5]** CA-2, CA-7, PM-16, PM-28, RA-2, RA-3<br>**[NIST-SP800-160V1]** 2.3, 2.4<br>**NERC CIP** 007-6-R2 |
| **RA-5 \| EV** | Applicable, but no additional EV-specific considerations. | **ISO/SAE 21434** WP-15-04, WP-15-05, WP-15-06, WP-15-07 |
| **RA-5 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 2.1 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **RA-5 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CA-2, CA-7, PM-16, PM-28, RA-2, RA-3 |
| **RA-5 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 2.1 |
| **RA-6:** Risk responses are identified and prioritized. | **Ecosystem:** This allows for better alignment of those responses based on risk to the organization. Risk responses may derive from discussing details of the response, such as the associated response time, any limitations, and any potential impacts to operations. Given the interdependences of the domains within the ecosystem, organizations may consider coordinating the responses with external organizations. Consider prioritizing responses to ensure safety and personal information security. | **[NIST-SP800-53r5]** CA-5, PM-4, PM-9, PM-28, RA-7 **NERC CIP** 007-6-R2 |
| **RA-6 \| EV** | Applicable, but no additional EV-specific considerations. | **ISO/SAE 21434** WP-13-01 |
| **RA-6 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 2.1 |
| **RA-6 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CA-5, PM-4, PM-9, PM-28, RA-7 |
| **RA-6 \| Utility/Building Management System** | Applicable, but no additional Utilities/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 2.1 |

### 5.1.5. Risk Management Category

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

In the context of the EV/XFC ecosystem, the risk tolerance for a particular domain may be influenced by the impact of an incident on partner organizations or the other domains.

**Table 6.** Identify: Risk Management Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **RM-1:**<br>Risk management processes are established, managed, and agreed to by organizational stakeholders. | **Ecosystem:** Risk management processes may include, but are not limited to, supply chain, cybersecurity, assets, business environment, and regulatory governance. The established framework should potentially include risk identification, assessment, monitoring, and mitigation strategies to protect ecosystem assets. This may include data, hardware, software, networks, and facilities. Members should consider ensuring risk management strategies are aligned with the organization's risk tolerance policies. | **[NIST-SP800-53r5]**<br>PM-9, PM-28<br>**ISA/IEC 62443-2-1:D4E1**<br>ORG 2.1 |
| **RM-1 \| EV** | Risk management processes are likely to include considerations of obligations to and from EV/XFC partners and suppliers | **ISO/SAE 21434**<br>WP-05-01 |
| **RM-1 \| XFC/EVSE** | Risk management processes should potentially include accounting for EV/XFC partners, suppliers, and organizations like North American Electric Reliability Corporation (NERC) and Federal Energy Regulatory Commission (FERC). | **ISA/IEC 62443-2-1:D4E1**<br>ORG 2.1 |
| **RM-1 \| Cloud/Third-Party** | Risk management processes should potentially include accounting for EV/XFC partners, web vendors, suppliers, and customers. | **[NIST-SP800-53r5]**<br>PM-9, PM-28 |
| **RM-1 \| Utility/Building Management System** | Risk management processes should potentially include accounting for EV/XFC partners, customers and organizations like NERC and FERC. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 2.1 |
| **RM-2:**<br>Organizational risk tolerance is determined and clearly expressed. | **Ecosystem:** Ecosystem elements may determine the risk tolerance associated with activities within the organization, such as product development, supply chain management, cybersecurity, asset management, business environment, and regulatory governance. Risk tolerance may be communicated through means such as policies, procedures, guidelines, and training programs. Risk tolerance should consider including special considerations for any safety, safety-critical, financial, or regulatory aspects. Organizations may communicate their risk tolerance to the other domains within the ecosystem. | **[NIST-SP800-53r5]**<br>PM-9 |
| **RM-2 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]**<br>PM-9 |
| **RM-2 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]**<br>PM-9 |
| **RM-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 2.1 |
| **RM-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations | **ISA/IEC 62443-2-1:D4E1**<br>ORG 2.1 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **RM-3:**<br>The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis. | **Ecosystem:** Elements of the ecosystem include energy, transportation, communication, or shipping. Risk analysis for the elements of the critical infrastructure is influenced by their (potentially) broad impact. Some sectors within the critical infrastructure have unique attack surfaces and there may be determined adversaries with a nation state level of capabilities. The actual role in the critical infrastructure is organization specific. | **[NIST-SP800-53r5]** PM-8, PM-9, PM-11, RA-9 |
| **RM-3 \| EV** | Applicable, but no additional EV specific considerations | **[NIST-SP800-53r5]** PM-8, PM-9, PM-11, RA-9 |
| **RM-3 \| XFC/EVSE** | Applicable, but no additional EVSE specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 2.1 |
| **RM-3 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party specific considerations | **[NIST-SP800-53r5]** PM-8, PM-9, PM-11, RA-9 |
| **RM-3 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System specific considerations | **ISA/IEC 62443-2-1:D4E1** ORG 2.1 |

### 5.1.6. Supply Chain Risk Management Category

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 processes to identify, assess, and manage supply chain risks.

Supply chain risk management (SCRM) is typically an intra-organization function; but, in the context of the EV/XFC ecosystem, organizations will need to understand the partner's SCRM so that the impacts of any risk inherited by partners impacts are understood and kept within the level of the organization's tolerance.

**Table 7.** Identify: Supply Chain Risk Management Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **SC-1:**<br>Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders. | **Ecosystem:** Roles within the supply chain may include partners, suppliers, customers, and service providers. These processes include activities such as cybersecurity analysis, passive/active assessments, or cyber threat intelligence collection, and ingestion. Organizations should consider identifying critical components, systems, and processes related to cyber supply chain risk management including a document methodology for doing so. Roles and responsibilities may be established and consistently implemented across the organization. Consider assessing the supply chain for potential cybersecurity risks, probability and impact of cyber events, and processes in place to manage risk. Management of the supply chain may include monitoring and implemented security controls across the ecosystem. | **[NIST-SP800-53r5]**<br>PM-30, SA-9, SR-1, SR-2, SR-3, SR-5<br>**[NIST-SP800-161]** |
| **SC-1 \| EV** | Critical components may include the head unit system, on-board-diagnostic interface, telematic control units, central gateway modules, battery management systems, electronic control units, and communication controllers. Subcomponents (e.g., microcontrollers, sensors, electrical wiring, connectors.) critical to the function of onboard controllers and management systems should consider being included in the evaluation of cyber supply chain risk. | **ISO/SAE 21434**<br>RQ-07-04, WP-07-01 |
| **SC-1 \| XFC/EVSE** | Critical components may include the charging station controller, power module controls, protection circuits, power conversion system, supply equipment communication controller, thermal management systems, human-machine interface, and EVSE meter equipment. Subcomponents (e.g., microcontrollers, sensors, electrical wiring, connectors.) critical to the function of onboard controllers and management systems should consider being included in the evaluation of cyber supply chain risk. | **[NIST-SP800-53r5]**<br>SR-1, SR-2, SR-3, SR-5<br>**[NIST-SP800-161]** |
| **SC-1 \| Cloud/Third-Party** | Critical components may include physical data centers, network equipment, servers, storage devices, operating systems, and encryption mechanisms. Subcomponents (e.g., microcontrollers, sensors, electrical wiring, connectors.) critical to the function of onboard controllers and management systems should consider being included in the evaluation of cyber supply chain risk. | **[NIST-SP800-53r5]**<br>SR-1, SR-2, SR-3, SR-5<br>**[NIST-SP800-161]** |
| **SC-1 \| Utility/Building Management System** | Critical components may include the power distribution units, remote-controlled breakers, local circuit protection, and generation/storage grid systems. Subcomponents (e.g., microcontrollers, sensors, electrical wiring, connectors.) critical to the function of onboard controllers and management systems should consider being included in the evaluation of cyber supply chain risk. | **[NIST-SP800-53r5]**<br>SR-1, SR-2, SR-3, SR-5<br>**[NIST-SP800-161]** |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **SC-2:**<br>Suppliers and third-party partners of information systems, components and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process. | **Ecosystem:** Assessments may include ecosystem partners, suppliers, customers, and service providers. Organizations may consider suppliers and partners involved in the development, manufacturing, and distribution of assets. Suppliers and partners should consider being prioritized based on risk and potential impact to the ecosystem. Consider assessing risks if suppliers and partners have proper policies, procedures, and security controls in place to mitigate the cybersecurity risks. | **[NIST-SP800-53r5]** PM-9, RA-3, SA-15, SR-2, SR-3, SR-5, SR-6<br>**[NIST-SP800-161]** 2.2, 3 |
| **SC-2 \| EV** | Applicable, but no additional EV-specific considerations. | **ISO/SAE 21434** RQ-07-04, WP-07-01 |
| **SC-2 \| XFC/EVSE** | Some of the equipment used within the XFC/ EVSE is highly specialized with a limited supply chain. Organizations can consider this specialized nature when determining and managing supply chain risk. | **[NIST-SP800-161]** 2.2, 3 |
| **SC-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-161]** 2.2, 3 |
| **SC-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-161]** 2.2, 3 |
| **SC-3:**<br>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. | **Ecosystem:** Consider contractual measures such as customer- and multi-level service-level agreements (SLAs), bilateral contracts, cost-plus contracts, etc. These measures must be negotiated and agreed upon in advance and include performance language. Ecosystem members may consider establishing contractual agreements with suppliers and third-party partners that enforce cybersecurity requirements to protect confidentiality, integrity, and availability of information. Contractual agreements may include security control, monitoring, and incident response requirements. | **[NIST-SP800-53r5]** SA-4, SA-9, SR-2, SR-3, SR-5 |
| **SC-3 \| EV** | Applicable, but no additional EV-specific considerations. | **[ISO/SAE 21434]** RQ-07-04, WP-07-01 |
| **SC-3 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** SA-4, SA-9 |
| **SC-3 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** SA-4, SA-9 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **SC-3 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** SA-4, SA-9 |
| **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. | **Ecosystem:** Consider methods such as audits, vulnerability scans, penetration tests, and other evaluation forms to routinely assess and confirm suppliers and third-party/EV/XFC partners are meeting contractual cybersecurity obligations. Promptly address security concerns or compliance issues with suppliers and third-party partners. Consider establishing formal procedures and contingency plans to manage and enforce contractual obligations within the ecosystem. | **[NIST-SP800-53r5]** AU-6, CA-2, CA-7, PS-7, SA-9, SA-11 |
| **SC-4 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** AU-6 |
| **SC-4 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-3-3:2013** SR 6.1 |
| **SC-4 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** AU-6 |
| **SC-4 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-3-3:2013** SR 6.1 |
| **SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers. | **Ecosystem:** Ecosystem members should consider regularly evaluating compliance of supplier and third-party providers/partners response and recovery activities to ensure incident response plans are aligned with ecosystem cyber supply chain risk management strategy. | **[NIST-SP800-53r5]** CP-2, CP-4, IR-3, IR-4, IR-8, IR-9 |
| **SC-5 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** IR-3, IR-4, IR-8, IR-9 |
| **SC-5 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 |
| **SC-5 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** IR-3, IR-4, IR-8, IR-9 |
| **SC-5 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 |

## 5.2. Protect Function Considerations Across the EV/XFC Domains

The Protect function defines activities that support the ability to limit or contain the impact of a potential cybersecurity event. Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

The Protect function consists of six Categories:

- Identity Management, Authentication, and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

### 5.2.1. Identity Management, Authentication and Access Control Category

Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. Relative to other cyber-ecosystems, the EV/XFC will need to provide greater access to external organizations to function. Consider more granular levels of identity management, authentication, and access controls to strike a balance between limiting exposure and allowing sufficient access.

**Table 8.** Protect: Identity Management, Authentication and Access Control

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AC-1:**<br>Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes. | **Ecosystem:** Consider implementing formal procedures and guidelines to issue, manage, and verify identities and credentials. Credential management may be performed by an independent entity. This may include the management of authentication mechanisms (e.g., single-factor, multi-factor) and unique identifiers, such as usernames, passwords, certificates, biometrics, smart cards, and hardware tokens. Implement mechanisms to track, log, approve, and audit access attempts and activities of devices within the ecosystem. Identities/credentials stored within the ecosystem may include manufacturer identities, employee identities, supplier identities, provider identities, device identities, test and validation certificates, software certificates, and system administration credentials. Consider that credentials should be promptly accredited and decommissioned when issued and revoked. | **[NIST-SP800-53r5]**<br>IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12<br>**NERC CIP**<br>004-6-R4, 007-6-R5 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AC-1 \| EV** | EV manufacturers can provide means to ensure the system is able to allow customers to authenticate interactions with and within their systems. Domain-specific identities/credentials stored within the EV may include credentials for authentication, software/firmware certificates, and diagnostics and maintenance. | **[NIST-SP800-53r5]** IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12 |
| **AC-1 \| XFC/EVSE** | EVSE manufacturers can provide means or ensure the system is able to allow customers to authenticate interactions with and within their systems. Domain-specific identities/credentials stored within the EVSE may include charging station identities, metering credentials, billing credentials, software/firmware certificates, and system administration credentials. | **ISA/IEC 62443-2-1:D4E1** USER 1.01, USER 1.02, USER 1.04, USER 1.06, USER 1.08, USER 1.09, USER 1.11<br>**ISA/IEC 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 |
| **AC-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12 |
| **AC-1 \| Utility/Building Management System** | Utility/building management devices/systems-specific identities/credentials may include control system credentials, energy management system credentials, and building access credentials. | **ISA/IEC 62443-2-1:D4E1** USER 1.01, USER 1.02, USER 1.04, USER 1.06, USER 1.08, USER 1.09, USER 1.11<br>**ISA/IEC 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 |
| **AC-2:** Physical access to assets is managed and protected. | **Ecosystem:** Physical connections to communication ports must be protected, and if deemed unnecessary, removed, or disabled. | **[NIST-IR8320]**<br>**[NIST-SP800-53r5]** PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9<br>**NERC CIP** 007-6-R5 |
| **AC-2 \| EV** | Physical access may include access to critical systems, such as battery management and charging management, diagnostic, or non-critical systems, such as the infotainment system. | **[NIST-SP800-53r5]** PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AC-2 \| XFC/EVSE** | Physical access may include (but is not limited to) battery energy storage systems (BESS), networking/communication equipment, and account/financial transaction equipment. EVSE-specific protections are warranted due to the unmanned nature of many EVSE installations. This may take the form of tamper-resistant tools (locks, proprietary tools, etc.), access and tamper logging switches/devices, or deactivating ports allowing unauthenticated access or modification of log/configuration data. This could also include physically securing the charge cable connector to prevent tampering or monitoring for tamper evident events and signals. EVSE owners/operators may consider surveilling the EVSE surroundings for unusual behavior. | **[NIST Handbook 44]** 1.10 G-S.8, 1.10 G-S.8.2, 3.40 S.3.1, 3.40 S.3.3<br>**ISA/IEC 62443-2-1:D4E1** ORG 3.1, AVAIL 1.1, AVAIL 1.2<br>**OIML D31:2019** 6.1.3.2.1, 6.1.3.2.4,<br>**OIML G22:2022** 4.4.3.2 |
| **AC-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9 |
| **AC-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 3.1, AVAIL 1.1, AVAIL 1.2 |
| **AC-3:**<br>Remote access is managed. | **Ecosystem:** Ecosystem members can consider establishing formal access control policies and guidelines that clearly define remote access privileges. Management may take the form of authentication, training, verification prior to access being granted, and automatic timeout threshold implementation. Managing remote access may include authentication and management and audit mechanisms to track, log, and approve access attempts and activities of devices within the ecosystem. | **[NIST-SP800-53r5]** AC-1, AC-2, AC-17, AC-19, AC-20, SC-7 SC-15<br>**NERC CIP** 004-6-R4, 004-6-R5 |
| **AC-3 \| EV** | This may include (but is not limited to) authorized over the air (OTA) updates, vehicle status/usage information, and customer remote access features. | **[NIST-SP800-53r5]** AC-2, AC-17, AC-19, AC-20<br>**ISO 24089:2023** |
| **AC-3 \| XFC/EVSE** | This may include (but is not limited to) authorized over the air (OTA) updates, EV chargers, BESS, networking/communication equipment, utility/building management systems, and account/financial transaction equipment. EVSE owners/operators may consider supporting different wireless protocols (such as Wi-Fi, Bluetooth, Near Field Communication (NFC), etc.) that might be necessary to provide remote access to the equipment. | **ISA/IEC 62443-2-1:D4E1** NET 1.01, NET 1.06, NET 3.3. NET 3.4<br>**ISA/IEC 62443-3-3:2013** SR 1.13, SR 2.6<br>**OIML D31:2019** 6.2.6.5, 6.2.6.5.3<br>**OIML G22:2022** 4.4, 4.4.3, 4.4.4, 4.4.8 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AC-3 \| Cloud/Third-Party** | This may include remote access from EVs, EVSE, web vendor, and utility/building management systems. | **[NIST-SP800-53r5]** AC-2, AC-17, AC-19, AC-20 |
| **AC-3 \| Utility/Building Management System** | This may include remote access from EVSE and Cloud/Third-Party systems, as well as other utility/building management systems and assets. | **ISA/IEC 62443-2-1:D4E1** NET 1.01, NET 1.06, NET 3.3. NET 3.4<br>**ISA/IEC 62443-3-3:2013** SR 1.13, SR 2.6 |
| **AC-4:**<br>Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | **Ecosystem:** Least privilege and separation of duties help contain the cyber security attacks encountered by the asset, component or system protected by the permissions. lists of required authorizations should consider being periodically reviewed to remove outdated permissions and may include Role Based Access Control (RBAC) or other access control paradigms. | **[NIST-SP800-53r5]** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24<br>**[NIST-SP800-160V1]** Appendix F.1.14<br>**NERC CIP** 004-6-R4 004-6-R5 007-6-R5 |
| **AC-4 \| EV** | EV reviews may include (but are not limited to) internal vehicle systems, remote access, and EVSE interfacing. EV manufacturers may consider defining and limiting what settings EV owners can modify during normal operation and identifying authorized drivers or users. | **[NIST-SP800-53r5]** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 |
| **AC-4 \| XFC/EVSE** | XFC/EVSE reviews may include (but are not limited to) EV charger, BESS, networking/communication equipment, utility/building management systems, and account/financial transaction equipment. EVSE manufacturers/owners/operators may consider how to implement the principles of least privilege and separation of duties for components at an EVSE site as well. | **PCI-DSS v4**<br>**ISA/IEC 62443-2-1:D4E1** USER 1.04, USER 1.05, USER 1.07, USER 2.1, USER 2.2<br>**ISA/IEC 62443-3-3:2013** SR 2.1<br>**OIML D31:2019** 6.2.5.2, 6.2.6.6 |
| **AC-4 \| Cloud/Third-Party** | Cloud/Third-Party reviews may include access permissions and authorizations from EVs, EVSE systems, web vendors, and utility/building management systems. | **PCI-DSS v4** |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AC-4 \| Utility/Building Management System** | The utility/building management system reviews may include access permissions and authorizations from EVSE and cloud/third-party systems, as well as other utility/building management systems and assets like SCADA, system controls, sensors, HMIs, sensors, and servers. | **ISA/IEC 62443-2-1:D4E1** USER 1.04, USER 1.05, USER 1.07, USER 2.1, USER 2.2<br>**ISA/IEC 62443-3-3:2013** SR 2.1 |
| **AC-5:**<br>Network integrity is protected (e.g., network segregation, network segmentation). | **Ecosystem:** The EV/XFC ecosystem members should consider including integrity protection measures for both IT and OT networks. Network integrity enables secure and available communications as well helping protect any network connected data and systems. Employing consistent network integrity assessments, security training, and incident response plans minimizes the frequency and impact of network security incidents. | **[NIST-SP800-53r5]** AC-4, AC-10, SC-7, SC-10, SC-20<br>**NERC CIP** 007-6-R1 |
| **AC-5 \| EV** | Networks may include (but are not limited to) internal Controller Area Network (CAN) links between systems, such as battery management, infotainment and charge controller systems, and external communications with EVSE and cloud/third-party systems. | **[NIST-SP800-53r5]** AC-4, SC-7, SC-10, SC-20 |
| **AC-5 \| XFC/EVSE** | EVSE owners/operators should consider protecting network integrity, including segmentation and segregation of networked devices at an EVSE installation such as EV charger, BESS, networking/communication equipment, utility/building management systems, and account/financial transaction equipment. | **PCI-DSS v4**<br>**ISA/IEC 62443-2-1:D4E1** NET 1.01, NET 1.06, USER 1.16<br>**ISA/IEC 62443-3-3:2013** SR 3.1, SR 3.8 |
| **AC-5 \| Cloud/Third-Party** | Cloud/Third-Party considerations may include networked links to/from EVs, EVSE systems, web vendors, and utility/building management systems. | **[NIST-SP800-53r5]** AC-4, SC-7, SC-10, SC-20<br>**PCI-DSS v4** |
| **AC-5 \| Utility/Building Management System** | The utility/building management system considerations may include network links to/from EVSE and Cloud/Third-Party systems, as well as other utility/building management systems and assets. | **ISA/IEC 62443-2-1:D4E1** NET 1.01, NET 1.06, USER 1.16<br>**ISA/IEC 62443-3-3:2013** SR 3.1, SR 3.8 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AC-6:**<br>Identities are proofed, bound to credentials, and asserted in interactions. | **Ecosystem:** Ecosystem members should consider asserting more tightly proofed and bound credentials for interactions with greater associated risk and discuss acceptable levels of credential complexity, credential renewal and reissuance frequency, as well as the use of multifactor authentication. This activity may include utilization of security features provided by industry standards, protocols, and tools, as well as relevant standards, protocols, and tools from other industries that utilize similar system architectures and equipment.<br>Increased or additional credentials may be considered for interactions of increased risk, such as when modifying system settings or protocols, performing routine maintenance and updates, and when utilizing apps containing PII and payment account access. | **[NIST-IR8014]**<br>**[NIST-SP800-53r5]** AC-16, IA-1, IA-2, IA-4, IA-5, IA-8, IA-12, PE-2, PS-3<br>**[NIST-SP800-207]**<br>**ATIS-I-0000070** 2-7<br>**NERC CIP** 004-6-R3 |
| **AC-6 \| EV** | EV-specific considerations include user accounts accessible from the EV and driver identification. | **[NIST-SP800-53r5]** AC-16, IA-1, IA-2, IA-4, IA-5, IA-8, IA-12<br>**PCI-DSS v4** |
| **AC-6 \| XFC/EVSE** | Applicable, no additional EVSE-specific considerations. | **PCI-DSS v4**<br>**ISA/IEC 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 |
| **AC-6 \| Cloud/Third-Party** | Applicable, no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** AC-16, IA-1, IA-2, IA-4, IA-5, IA-8, IA-12<br>**PCI-DSS v4** |
| **AC-6 \| Utility/Building Management System** | Applicable, no additional Utility/Building Management System-specific considerations. | **PCI-DSS v4**<br>**ISA/IEC 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AC-7:**<br>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). | **Ecosystem:** EV/XFC ecosystem may consider the implementation of multi-factor authentication (MFA) where possible. Assets may include data, hardware, software, networks, and facilities. | **[NIST-SP800-53r5]**<br>AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10<br>**[NIST-SP800-207]**<br>**IETF-RFC4082**<br>2-5<br>**NERC CIP**<br>007-6-R5 |
| **AC-7 \| EV** | Transactions and interactions may include remote vehicle access by both user and manufacturer as well as interfaces with EVSE networks. | **[NIST-SP800-53r5]**<br>AC-14, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10 |
| **AC-7 \| XFC/EVSE** | Transactions and interactions may include remote access to devices, interfaces with physical devices such as EVs, cloud/third-party systems, and utility/building management systems. | **ISA/IEC 62443-3-3:2013**<br>SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 |
| **AC-7 \| Cloud/Third-Party** | Transactions and interactions may include network links to/from EVs, EVSE systems, web vendors, and utility/building management systems. | **[NIST-SP800-53r5]**<br>AC-14, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10 |
| **AC-7 \| Utility/Building Management System** | Transactions and interactions may include network links to/from EVSE and cloud/third-party systems, as well as other utility/building management systems and assets. | **ISA/IEC 62443-3-3:2013**<br>SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 |

### 5.2.2. Awareness and Training Category

The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

The Awareness and Training category is not unique to the EV/XFC ecosystem, and like other cyber-ecosystems, focuses on privileged users who operate, monitor, and maintain systems and interfaces.

**Table 9.** Protect: Awareness and Training Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AT-1:**<br>All users are informed and trained. | **Ecosystem:** User training may be recurring and include information about how to interact correctly with the system as well as education about common cybersecurity methods and warning signs before, during, and after an attack or incident. | **[NIST-SP800-53r5]**<br>AT-2, PM-13, PM-14 |
| **AT-1 \| EV** | This may include staff at multiple levels, from administrative staff to design and manufacturing staff. EV manufacturers may consider including EV owner cybersecurity information and recommend best practices in the vehicle manual. Information provided in the manual may include the recommended use of multifactor authentication, PIN, and recommended settings. | **[NIST-SP800-53r5]**<br>AT-2, PM-14 |
| **AT-1 \| XFC/EVSE** | This may include staff at multiple levels, from administrative staff to design, manufacturing, maintenance, and operations staff. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 1.4 |
| **AT-1 \| Cloud/Third-Party** | This may include staff at multiple levels, from administrative and operations staff to EV/XFC partners and vendors. App developers can consider encouraging positive cyber practices among users of the app, like multifactor identification and strong passwords, as well as incorporating good cyber coding practices and assessments. | **[NIST-SP800-53r5]**<br>AT-2, PM-14 |
| **AT-1 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 1.4 |
| **AT-2:**<br>Privileged users understand their roles and responsibilities. | **Ecosystem:** Privileged users include (but are not limited to) admin/root users/accounts, system administrators, and developers. Ecosystem members can consider clearly defining and routinely updating roles and responsibilities, and then implement training programs to help privileged users understand and abide by their roles and responsibilities. Consider continually testing awareness levels, and reevaluate and retrain as needed to help maintain system security. Privileged user-specific training should consider emphasizing elevated attacker desire to compromise privileged accounts and the consequences of breaches. | **[NIST-SP800-53r5]**<br>AT-3, PM-13<br>**[NIST-SP800-161]**<br>Appendix E |
| **AT-2 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]**<br>AT-3, PM-13 |
| **AT-2 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]**<br>AT-3, PM-13 |
| **AT-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]**<br>AT-3, PM-13 |
| **AT-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]**<br>AT-3, PM-13 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AT-3:**<br>Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities. | **Ecosystem:** Members can consider clearly defining and routinely updating roles and responsibilities and then implementing training programs to help third-party-relevant parties understand and abide by their roles and responsibilities. Awareness levels may be continually tested, reevaluated, and retrained to maintain system security. Understanding roles and responsibilities may include identifying ways in which cybersecurity may be compromised and common preventative measures. | **[NIST-SP800-53r5]**<br>AT-3, PS-7, SA-9 |
| **AT-3 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]**<br>AT-3, PS-7 |
| **AT-3 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 1.3, ORG 1.4 |
| **AT-3 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]**<br>AT-3, PS-7 |
| **AT-3 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 1.3, ORG 1.4 |
| **AT-4:**<br>Senior executives understand their roles and responsibilities. | **Ecosystem:** The level of resources applied to cybersecurity is correlated with the level of buy-in from senior executives. Senior executives that understand their roles and responsibilities should consider providing leadership throughout the organization. Ecosystem members may consider clearly defining and routinely updating roles and responsibilities of senior executives, and then developing routine training programs to help understand and abide by those roles and responsibilities. Awareness levels may be continually tested, reevaluated, and retrained to maintain system security. Senior executive-specific training should consider emphasizing elevated attacker desire to compromise executive accounts and the consequences of breaches. | **[NIST-SP800-53r5]**<br>AT-3, PM-2, PM-13, PM-29 |
| **AT-4 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]**<br>PM-2, PM-13, PM-29 |
| **AT-4 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 1.3, ORG 1.4 |
| **AT-4 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]**<br>PM-2, PM-13, PM-29 |
| **AT-4 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 1.3, ORG 1.4 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AT-5:**<br>Physical and cybersecurity personnel understand their roles and responsibilities. | **Ecosystem:** Understanding roles and responsibilities includes clearly defining and routinely updating roles and responsibilities, and then implementing training programs to help physical and cybersecurity personnel understand and abide by their roles and responsibilities. Awareness levels may be continually tested, reevaluated, and retrained to maintain system security. Physical/cybersecurity personnel-specific training should consider emphasizing the best practices to adopt and how to identify and report cybersecurity risks.<br>This should consider including personnel involved in design, manufacturing, maintenance, and administration/operation roles. | **[NIST-SP800-53r5]** AT-3, CP-3, IR-2, PM-13 |
| **AT-5 \| EV** | Applicable, but no additional EV specific considerations. | **[NIST-SP800-53r5]** AT-3, IR-2, PM-13 |
| **AT-5 \| XFC/EVSE** | Applicable, but no additional EVSE specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.3, ORG 1.4 |
| **AT-5 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party specific considerations. | **[NIST-SP800-53r5]** AT-3, IR-2, PM-13 |
| **AT-5 \| Utility/Building Management System** | Utility/Building Management Systems may consider existing physical security requirements and/or regulations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.3, ORG 1.4 |

### 5.2.3. Data Security Category

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

The domains within the EV/XFC ecosystem may be subject to laws and regulations with specific data security requirements, and the domains may have an obligation to provide data security for partner organizations. The tools, techniques, processes, and procedures will require a level of inter-organization cooperation that other organizations do not typically encounter.

**Table 10.** Protect: Data Security Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **DS-1:**<br>Data-at-rest is protected. | **Ecosystem:** Ecosystem members can consider having increased protections for sensitive, PII, or transactional data. Data-at-rest (DAR) protections may be provided through measures such as:<br>• Securing and tamper-resistant data storage.<br>• Encrypting all data.<br>• Restricting access to all data around a strict need and for a specified time period.<br>• Monitoring and conducting regular security audits of protection mechanisms.<br>• Regularly updating the software and firmware of all onboard electronic management and control systems.<br>Which DAR protection measure(s) to implement is determined on a case-by-case basis in a manner that is consistent with the organization's risk management. | **[NIST-SP800-37r2]**<br>**[NIST-SP800-53r5]** MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28<br>**[NIST-SP800-175Br1]**<br>**[NIST-SP800-209]**<br>**NERC CIP** 004-6-R4, 004-6-R5, 011-2-R1 |
| **DS-1 \| EV** | DAR includes any information that is stored onboard electronic management and control systems within the EV. This data may include any information cached or stored on the vehicle, information on vehicle performance, battery performance, charging history, location history, associated accounts, and charging profiles from EV/XFC partners, and suppliers/vendors. | **[NIST-SP800-53r5]** MP-3, MP-4, SC-28<br>**[NIST-SP800-175Br1]**<br>**[NIST-SP800-209]** |
| **DS-1 \| XFC/EVSE** | DAR includes any information that is in equipment, firmware, or software within the EVSE. This data may include information from EV owners, EV/XFC partners, and suppliers/vendors as well as reservations and credentials used to access accounts and databases. | **[NIST Handbook 44]** 3.40 S.3.4(a)<br>**ISA/IEC 62443-2-1:D4E1** CM 1.3, DATA 1.2<br>**ISA/IEC 62443-3-3:2013** SR 3.4, SR 4.1<br>**OIML D31:2019** 6.2.3.4 |
| **DS-1 \| Cloud/Third-Party** | DAR includes any information that is stored in databases owned and managed by third parties. This data may include information from EV owners, EV/XFC partners, customers, and cloud and payment processing vendors. Consider protecting information database access from unauthorized access and security breaches. | **[NIST-SP800-53r5]** MP-3, MP-4, SC-28<br>**[NIST-SP800-175Br1]**<br>**[NIST-SP800-209]** |
| **DS-1 \| Utility/Building Management System** | DAR includes any information that is stored on utility servers. This data may include load forecasting and account information from EV/XFC partners, utility/building management partners, and suppliers/vendors. | **ISA/IEC 62443-2-1:D4E1** CM 1.3, DATA 1.2<br>**ISA/IEC 62443-3-3:2013** SR 3.4, SR 4.1 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **DS-2:**<br>Data-in-transit (DIT) is protected. | **Ecosystem:** Ecosystem members may consider having increased protections for sensitive, PII, or transactional data. Data-in-transit (DIT) protections may be provided through measures such as:<br>• Securing and tamper-resistant communication systems and protocols for all transmitted data.<br>• Encrypting and authenticating data transmitted over wired or wireless communication channels.<br>• Monitoring and conducting regular security audits of protection mechanisms.<br>• Error detecting/correcting protocols.<br>Which DIT protection measure(s) to implement is determined on a case-by-case basis in a manner that is consistent with the organization's risk management. | **[NIST-SP800-53r5]**<br>SC-8, SC-11, SC-12<br>**NERC CIP**<br>004-6-R4, 004-6-R5 |
| **DS-2 \| EV** | DIT may include any information that is transmitted over wired or wireless communication channels onboard electronic management and control systems within the EV or data leaving the EV. This data may include information on vehicle performance, battery performance, charging history, location and financial history, and vehicle owners from EV/XFC partners, and suppliers/vendors. Consider additional DIT protections for over-the-air (OTA) updates. | **[NIST-SP800-53r5]**<br>SC-8, SC-11, SC-12<br>**ISO 24089:2023**<br>5.3.4.1, 7.3.1.3, 7.3.4.7, and 9.3.2.7 |
| **DS-2 \| XFC/EVSE** | EVSE owners/operators should consider encrypting all traffic leaving the EVSE. | **PCI-DSS v4**<br>**ISA/IEC 62443-2-1:D4E1**<br>NET 1.01, NET 1.06, NET 1.08, DATA 1.2, DATA 1.6, USER 1.16<br>**ISA/IEC 62443-3-3:2013**<br>SR 3.1, SR 3.8, SR 4.1, SR 4.2<br>**OIML D31:2019**<br>6.2.5.2<br>**OIML D22:2022**<br>4.4.9 |
| **DS-2 \| Cloud/Third-Party** | DIT may include information from EV owners, EV/XFC partners, customers, and cloud and payment processing vendors. Cloud/third-party owners/operators might consider encrypting all traffic. | **[NIST-SP800-53r5]**<br>SC-8, SC-11, SC-12<br>**PCI-DSS v4** |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **DS-2 \| Utility/Building Management System** | DIT may include information from EV/XFC partners, utility/building management partners, and suppliers/vendors. Utility/building management owners/operators may consider encrypting all operational data. | **ISA/IEC 62443-2-1:D4E1** NET 1.01, NET 1.06, NET 1.08, DATA 1.2, DATA 1.6, USER 1.16<br>**ISA/IEC 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 |
| **DS-3:**<br>Assets are formally managed throughout removal, transfer, and disposition. | **Ecosystem:** Manage assets, which may include hardware, software, information databases, and developmental/operational tools or systems and the data itself. In addition to the day-to-day management activities, formal asset management includes creating, using, and updating asset management activities or strategies. | **[NIST-SP800-53r5]** CM-8, MP-6, PE-16, PE-20<br>**NERC CIP** 011-2-R2 |
| **DS-3 \| EV** | Managed data may include information on vehicle performance, battery performance, charging history, location history, and vehicle owners from EV/XFC partners, and suppliers/vendors. Transfer of EV assets should consider including encryption and authentication protocols and should consider only being managed by authorized parties. Consider going through a formal provision process when updating firmware and verifying that updates can only be made by a certified party. Consider including guidelines for data retention, backup, and secure disposal in any procedures. | **[NIST-SP800-53r5]** CM-8, MP-6, PE-16, PE-20<br>**ISO 24089:2023** 5.3.4.1, 7.3.1.3, 7.3.4.7, 9.3.2.7 |
| **DS-3 \| XFC/EVSE** | Associated data may include information from EV owners, EV/XFC partners, and suppliers/vendors. | **ISA/IEC 62443-2-1:D4E1** COMP 1.1, USER 1.04, USER 1.05<br>**ISA/IEC 62443-3-3:2013** SR 4.2 |
| **DS-3 \| Cloud/Third-Party** | Data may include information from EV owners, EV/XFC partners, customers, and cloud and payment processing vendors. EVSE owners/operators should consider implementing or integrating asset management systems for all EVSE assets in the network. | **[NIST-SP800-53r5]** CM-8, MP-6, PE-16, PE-20 |
| **DS-3 \| Utility/Building Management System** | Data may include information from EV/XFC partners, utility/building management partners, and suppliers/vendors. | **ISA/IEC 62443-2-1:D4E1** COMP 1.1, USER 1.04, USER 1.05<br>**ISA/IEC 62443-3-3:2013** SR 4.2 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **DS-4:**<br>Adequate capacity to ensure availability is maintained. | **Ecosystem:** Measures to augment capacity may include:<br>• Formal procedures and activities to monitor system performance<br>• Redundant transmission systems<br>• Alternate transmission systems (such as radio frequency (RF), wired or optical systems)<br>Methods such as load balancing address abnormal server loads due to elevated traffic from user activity, incorrect server configurations, or cybersecurity events. | **[NIST-SP800-53r5]** AU-4, CP-2, CP-6, CP-7, PE-11, SC-5<br>**[NIST-SP800-160V1]** Appendix F.4<br>**IEC62439-3** 4, 5, Appendix P.2.3, 4.6, 4.8, 4.9, 4.12, 4.13<br>**NERC CIP** 009-6-R1 |
| **DS-4 \| EV** | This may include availability of the EV infrastructure that manages networks, processing, and storage capacities. | **[NIST-SP800-53r5]** CP-2, CP-6, CP-7<br>**[NIST-SP800-160V1]** Appendix F.4 |
| **DS-4 \| XFC/EVSE** | This may include availability of the XFC/EVSE charging network, supporting processes for charging, and information from EV owners, EV/XFC partners, and suppliers/vendors. | **[NIST Handbook 44]** 3.40 S.3.4 (c)<br>**ISA/IEC 62443-3-3:2013** SR 7.1, SR 7.2<br>**OIML G22:2022** 4.4.9.2.2<br>**OIML D31:2019** 6.2.4.4.1 |
| **DS-4 \| Cloud/Third-Party** | This may include information from EV owners, EV/XFC partners, customers, and cloud and payment processing vendors. Cloud and third-party system providers may consider implementing high-availability networks with the required redundancy of gateways, servers, etc. | **[NIST-SP800-53r5]** CP-2, CP-6, CP-7<br>**[NIST-SP800-160V1]** Appendix F.4 |
| **DS-4 \| Utility/Building Management System** | This may include information from EV/XFC partners, utility/building management partners, and suppliers/vendors. | **ISA/IEC 62443-3-3:2013** SR 7.1, SR 7.2 |
| **DS-5:**<br>Protections against data leaks are implemented. | **Ecosystem:** Ecosystem members may consider initially identifying what is classified as sensitive data, where they are stored, and where there is data transfer between systems, then apply appropriate protective measures, such as cryptography, access control, proper sanitization or disposal of information systems, destruction of data, and other confidentiality protections. | **[NIST-SP800-53r5]** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4<br>**NERC CIP** 004-6-R4, 004-6-R5, 007-6-R3, 007-6-R4, 007-6-R5, 011-2-R2 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **DS-5 \| EV** | Data leak protections may apply to information on vehicle performance, battery performance, charging information and history, location and location history, and vehicle owners from EV/XFC partners, and suppliers/vendors. Special consideration may be paid to any communication interfaces internal or external to the EV. This may take the form of a gateway protecting access to any internal vehicle data buses or encrypting information leaving the EV. EV manufacturers may consider establishing formal procedures to manage access to sensitive information. | **[NIST-SP800-53r5]** AC-4, AC-5, AC-6, PS-6, SC-7, SC-8, SC-13 |
| **DS-5 \| XFC/EVSE** | Data leak protections may apply to information from EV owners, payment information, EV/XFC partners, and suppliers/vendors. EVSE owners/operators may want to consider how meta data of the EVSE is exposed and limit access to it. | **ISA/IEC 62443-2-1:D4E1** NET 1.01, NET 1.06, NET 1.08, DATA 1.1, DATA 1.2<br>**ISA/IEC 62443-3-3:2013** SR 5.2 |
| **DS-5 \| Cloud/Third-Party** | Data leak protections may apply to information from EV owners, EV/XFC partners, customers, and cloud and payment processing vendors. Special consideration may be paid by cloud/third-party owners/operators on what information may be exposed through application program interfaces (APIs). | **[NIST-SP800-53r5]** AC-4, AC-5, AC-6, PS-6, SC-7, SC-8, SC-13 |
| **DS-5 \| Utility/Building Management System** | Data leak protections may apply to information from EV/XFC partners, utility/building management partners, and suppliers/vendors. | **ISA/IEC 62443-2-1:D4E1** NET 1.01, NET 1.06, NET 1.08, DATA 1.1, DATA 1.2<br>**ISA/IEC 62443-3-3:2013** SR 5.2 |
| **DS-6:**<br>Integrity checking mechanisms are used to verify software, firmware, and information integrity. | **Ecosystem:** Integrity checking mechanisms to verify software, firmware, and information integrity may be considered for use. This may take the form of a secure communication channel standard (e.g., open charge point protocol (OCPP), or other standards), or a more advanced cryptographic mechanisms, such as digital signatures to validate the integrity of the firmware or software. | **[NIST-SP800-53r5]** SI-7, SI-10<br>**[NIST-SP800-160V1]** 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F<br>**[NIST-SP800-161]**<br>**[NIST-SP800-193]**<br>**[NIST-SP800-218]** PO.3.3, PS.1 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **DS-6 \| EV** | This may include secure communication channels, cryptographic mechanisms, and digital signatures to validate the integrity of the firmware or software. EV systems that may utilize these methods include the onboard control units, communication networks, and charging infrastructure. | **[NIST-SP800-160V1]** 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F<br>**[NIST-SP800-193]**<br>**[NIST-SP800-218]** PO.3.3, PS.1<br>**ISO 24089:2023** 5.3.4.1, 7.3.1.3, 7.3.4.7, 9.3.2.7 |
| **DS-6 \| XFC/EVSE** | EVSE manufacturers may provide means to use integrity checking mechanisms to verify software, firmware, and information integrity, such as including alerting capabilities on compromised software/firmware updates. This may include secure software updates and verification of EV connection integrity and identity. | **[NIST Handbook 44]** 1.10 G-S.1 (c), (d)<br>**ISA/IEC 62443-2-1:D4E1** ORG 2.2, DATA 1.2, USER 1.16<br>**ISA/IEC 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8<br>**OIML D31:2019** 6.1.1, 6.2.2.1.1, 6.2.2.1.2<br>**OIML G22:2022** 4.4.2, 4.4.5.1 |
| **DS-6 \| Cloud/Third-Party** | This may include measures to verify user identities and protect against unauthorized access. Cloud and third-party systems may consider implementing allow-lists for software sources. | **[NIST-SP800-160V1]** 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F<br>**[NIST-SP800-193]**<br>**[NIST-SP800-218]** PO.3.3, PS.1 |
| **DS-6 \| Utility/Building Management System** | This may include metering data collected about energy consumed, information used to manage loads and balance power, and local breaker/switchgear control commands. | **ISA/IEC 62443-2-1:D4E1** ORG 2.2, DATA 1.2, USER 1.16<br>**ISA/IEC 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 |
| **DS-7:**<br>The development and testing environment(s) are separate from the production environment. | **Ecosystem:** Separating development and testing environments from production environments is considered a best practice. Exceptions, such as early release (e.g., beta versions), can be managed closely while trying to keep as much separation as possible between development and production. | **[NIST-SP800-53r5]** CM-2, SA-3<br>**[NIST-SP800-160V1]** 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **DS-7 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CM-2, SA-3 |
| **DS-7 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** NET 1.01 |
| **DS-7 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CM-2, SA-3 |
| **DS-7 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** NET 1.01 |
| **DS-8:** Integrity checking mechanisms are used to verify hardware integrity. | **Ecosystem:** Examples of hardware integrity checking mechanisms include trusted platform modules, acceptance testing, component and subassembly verification, tamper detection, etc. | **[NIST-IR800-8320]** **[NIST-SP800-53r5]** AC-25, SA-10, SI-7, SR-9, SR-10 **[NIST-SP1800-19]** **[NIST-SP1800-34]** **FIPS 140-3** |
| **DS-8 \| EV** | EV-specific hardware under evaluation may include the battery system, charge controller, propulsion and control systems, electrical wiring, and connectors. | **[NIST-SP800-53r5]** AC-25, SA-10, SI-7, SR-9, SR-10 **FIPS 140-3** |
| **DS-8 \| XFC/EVSE** | EVSE-specific measures may include verifying the integrity of the safety systems (connector ground, overcurrent protection, and cooling system), verification of connected EV identity, or verifying EVSE on-board hardware has not been tampered with. | **[NIST-SP800-53r5]** AC-25, SA-10, SI-7, SR-9, SR-10 **FIPS 140-3** |
| **DS-8 \| Cloud/Third-Party** | Applicable, but no additional Cloud-Third-Party specific considerations. | **[NIST-SP800-53r5]** AC-25, SA-10, SI-7, SR-9, SR-10 **FIPS 140-3** |
| **DS-8 \| Utility/Building Management System** | This may include periodic testing of breaker functionality and regular maintenance and monitoring or energy infrastructure. | **[NIST-SP800-53r5]** AC-25, SA-10, SI-7, SR-9, SR-10 **FIPS 140-3** |

### 5.2.4. Information Protection and Processes Category

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.

Due to the interdependencies within the EV/XFC ecosystem, the domains will require a greater level of inter-organization cooperation.

**Table 11.** Protect: Information Protection Processes and Procedures Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **IP-1:**<br>A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality). | **Ecosystem:** Consider configuring the components within the IT and ICS systems within the context of what is required of the component rather than what the component is capable of doing. Disabling unnecessary capabilities and limiting the functionality of devices reduces the attack surface, limits the spread of an attack in the event of a compromise, and facilitates the detection of anomalies by reducing complexity. Consider third-party systems and devices in addition to intra-organization interfaces. | **[NIST-SP800-53r5]** CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10<br>**[NIST-SP800-137]** Section D<br>**[NIST-SP800-160V1]** 3.4.9, 3.4.10, 3.4.11, Appendix F, Appendix G<br>**NERC CIP** 012-1-R1 |
| **IP-1 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CM-3, CM-5, CM-6, CM-7, CM-9<br>**[NIST-SP800-160V1]** 3.4.9, 3.4.10, 3.4.11, Appendix F, Appendix G |
| **IP-1 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** CM 1.3, CM 1.4<br>**ISA/IEC 62443-3-3:2013** SR 7.6<br>**OIML D 31** 6.1.4.1 |
| **IP-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Thirty-Party-specific considerations. | **[NIST-SP800-53r5]** CM-3, CM-5, CM-6, CM-7, CM-9<br>**[NIST-SP800-160V1]** 3.4.9, 3.4.10, 3.4.11, Appendix F, Appendix G |
| **IP-1 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** CM 1.3, CM 1.4<br>**ISA/IEC 62443-3-3:2013** SR 7.6 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **IP-2:**<br>A System Development Life Cycle to manage systems is implemented. | **Ecosystem:** Consider including security requirements, failure analyses, and preventative measures in software development lifecycle (SDLC) planning. | **[NIST-SP800-53r5]** SA-3, SA-4, SA-8, SA-10, SA-11<br>**[NIST-SP800-160V1]** 3.2.1, Appendix F.3 |
| **IP-2 \| EV** | This may include development systems and assets, original equipment manufacturer (OEM)/owner information assets and recommended/required replacement schedules. | **[NIST-SP800-53r5]** SA-3, SA-4, SA-8, SA-10, SA-11<br>**[NIST-SP800-160V1]** 3.2.1, Appendix F.3 |
| **IP-2 \| XFC/EVSE** | This may include development systems and assets, EV owner information, manufacturing systems and assets, and EV/XFC partner information systems. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1, ORG 2.3 |
| **IP-2 \| Cloud/Third-Party** | This may include development systems and assets, EV owner information, and EV/XFC partner information systems. | **[NIST-SP800-53r5]** SA-3, SA-4, SA-8, SA-10, SA-11<br>**[NIST-SP800-160V1]** 3.2.1, Appendix F.3 |
| **IP-2 \| Utility/Building Management System** | This may include development systems and assets and EV/XFC partner information systems. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1, ORG 2.3 |
| **IP-3:**<br>Configuration change control processes are in place. | **Ecosystem:** The ecosystem should consider employing configuration change control for the domain and elements that is consistent with the software development life cycle to maintain a functioning baseline. Domains must monitor all changes to validate impacts and integrity and conduct impact analyses prior to deploying a change.<br>Organizations should consider providing a mechanism so changes to the firmware and software can be returned to a proper working state. | **[NIST-SP800-53r5]** CM-3, CM-4, SA-10<br>**[NIST-SP800-137]** Section D<br>**[NIST-SP800-160V1]** 3.3.5, 3.8.3, 3.8.4<br>**NERC CIP** 007-6-R2 |
| **IP-3 \| EV** | This may include development systems, OTA updates to customer vehicles, and operational systems. | **[NIST-SP800-53r5]** CM-3, CM-4, SA-10<br>**ISO 24089:2023** 4.3.4.4, 4.3.4.6, 6.3.4.7, 7.3.2.1, 7.3.4.10, 9.3.2.14 |
| **IP-3 \| XFC/EVSE** | This may include development systems, operational systems, and IT/ICS systems. EVSE manufacturers may consider implementing configuration management mechanisms to prevent unwanted changes that might occur by maintenance errors. | **ISA/IEC 62443-2-1:D4E1** CM 1.3, CM 1.4<br>**ISA/IEC 62443-3-3:2013** SR 7.6 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **IP-3 \| Cloud/Third-Party** | This may include development systems, operational systems, and IT/ICS systems. | **[NIST-SP800-53r5]** CM-3, CM-4, SA-10 |
| **IP-3 \| Utility/Building Management System** | This may include development systems, operational systems, and IT/ICS systems. | **ISA/IEC 62443-2-1:D4E1** CM 1.3, CM 1.4<br>**ISA/IEC 62443-3-3:2013** SR 7.6 |
| **IP-4:**<br>Backups of information are conducted, maintained, and tested. | **Ecosystem:** Backups may include software versions, licenses, system information, certificates, key material, and/or user information. The length of time these backups are maintained should be considered based on their business needs or compliance requirements. | **[NIST-SP800-53r5]** CP-4, CP-6, CP-9<br>**NERC CIP** 009-6-R1, 009-6-R2 |
| **IP-4 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CP-4, CP-6, CP-9 |
| **IP-4 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** AVAIL 2.1<br>**ISA/IEC 62443-3-3:2013** SR 7.3, SR 7.4 |
| **IP-4 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CP-4, CP-6, CP-9 |
| **IP-4 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** AVAIL 2.1<br>**ISA/IEC 62443-3-3:2013** SR 7.3, SR 7.4 |
| **IP-5:**<br>Policy and regulations regarding the physical operating environment for organizational assets are met. | **Ecosystem:** The physical operating environment may impact safety and the function of IT and OT components. This could include reviewing emergency lighting, fire protection, and climate controls. Meeting these policies may include activities such as creating and consistently updating policies regarding access controls, awareness and training, maintenance, or safety criteria. Consider regulations and policies at all levels. | **[NIST-SP800-53r5]** PE-1, PE-12, PE-13, PE-14<br>**ISO/SAE 21434** |
| **IP-5 \| EV** | This may include assets connected to, or accessible from, EVSE or Utility/Building assets (e.g., BESS, charging ports, system temperature/safety thresholds). | **[NIST-SP800-53r5]** PE-1, PE-12, PE-13, PE-14<br>**ISO/SAE 21434** |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **IP-5 \| XFC/EVSE** | This may include automatic failsafe states for EVSE assets connected to EV, Cloud/Third-Party, or Utility/Building assets. This may include physical status indications (e.g., tamper alarms, sensor readings) for deployed equipment and panels. | **[NIST Handbook 44]** 3.40 S.3.3<br>**ISA/IEC 62443-2-1:D4E1** ORG 3.1, AVAIL 1.2 |
| **IP-5 \| Cloud/Third-Party** | This may include Cloud/Third-Party assets connected to utility/building assets. | **[NIST-SP800-53r5]** PE-1, PE-12, PE-13, PE-14 |
| **IP-5 \| Utility/Building Management System** | This may include physical status indications (e.g., tamper alarms) for deployed equipment and panels. | **ISA/IEC 62443-2-1:D4E1** ORG 3.1, AVAIL 1.2 |
| **IP-6:**<br>Data is destroyed according to policy. | **Ecosystem:** Consider any organization data that is located within third-party or partner organizations and provide mechanisms and procedures to verify that data destruction has been done in accordance with the ecosystem's policy. The ecosystem may conduct audits and reviews to ensure that data is destroyed according to policy. Consider reviewing data sanitization procedures and component disposal. | **[NIST-SP800-53r5]** MP-6, SR-12<br>**NERC CIP** 011-2-R2 |
| **IP-6 \| EV** | Policies related to account, payment systems and information, transactional, PII, or other sensitive data may be treated as higher priority, including additional policies or mechanisms regarding data destruction, data sanitization, or auditing. | **[NIST-SP800-53r5]** MP-6, SR-12 |
| **IP-6 \| XFC/EVSE** | Policies related to account, payment systems and information, transactional, PII, or other sensitive data may be treated as higher priority, including additional policies or mechanisms regarding data destruction, data sanitization, or auditing. | **ISA/IEC 62443-2-1:D4E1** DATA 1.6<br>**ISA/IEC 62443-3-3:2013** SR 4.2 |
| **IP-6 \| Cloud/Third-Party** | This may include account, financial, or connection data, as well as the creation of a data destruction policy. Cloud providers handling financial payment card data may likely be implementing data storage, data retention, and data disposal policy consistent with existing standards (i.e., Payment Card Industry Data Security Standard (DSS)). | **[NIST-SP800-53r5]** MP-6, SR-12 |
| **IP-6 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** DATA 1.6<br>**ISA/IEC 62443-3-3:2013** SR 4.2 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **IP-7:**<br>Protection processes are improved. | **Ecosystem:** The motivation for such improvements may come from lessons learned, improved attacker capabilities (as documented by threat and vulnerability reports), a change in the criticality of an asset as well as improved or increased security tools or practices. Organizations can consider implementing processes to validate the improvements were implemented effectively (e.g., establishing after action report process, documenting lessons learned, and updating response and recovery plans).<br>Protection processes related to sensitive user data may be considered as a higher priority. | **[NIST-SP800-53r5]** CA-2, CA-7, CA-8, CP-2, CP-4, IR-3, IR-8, PL-2, PM-6<br>**NERC CIP** 009-6-R3 |
| **IP-7 \| EV** | Protection processes related to safety critical systems may be considered as higher priority. Manufacturers may consider implementing a database of past events to better track and manage events and corresponding improvement processes. | **[NIST-SP800-53r5]** CA-2, CA-7, CA-8 |
| **IP-7 \| XFC/EVSE** | Protection processes related to safety critical systems may be considered as a higher priority. Owners/operators/manufacturers may consider implementing a database of past events to better track and manage events and corresponding improvement processes. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1 |
| **IP-7 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CA-2, CA-7, CA-8 |
| **IP-7 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1 |
| **IP-8:**<br>Effectiveness of protection technologies is shared. | **Ecosystem:** Consider participation in collaborative forums such as the E-ISAC or Auto-ISAC. Sharing the effectiveness of protection technologies benefits the community, and distributing within the domain is especially beneficial. | **[NIST-SP800-53r5]** AC-21, CA-7, CP-2, IR-6, SI-4<br>**[NIST-SP800-150]**<br>**NERC CIP** 009-6-R3 |
| **IP-8 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** IR-6<br>**[NIST-SP800-150]** |
| **IP-8 \| XFC/EVSE** | Manufacturers may consider including standards development and interoperability of systems and components as part of the information sharing process. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1 |
| **IP-8 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** IR-6<br>**[NIST-SP800-150]** |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **IP-8 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1 |
| **IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. | **Ecosystem:** Response and recovery plans identify essential functions and associated contingency requirements, as well as provide a roadmap for implementation. These plans may include incident response, business continuity, incident recovery, and disaster recovery plans. Plans may consider incorporating recovery objectives, restoration priorities, tests, metrics, contingency roles, personnel assignments, and contact information. Consider prioritizing maintaining essential functions despite system disruption or manipulation when developing plans, as well as the eventual restoration to normal operations. Members can consider updating response and recovery plans based on improvements identified in PR.IP-7, including testing (e.g., pen testing) to ensure efficacy of plans. Implementing RS.RP-1 and RC.RP-1 is dependent on and consistent with this Subcategory. | **[NIST-SP800-53r5]** CM-3, CM-4, SA-10<br>**[NIST-SP800-61r2]** Section D<br>**[NIST-SP800-160V1]** 6.5, 6.6, Appendix F.2<br>**IEC61850-90-12** 5.8, 4.12-4.14<br>**NERC CIP** 009-6-R1, 009-6-R3 |
| **IP-9 \| EV** | Manufacturers should consider defining clear responsibilities for the vehicle components during response and recovery plans. The components may include hardware, software, networks, operators, and cloud/third-party systems providers. | **[NIST-SP800-53r5]** CM-3, CM-4, SA-10<br>**[NIST-SP800-61r2]** Section D<br>**[NIST-SP800-160V1]** 6.5, 6.6, Appendix F.2<br>**IEC61850-90-12** 5.8, 4.12-4.14 |
| **IP-9 \| XFC/EVSE** | Manufacturers/owners should consider defining clear responsibilities for the charging site components during response and recovery plans. The components may include hardware, software, networks, operators, and cloud/third-party systems providers. | **[NIST Handbook 44]** 3.40 S.2.3<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.8, AVAIL 1.1 |
| **IP-9 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CM-3, CM-4, SA-10<br>**[NIST-SP800-61r2]** Section D<br>**[NIST-SP800-160V1]** 6.5, 6.6, Appendix F.2 |
| **IP-9 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.8, AVAIL 1.1 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **IP-10:**<br>Response and recovery plans are tested. | **Ecosystem:** Testing may be conducted stand alone or in conjunction with other members. Ecosystem members can consider additional steps to verify that the appropriate parties are included in recovery and response plan tests, which may include contingency plan testing, business continuity testing, or incident response testing. When scenarios cannot be feasibly tested, a tabletop exercise (TTX) format may be used. After action reports (AARs) may be subsequently written and used to improve response. | **[NIST-SP800-53r5]**<br>CP-4, IR-3, PM-14<br>**[NIST-SP800-115]**<br>**[NIST-IR8270]**<br>**IEC 61850-90-4**<br>14.2.4, 5.4.2.5<br>**NERCGridEx**<br>**NERC CIP**<br>009-6-R2 |
| **IP-10 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]**<br>CP-4, IR-3, PM-14<br>**[NIST-SP800-115]** |
| **IP-10 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>EVENT 1.8, AVAIL 1.1<br>**ISA/IEC 62443-3-3:2013**<br>SR 3.3 |
| **IP-10 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]**<br>CP-4, IR-3, PM-14<br>**[NIST-SP800-115]** |
| **IP-10 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>EVENT 1.8, AVAIL 1.1<br>**ISA/IEC 62443-3-3:2013**<br>SR 3.3 |
| **IP-11:**<br>Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening). | **Ecosystem:** This may include practices such as deprovisioning, personnel screening, new hire training, policy development and communication, and ensuring data use adheres to company mission and goals. | **[NIST-SP800-53r5]**<br>PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21<br>**NERC CIP**<br>004-6-R2, 004-6-R3, 004-6-R4, 004-6-R5 |
| **IP-11 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]**<br>PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9 |
| **IP-11 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 1.1, ORG 1.2 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **IP-11 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9 |
| **IP-11 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1, ORG 1.2 |
| **IP-12:** A vulnerability management plan is developed and implemented. | **Ecosystem:** Vulnerability management plans may include vulnerability identification, scoring, mitigation, response, information sharing, and coordinated efforts. Ecosystem members may consider using a measurement framework and Cyber Threat Intelligence (CTI) to determine risk postures from vulnerabilities and prioritize management activities or strategies. (e.g., The Common Vulnerability Scoring System (CVSS), National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CVE), and Common Weakness Enumeration (CWE)). | **[NIST-SP800-53r5]** RA-1, RA-3, RA-5, SI-2<br>**CISA-CIVR-PB** Appendix A<br>**NERC CIP** 007-6-R2, 007-6-R3 |
| **IP-12 \| EV** | This may include development systems, OTA updates to customer vehicles, and operational systems. | **[NIST-SP800-53r5]** RA-1, RA-3, RA-5<br>**ISO/SAE 21434** RQ-05-09, RQ-05-10, RQ-08-05, RQ-08-07, RQ-08-08<br>**ISO 24089:2023** 4.3.3.1, 7.3.1.3 |
| **IP-12 \| XFC/EVSE** | This may include development systems, operational systems, and IT/ICS systems. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.9 |
| **IP-12 \| Cloud/Third-Party** | This may include development systems, operational systems, and IT/ICS systems. | **[NIST-SP800-53r5]** RA-1, RA-3, RA-5 |
| **IP-12 \| Utility/Building Management System** | This may include development systems, operational systems, and IT/ICS systems. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.9 |

### 5.2.5. Maintenance Category

Maintenance and repairs of industrial control and information system components are performed, consistent with policies and procedures.

Though maintenance and repairs of OT and IT system components are not unique to the EV/XFC ecosystem, organizations need to understand the level of interdependencies between IT and OT and the corresponding influence on maintenance policy and procedures.

**Table 12.** Protect: Maintenance Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **MA-1:**<br>Maintenance and repair of organizational assets are performed and logged with approved and controlled tools. | **Ecosystem:** An approved suite of tools may be put in place to control the configuration, planning and maintenance of assets, including consideration for automated discovery and policy compliance checks. This may include tools utilized for both local, physical maintenance, and repair as well as remote servicing of equipment. Ensure that any maintenance or repair done by a partner or subcontractor on behalf of the organization is done in a manner that is approved by the organization. | **[NIST-SP800-53r5]**<br>MA-1, MA-2, MA-3, MA-5, MA-6<br>**NERC CIP**<br>006-6-R3 |
| **MA-1 \| EV** | This may involve providing a maintenance institution validation process so EV owners can identify accredited mechanics. Accreditation may include verifying that the tooling used is qualified, and that maintenance technicians or mechanics are appropriately trained or certified. | **[NIST-SP800-53r5]**<br>MA-1, MA-2, MA-3, MA-5, MA-6 |
| **MA-1 \| XFC/EVSE** | This may involve verifying physical anti-tamper mechanisms, such as door sensors or tamper-evident seals, to ensure that processes are being followed. EVSE owners/operators/manufacturers may consider logging and auditing remote maintenance sessions. | **ISA/IEC 62443-2-1:D4E1**<br>AVAIL 1.2 |
| **MA-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party specific considerations. | **[NIST-SP800-53r5]**<br>MA-1, MA-2, MA-3, MA-5, MA-6 |
| **MA-1 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>AVAIL 1.2 |
| **MA-2:**<br>Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. | **Ecosystem:** Manual approval of remote maintenance access and Multi-Factor Authentication (MFA) may help prevent unauthorized access. This maintenance may entail safety aspects of all systems that depend on or interact with the asset being worked on. | **[NIST-SP800-53r5]**<br>MA-4<br>**[NIST-SP800-161]**<br>V1 Appendix F1.14<br>**NERC CIP**<br>006-6-R3 |
| **MA-2 \| EV** | Applicable, but no additional EV specific considerations. | **[NIST-SP800-53r5]**<br>MA-4 |
| **MA-2 \| XFC/EVSE** | This may involve verifying that sensors or tamper-evident seals are installed to ensure that processes are being followed. Both physical access and wireless access methods may be considered. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 3.1<br>**OIML D31:2019**<br>6.2.8.3 |
| **MA-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party specific considerations. | **[NIST-SP800-53r5]**<br>MA-4 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **MA-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 3.1 |

### 5.2.6. Protective Technology Category

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Much of the technology within the EV/XFC ecosystem is single purpose or unique to the domains within the ecosystem. Commercial off-the-shelf (COTS) security solutions may need modification or tuning to function properly and avoid unintended consequences.

**Table 13.** Protect: Protective Technology Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. | **Ecosystem:** These logs may include information regarding asset access, modification, communications, data, or use.<br>Logging all events is not practical; therefore, audit logging should consider being informed by risk, organizational needs, risk tolerance and industry best practices. Logs may be used for activities such as establishing system baselines, tracking changes, identifying trends between units, diagnosing problems, detecting anomalies, etc.<br>Wherever practical, logging and audit mechanisms should consider producing data elements in accordance with standard data formats to facilitate parsing and consumption by analytic teams.<br>Consider maintaining audit logs for extended periods to support forensic analysis. Audit logging should consider being determined by risk tolerance and tailored by industry best practices. | **[NIST-SP800-53r5]** AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16<br>**[NIST-SP800-92]**<br>**[NIST-SP800-161]** 3.3.2, 3.3.5<br>**NERC CIP** 006-6-R1 |
| **PT-1 \| EV** | EV manufacturers can consider logging system status and health over time, including indicators such as battery health. | **[NIST-SP800-53r5]** AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16<br>**[NIST-SP800-92]** |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **PT-1 \| XFC/EVSE** | Logging calibration parameters, access, maintenance, and updates may be considered. | **[NIST Handbook 44]** 3.40 S.3.3<br>**ISA/IEC 62443-2-1:D4E1** NET 1.10, DATA 1.1, EVENT 1.4, EVENT 1.7<br>**ISA/IEC 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12<br>**OIML D31:2019** 6.2.8.4.6 |
| **PT-1 \| Cloud/Third-Party** | In addition to sending metering values from EVSE to the cloud, cloud/third-party owners/operators may also consider logging smart meters for the utility/building management systems. | **[NIST-SP800-53r5]** AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16<br>**[NIST-SP800-92]** |
| **PT-1 \| Utility/Building Management System** | Logging historical system demand as a function of time and location may be considered. | **ISA/IEC 62443-2-1:D4E1** NET 1.10, DATA 1.1, EVENT 1.4, EVENT 1.7<br>**ISA/IEC 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 |
| **PT-2:**<br>Removable media is protected, and its use restricted according to policy. | **Ecosystem:** Removable media may include hard drives, flash drives, Compact Discs (CDs), Digital Versatile Discs (DVDs), and Secure Digital (SD) cards. Authorized use practices may include encryption, access management, sanitization, and malware scanning when utilizing removable media to limit cybersecurity risks.<br>Both physical and wireless access methods can be considered for removable media. | **[NIST-SP800-53r5]** MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8<br>**NERC CIP** 006-6-R2, 007-6-R1 |
| **PT-2 \| EV** | Removable media may include connections made through EV-specific ports or hardware (e.g., On-Board Diagnostic II (OBD-II), Controller Area Network (CAN), Infotainment). | **[NIST-SP800-53r5]** MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **PT-2 \| XFC/EVSE** | Removable media may include EVSE-specific ports or hardware (e.g., maintenance ports, maintenance service equipment, diagnostic equipment, etc). | **[NIST Handbook 44]** 1.10 G-S.8.2<br>**ISA/IEC 62443-2-1:D4E1** DATA 1.1, DATA 1.2<br>**ISA/IEC 62443-3-3:2013** SR 2.3<br>**OIML G22:2022** 4.4.3.2.1, 4.4.3.2.3<br>**OIML D31:2019** 6.1.3.2.1, 6.1.3.2.4 |
| **PT-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 |
| **PT-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management-specific considerations. | **ISA/IEC 62443-2-1:D4E1** DATA 1.1, DATA 1.2<br>**ISA/IEC 62443-3-3:2013** SR 2.3 |
| **PT-3:**<br>The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | **Ecosystem:** The principle of least functionality reduces the attack surface, facilitates anomaly detection, and may help contain an incident in the event of a compromise. Consideration may be given to whether non-essential functionalities including connection ports, communication protocols, and active modes should consider being deactivated. | **[NIST-SP800-53r5]** AC-2, AC-3, CM-7<br>**NERC CIP** 007-6-R1 |
| **PT-3 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** AC-2, AC-3, CM-7 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **PT-3 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>NET 1.01, NET 1.06, NET 1.07, NET 2.2, COMP 1.1, DATA 1.1, DATA 1.2, DATA 1.8, DATA 1.9, USER 1.04, USER 1.05, USER 1.06, USER 1.08, USER 1.09, USER 1.11, USER 1.15, USER 1.17, USER 1.18, USER 2.1, USER 2.2, USER 2.3, USER 2.4<br>**ISA/IEC 62443-3-3:2013**<br>SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 |
| **PT-3 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]**<br>AC-2, AC-3, CM-7 |
| **PT-3 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>NET 1.01, NET 1.06, NET 1.07, NET 2.2, COMP 1.1, DATA 1.1, DATA 1.2, DATA 1.8, DATA 1.9, USER 1.04, USER 1.05, USER 1.06, USER 1.08, USER 1.09, USER 1.11, USER 1.15, USER 1.17, USER 1.18, USER 2.1, USER 2.2, USER 2.3, USER 2.4<br>**ISA/IEC 62443-3-3:2013**<br>SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **PT-4:**<br>Communications and control networks are protected. | **Ecosystem:** The ecosystem may consider enacting protection of communications and control networks throughout the lifecycle. Some controls can only be applied during the architectural phase, while others can be added in the operations or deployment phases.<br>Implementing some security measures can lead to performance degradation. Organizations may verify that protective measures will not adversely affect overall system performance requirements.<br>These network protections may consider following common IT or OT network protections, including firewalls, encryption, antivirus, etc. | **[NIST-SP800-53r5]** AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47<br>**[NIST-SP800-160V1]** Appendix F<br>**NERC CIP** 006-6-R1 |
| **PT-4 \| EV** | Communication and control networks may include information systems for internally communicated traffic, onboard electronic management and control systems, and interfaces with external networks or information systems. Networks may include a vehicle's central gateway module, sensors, control units, communication modules, telematics units, and battery management systems. External systems may include network traffic with charging stations, grid systems, and external servers. The use of hardware/software gateways should be considered. EV manufacturers may consider the use of mechanisms to segment a vehicle's internal networks, and authenticate devices on the internal network, as well as communication between internal networks. | **[NIST-SP800-53r5]** AC-12, AC-17, AC-18, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23 |
| **PT-4 \| XFC/EVSE** | Communication and control networks may include information systems for internally communicated traffic, onboard electronic management and control systems, and interfaces with external networks or information systems. EVSE manufacturers can consider incorporating protections for non-standard networks including Internet of Things (IoT), Industrial Internet of Things (IIoT), and Mesh networks. | **ISA/IEC 62443-2-1:D4E1**<br>CM 1.3, NET 1.01, NET 1.02, NET 1.04, NET 1.05, NET 1.06, NET 1.09, USER 1.16<br>**ISA/IEC 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6<br>**OIML D31:2019** 6.2.2.1.1, 6.2.5.2.d |
| **PT-4 \| Cloud/Third-Party** | Cloud/Third-Party owners/operators may consider implementing protection mechanisms for and with communications and network traffic in EVs, EVSEs, smart grid systems, and both normal and abnormal scenarios. | **[NIST-SP800-53r5]** AC-12, AC-17, AC-18, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **PT-4 \| Utility/Building Management System** | Utility/Building management owners/operators may consider implementing protection mechanisms to communications and network traffic in EVSEs, smart grid systems, and other utility and building management systems. | **ISA/IEC 62443-2-1:D4E1** CM 1.3, NET 1.01, NET 1.02, NET 1.04, NET 1.05, NET 1.06, NET 1.09, USER 1.16<br>**ISA/IEC 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 |
| **PT-5:**<br>Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | **Ecosystem:** These mechanisms may be implemented to automatically activate upon detecting adverse conditions. Resilience mechanisms may include fault tolerant architectures, resource management strategies and activities, backup/recovery plans, and cyber security protection frameworks. | **[NIST-SP800-53r5]** CP-7, CP-8, CP-11, CP-12, CP-13, PE-11, PL-8, SC-6, SC-24 |
| **PT-5 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CP-7, CP-8, CP-11, CP-12, CP-13 |
| **PT-5 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-3-3:2013** SR 7.1, SR 7.2 |
| **PT-5 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]**<br>CP-7, CP-8, CP-11, CP-12, CP-13 |
| **PT-5 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-3-3:2013** SR 7.1, SR 7.2 |

## 5.3. Detect Function Considerations Across the EV/XFC Domains

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.

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

### 5.3.1. Anomalies and Events

Anomalous activity is detected, and the potential impact of events is understood.

In the context EV/XFC, anomalies that occur within domains may also impact other domains or the entire ecosystem. Agreements made in advance regarding data and event sharing between the various ecosystem members and domains warrant consideration.

**Table 14.** Detect: Anomalies and Events Category

| Subcategory\| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AE-1:**<br>A baseline of network operations and expected data flows for users and systems is established and managed. | **Ecosystem:** EV/XFC ecosystem members can consider using operational data in these baselining efforts. This baseline may be used to help behavioral anomaly detections and determine anomalous cybersecurity activities or events. Baseline information cataloged may include normal traffic levels, message formats, safe operating ranges, network/system activity, etc. Higher baseline levels of information may be kept for more critical systems. | **[NIST-SP800-53r5]** AC-4, CA-3, CM-2, SC-16, SI-4<br>**[NIST-SP800-92]**<br>**[NIST-SP800-161]** 3.3.2, 3.3.5 |
| **AE-1 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** AC-4, CA-3, CM-2, SC-16, SI-4 |
| **AE-1 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** NET 1.01 |
| **AE-1 \| Cloud/Third-Party** | Cloud/Third-Party considerations may include maintaining a baseline of users' behaviors such as, charging sessions telemetry, and devices' configurations, in order to detect any suspicious or malicious deviations. | **[NIST-SP800-53r5]** AC-4, CA-3, CM-2, SC-16, SI-4 |
| **AE-1 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** NET 1.01 |
| **AE-2:**<br>Detected events are analyzed to understand attack targets and methods. | **Ecosystem:** Event analysis may utilize Cyber Threat Intelligence (CTI) sources, such as Information Sharing and Analysis Centers (ISACs) or vulnerability databases, to better understand and determine the impacts and attack vectors or vulnerabilities used during the event. | **[NIST-SP800-53r5]** AU-6, CA-7, IR-4, RA-5, SI-4<br>**[NIST-SP800-128]**<br>**NERC CIP** 007-6-R4 |
| **AE-2 \| EV** | Applicable, but no additional EV specific considerations. | **[NIST-SP800-53r5]** AU-6, CA-7, IR-4, RA-5, SI-4 |

| Subcategory\| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AE-2 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.7<br>**ISA/IEC 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 |
| **AE-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** AU-6, CA-7, IR-4, RA-5, SI-4<br>**[NIST-SP800-128]** |
| **AE-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.7<br>**ISA/IEC 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 |
| **AE-3:** Event data are collected and correlated from multiple sources and sensors. | **Ecosystem:** A diverse set of sources may provide a more complete understanding. Ecosystem members may consider using correlated data from multiple systems or partners to better analyze events. Consider collecting event data from all networks, systems, and communication affected or involved in the cyber event. EV/XFC ecosystem members may consider correlating data across domains. Cyber events may be analyzed to predict consequences and develop better indicators of ongoing cyber-attacks. | **[NIST-SP800-53r5]** AU-6, CA-7, CP-2, IR-4, IR-5, IR-8, SI-4<br>**[NIST-SP800-160V1]** 3.3.7, Appendix G.2, Appendix G.3<br>**NERC CIP** 007-6-R4 |
| **AE-3 \| EV** | Important EV-specific data collected may include Battery Management System (BMS) sensor data readings, communications with the external systems, information generated by or related to safety-critical systems, etc. | **[NIST-SP800-53r5]** IR-4, IR-5, IR-8 |
| **AE-3 \| XFC/EVSE** | Important EVSE-specific data collected may include output current and voltage sensor readings, communications with external systems including the EV, etc. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.7<br>**ISA/IEC 62443-3-3:2013** SR 6.1 |
| **AE-3 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** IR-4, IR-5, IR-8 |

| Subcategory\| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AE-3 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.7<br>**ISA/IEC 62443-3-3:2013** SR 6.1 |
| **AE-4:**<br>Impact of events is determined. | **Ecosystem:** Impact analysis may be used to prioritize event handling actions and activities. Event impact may be determined with regard to the systems, networks, and communications involved or effected in the attacks, their stated functions, how functions have been compromised, and road to recovery or restoration of normal functionality. | **[NIST-SP800-53r5]** CP-2, IR-3, IR-4, IR-5, IR-8, SI-4<br>**[NIST-SP800-61r2]** |
| **AE-4 \| EV** | Applicable, but no additional EV-specific considerations. | **ISO/SAE 21434** 15-01, RQ-08-04, RQ-08-05 |
| **AE-4 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.8 |
| **AE-4 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-3, IR-4, IR-5, IR-8, SI-4 |
| **AE-4 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.8 |
| **AE-5:**<br>Incident alert thresholds are established. | **Ecosystem:** Thresholds are established to distinguish between anomalies and cyber events, which may initiate a response when the system leaves the normal operating range or is considered under attack/duress. When considering thresholds, consider including the creation and updating of relevant threshold criteria. EV/XFC ecosystem members can consider integrating operational limits into alert thresholds. | **[NIST-SP800-53r5]** IR-4, IR-5, IR-8<br>**NERC CIP** 007-6-R4, 007-6-R5 |
| **AE-5 \| EV** | Applicable, but no additional EV-specific considerations. | **ISO/SAE 21434** Clause 8 and clause 13.3 |
| **AE-5 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.1, EVENT 1.7 |
| **AE-5 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** IR-4, IR-5, IR-8 |
| **AE-5 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.1, EVENT 1.7 |

### 5.3.2. Security Continuous Monitoring

The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

Due to the interdependence of IT and OT in the EV/XFC ecosystem, fusion of data from IT and OT events will add significant value to the subsequent analysis.

**Table 15.** Detect: Security Continuous Monitoring Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **CM-1:**<br>The network is monitored to detect potential cybersecurity events. | **Ecosystem:** This may include implementing network monitoring tools and methods to analyze network traffic for unauthorized or abnormal access attempts, irregular network traffic volume or contents, or flow of information including increased monitoring to information leaving the network. Ecosystem members may consider establishing formal procedures and contingency plans for reporting and responding to detected cybersecurity risks. | **[NIST-IR7800]**<br>**[NIST-SP800-53r5]** AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16<br>**NERC CIP** 006-6-R1, 006-6-R2 |
| **CM-1 \| EV** | Network monitoring may include internally communicated traffic within the EV and traffic with external systems, including EVSE and Cloud/Third-Party systems. The network may include the vehicle's central gateway module, sensors, control units, communication modules, telematics units, and battery management systems. Data exchange between external systems may include information on vehicle performance, battery performance, charging history, vehicle owners, communications with charging stations, grid systems, and external servers. | **[NIST-SP800-53r5]** AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16 |
| **CM-1 \| XFC/EVSE** | Network monitoring may include internally communicated traffic within the EVSE and traffic with external systems, including EV and Cloud/Third-Party systems. The network may include information on transactions, charging and battery-related information/metrics, and sensor readings. EVSE owners/operators may consider including non-standard networks including IoT, IIoT and Mesh networks. EVSE owners/operators may consider collecting data and monitor the telemetry from multiple sources and sensors, which may provide a more complete network status. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.1<br>**ISA/IEC 62443-3-3:2013** SR 6.2 |
| **CM-1 \| Cloud/Third-Party** | Monitoring may include network traffic with EVs, EVSEs, smart grid systems, and both normal and abnormal activity. | **[NIST-SP800-53r5]** AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16 |
| **CM-1 \| Utility/Building Management System** | Monitoring may include network traffic with EVSEs, smart grid systems, and other utility and building management systems. Utility/Building Management owners/operators can consider including non-standard networks, including IoT, IIoT and Mesh networks. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.1<br>**ISA/IEC 62443-3-3:2013** SR 6.2 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **CM-2:**<br>The physical environment is monitored to detect potential cybersecurity events. | **Ecosystem:** Monitoring may include continuously monitoring critical components, systems, and processes that have been identified as potential cybersecurity risks, are safety-critical, or have safety considerations. Subcomponents (e.g., microcontrollers, sensors, electrical wiring, connectors.) critical to the function of onboard controllers and management systems may be included in the continuous monitoring of the physical environment. | **[NIST-SP800-53r5]**<br>CA-7, PE-6, PE-20 |
| **CM-2 \| EV** | Critical hardware components may include the head unit system, on-board-diagnostic interfaces, telematic control units, central gateway modules, battery management systems, electronic control units, and communication controllers. This may include logging, alarming or monitoring CAN access ports, physical access ports, and connections. | **[NIST-SP800-53r5]**<br>PE-6, PE-20 |
| **CM-2 \| XFC/EVSE** | Critical hardware components may include the charging station controllers, power module controls, protection circuits, power conversion systems, supply equipment communication controllers, thermal management systems, human-machine interfaces, and EVSE meter equipment. This may include means to monitor status such as tamper switches or alarms, and sensors for safety-critical systems/components. | **ISA/IEC 62443-2-1:D4E1**<br>EVENT 1.1 |
| **CM-2 \| Cloud/Third-Party** | Critical hardware components may include physical data centers, network equipment, servers, or storage devices. | **[NIST-SP800-53r5]**<br>PE-6, PE-20 |
| **CM-2 \| Utility/Building Management System** | This may include monitoring the status of equipment with tools such as area access monitoring and device tamper switches or alarms. Critical hardware components may include the power distribution units, remote-controlled breakers, local circuit protection, and generation/storage grid systems. | **ISA/IEC 62443-2-1:D4E1**<br>EVENT 1.1 |
| **CM-3:**<br>Personnel activity is monitored to detect potential cybersecurity events. | **Ecosystem:** Personnel monitoring may include activities during pre-deployment (e.g., manufacturing, assembly, and distribution), deployment (e.g., installation and commissioning), and post-deployment (e.g., operation, maintenance, and upgrade). This may include limiting ease of access to internal systems or components after development, monitoring new connections or connection attempts, and monitoring changes in system settings. | **[NIST-SP800-53r5]**<br>AC-2, AU-12, AU-13, CA-7, CM-10, CM-11<br>**NERC CIP**<br>006-6-R1, 007-6-R4, 007-6-R5 |
| **CM-3 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]**<br>AC-2, AU-12, AU-13 |
| **CM-3 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>EVENT 1.1<br>**ISA/IEC 62443-3-3:2013**<br>SR 6.2 |
| **CM-3 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]**<br>AC-2, AU-12, AU-13 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **CM-3 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.1<br>**ISA/IEC 62443-3-3:2013** SR 6.2 |
| **CM-4:**<br>Malicious code is detected. | **Ecosystem:** Detection activities may incorporate commonly used Tactics, Techniques, and Procedures (TTPs), unauthorized code execution, and/or unusual system activity. | **[NIST-SP800-53r5]** SC-44, SI-3, SI-4, SI-8<br>**[NIST-SP800-218]**<br>**NERC CIP** 007-6-R3 |
| **CM-4 \| EV** | EV manufacturers can consider providing means to ensure the ability to analyze and detect malicious code affecting software and firmware on EV computer systems that may include vehicle control units, communication modules, charging systems, and battery management systems. | **[NIST-SP800-53r5]** SI-3, SI-4, SI-8<br>**ISO/SAE 21434** RQ-08-01, RQ-08-03 |
| **CM-4 \| XFC/EVSE** | EVSE manufacturers may consider providing means of ensuring the ability to analyze and detect malicious code affecting software and firmware on EVSE computer systems that may include the communication modules, charge control systems, power distribution modules, and energy management systems. | **ISA/IEC 62443-2-1:D4E1** COMP 2.2<br>**ISA/IEC 62443-3-3:2013** SR 3.2 |
| **CM-4 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** SI-3, SI-4, SI-8 |
| **CM-4 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** COMP 2.2<br>**ISA/IEC 62443-3-3:2013** SR 3.2 |
| **CM-5:**<br>Unauthorized mobile code is detected. | **Ecosystem:** Mobile code includes software being sent between devices, software or code that is remotely executable on another device, and/or scripted code formats. Members may consider only providing access to controlled and monitored mobile code. | **[NIST-SP800-53r5]** SC-18, SC-44, SI-4<br>**NERC CIP** 007-6-R3 |
| **CM-5 \| EV** | Applicable, but no additional EV specific considerations. | **[NIST-SP800-53r5]** SC-18, SC-44<br>**ISO/SAE 21434** RQ-08-01, RQ-08-03 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **CM-5 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** USER 1.06, EVENT 1.1<br>**ISA/IEC 62443-3-3:2013** SR 2.4 |
| **CM-5 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** SC-18, SC-44 |
| **CM-5 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** USER 1.06, EVENT 1.1<br>**ISA/IEC 62443-3-3:2013** SR 2.4 |
| **CM-6:**<br>External service provider activity is monitored to detect potential cybersecurity events. | **Ecosystem:** Directly applicable to the EV/XFC ecosystem. The ecosystem comprises four distinct domains that require a level of service from each other to function. | **[NIST-SP800-53r5]** CA-7, PS-7, SA-4, SA-9, SI-4<br>**NERC CIP** 006-6-R1, 007-6-R4, 007-6-R5 |
| **CM-6 \| EV** | Service provider activity may include remote access attempts and software updates to onboard electronic management and control systems. EV manufacturers may consider monitoring external service interactions with hardware components that may include the telematics units, infotainment and navigation systems, remote keyless entry systems, diagnostic ports, and charging systems. | **[NIST-SP800-53r5]** CA-7, PS-7, SA-4, SA-9<br>**ISO/SAE 21434** RQ-08-01, RQ-08-03 |
| **CM-6 \| XFC/EVSE** | Service provider activity may include remote access attempts, configuration changes, software updates, and diagnostic tests to onboard electronic management and control systems. EVSE manufacturers can consider monitoring external service interactions with hardware components that may include metering equipment, payment processing units, communication modules, and charge control systems. EVSE owner/operators may consider implementing remote access controls for remote EVSE manufacturers. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1, ORG 1.3 |
| **CM-6 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party specific considerations. | **[NIST-SP800-53r5]** CA-7, PS-7, SA-4, SA-9 |
| **CM-6 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1, ORG 1.3 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **CM-7:**<br>Monitoring for unauthorized personnel, connections, devices, and software is performed. | **Ecosystem:** The effectiveness of this subcategory depends on the implementation of other CSF Subcategories, such as putting processes in place to monitor organizational systems, controlling physical access to equipment, track and monitor assets, or maintaining change management controls. | **[NIST-SP800-53r5]**<br>AU-12, CA-7, CM-3, CM-8, PE-6, PE-20, SI-4<br>**NERC CIP**<br>006-6-R1, 007-6-R3, 005-6-R4, 007-6-R5 |
| **CM-7 \| EV** | This may include steps of the equipment lifecycle, from manufacture and assembly to operation and maintenance. Factors for monitoring may include new connections to communication buses, new mobile devices connections, electronics hardware access, and changes in settings. | **[NIST-SP800-53r5]**<br>CM-3, CM-8, PE-6, PE-20<br>**ISO/SAE 21434**<br>RQ-08-01, RQ-08-03 |
| **CM-7 \| XFC/EVSE** | This may include steps of the equipment lifecycle, from manufacture, assembly, deployment, operation, and maintenance. Factors to monitor may include new connections to communication buses, EV identification at charging port, and opening of the EVSE enclosure. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 2.2, EVENT 1.1 |
| **CM-7 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]**<br>CM-3, CM-8, PE-6, PE-20 |
| **CM-7 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 2.2, EVENT 1.1 |
| **CM-8:**<br>Vulnerability scans are performed. | **Ecosystem:** Scans may be performed by the organization itself or contracted out to external parties such as red/purple team and penetration testing activities. | **[NIST-SP800-53r5]**<br>RA-5<br>**[NIST-SP800-115]** |
| **CM-8 \| EV** | Vulnerability scans may include the telematics units, infotainment and navigation systems, remote keyless entry systems, diagnostic ports, and charging systems. | **[NIST-SP800-53r5]**<br>RA-5<br>**[NIST-SP800-115]**<br>**ISO/SAE 21434**<br>RC-10-12, RQ-08-01, RQ-08-03, RQ-11-01 |
| **CM-8 \| XFC/EVSE** | Vulnerability scans may include metering equipment, payment processing units, communication modules, and charge control systems. EVSE owners/operators may consider implementing a vulnerabilities management solution for continuous vulnerability assessment for all EVSE equipment on site's network. | **ISA/IEC 62443-2-1:D4E1**<br>ORG 2.2, EVENT 1.1 |
| **CM-8 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]**<br>RA-5<br>**[NIST-SP800-115]** |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **CM-8 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 2.2, EVENT 1.1 |

### 5.3.3. Detection Processes

Detection processes and procedures are maintained, tested, and updated to ensure awareness of anomalous events.

This category is common to all cyber ecosystems; however, the EV/XFC ecosystem is relatively new, and, therefore, additional consideration is warranted so that the most current best practices and processes may be embraced.

**Table 16.** Detect: Detection Processes Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **DP-1:** Roles and responsibilities for detection are well defined to ensure accountability. | **Ecosystem:** EV/XFC ecosystem members may consider having well-defined ecosystem-wide detection roles and responsibilities in addition to the domains' internal activities. This may include creating or updating roles and responsibilities to include or improve detection activities. Roles and responsibilities may include event detection, diagnosis, status communications, and response plan decisions or actions. | **[NIST-SP800-53r5]** CA-2, CA-7, PM-14 |
| **DP-1 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CA-2, CA-7 |
| **DP-1 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.3 |
| **DP-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CA-2, CA-7 |
| **DP-1 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.3 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **DP-2:**<br>Detection activities comply with all applicable requirements. | **Ecosystem:** Activities and requirements include (but are not limited to) policy, contractual, regulation, and legal requirements. | **[NIST-SP800-53r5]**<br>AC-1, AT-1, AU-1, CA-1, CA-2, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1 PE-1, PL-1, PM-1, PM-14, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SI-4, SR-1, SR-9, SR-10<br>**[NIST-SP800-61r2]**<br>**NERC CIP**<br>007-6-R4 |
| **DP-2 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]**<br>SI-1, SI-4, SR-1, SR-9, SR-10 |
| **DP-2 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>EVENT 1.1 |
| **DP-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]**<br>SI-1, SI-4, SR-1, SR-9, SR-10 |
| **DP-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>EVENT 1.1 |
| **DP-3:**<br>Detection processes are tested. | **Ecosystem:** Consider regular testing detection processes for accuracy, coverage, and completeness, or against known threats or vulnerabilities. Detection processes may be tested using audits and adversarial emulation activities. | **[NIST-SP800-53r5]**<br>CA-2, CA-7. PM-14, SI-3, SI-4<br>**NERC CIP**<br>006-6-R3 |
| **DP-3 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]**<br>CA-2, CA-7. PM-14, SI-3, SI-4 |
| **DP-3 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1**<br>EVENT 1.1<br>**ISA/IEC 62443-3-3:2013**<br>SR 3.3 |
| **DP-3 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]**<br>CA-2, CA-7. PM-14, SI-3, SI-4 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **DP-3 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.1<br>**ISA/IEC 62443-3-3:2013** SR 3.3 |
| **DP-4:**<br>Event detection information is communicated. | **Ecosystem:** Event information may include event origin, type, scale, effected systems, or consequences to delivered product and communicated to affected relevant parties. | **[NIST-SP800-53r5]** AU-6, CA-2, CA-7, RA-5, SI-4<br>**NERC CIP** 008-6-R4 |
| **DP-4 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** AU-6, CA-2, CA-7 |
| **DP-4 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.2<br>**ISA/IEC 62443-3-3:2013** SR 6.1 |
| **DP-4 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** AU-6, CA-2, CA-7 |
| **DP-4 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System specific considerations. | **ISA/IEC 62443-2-1:D4E1** EVENT 1.2<br>**ISA/IEC 62443-3-3:2013** SR 6.1 |
| **DP-5:**<br>Detection processes are continuously improved. | **Ecosystem:** These improvements may take the form of additional or increased tool use, activities, or Cyber Threat Intelligence use. | **[NIST-SP800-53r5]** CA-2, CA-7, PL-2, PM-14, RA-5, SI-4 |
| **DP-5 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CA-2, CA-7, PL-2, PM-14, RA-5 |
| **DP-5 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1 |
| **DP-5 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CA-2, CA-7, PL-2, PM-14, RA-5 |
| **DP-5 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **ISA/IEC 62443-2-1:D4E1** ORG 1.1 |

## 5.4. Respond Function Considerations Across the EV/XFC Domains

The activities in the Respond function support the ability to contain the impact of an incident by developing and implementing the appropriate responses to a detected cybersecurity attack or anomalous incident.

The Respond function actions are triggered by the outputs generated by the Detect function and the Protect function provides the ability to execute the proper response to an incident according to a pre-defined plan.

The objectives of the Response function are to:

- Contain events using a verified response procedure.
- Communicate the occurrence and impact of the incident to operations and relevant parties.
- Develop processes to respond to and mitigate new known or anticipated threats or vulnerabilities.
- Evolve response strategies and plans based on lessons learned.

### 5.4.1. Analysis

Analysis is conducted to verify the efficacy of the response and support recovery activities.

In the context of the EV/XFC ecosystem, the analysis should include the efficacy of IT and OT responses.

**Table 17.** Respond: Analysis Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AN-1:**<br>Notifications from detection systems are investigated. | **Ecosystem:** Investigations may include combining relevant notifications together, adding an initial detection system, or updating the notifications to investigate. Investigation should consider being used as a tool in system diagnosis, event/incident response and mitigations. | **[NIST-SP800-53r5]**<br>AU-6, CA-7, IR-4, IR-5, PE-6, RA-5, SI-4 |
| **AN-1 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]**<br>CA-7, IR-5, SI-4 |
| **AN-1 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]**<br>CA-7, IR-5, SI-4<br>**ISA/IEC 62443-2-1:D4E1**<br>ORG 1.1, EVENT 1.7, EVENT 1.8<br>**ISA/IEC 62443-3-3:2013**<br>SR 6.1 |
| **AN-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]**<br>CA-7, IR-5, SI-4 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AN-1 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** CA-7, IR-5, SI-4<br>**ISA/IEC 62443-2-1:D4E1** ORG 1.1, EVENT 1.7, EVENT 1.8<br>**ISA/IEC 62443-3-3:2013** SR 6.1 |
| **AN-2:** The impact of the incident is understood. | **Ecosystem:** In addition to the impacts to system availability, data protection and integrity, consider broader impacts such as loss of productivity, impact to external users/customers, damage to reputation, etc. | **[NIST-SP800-53r5]** CP-2, IR-4, RA-3<br>**[NIST-SP800-61r2]** 3 |
| **AN-2 \| EV** | Impacts to safety critical systems and components should consider being treated as high priority or understood in greater detail. | **[NIST-SP800-53r5]** CP-2, IR-4, RA-3<br>**[NIST-SP800-61r2]** 3.2.4 |
| **AN-2 \| XFC/EVSE** | Impacts to safety critical systems and components should consider being treated as high priority or understood in greater detail. | **[NIST-SP800-53r5]** CP-2, IR-4, RA-3<br>**[NIST-SP800-61r2]** 3.2.4<br>**ISA/IEC 62443-2-1:D4E1** ORG 1.1, EVENT 1.7 |
| **AN-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, RA-3 |
| **AN-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, RA-3<br>**ISA/IEC 62443-2-1:D4E1** ORG 1.1, EVENT 1.7 |
| **AN-3:** Forensics are performed. | **Ecosystem:** Forensics provide information that aids in selecting response actions and informs improvements for future response plans. | **[NIST-SP800-53r5]** AU-7, IR-4<br>**[NIST-SP800-61r2]** 2.4.2, 2.4.3, 3.1.1<br>**NERC CIP** 009-6-R1 |
| **AN-3 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 2.4.2, 2.4.3, 3.1.1 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AN-3 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 2.4.2, 2.4.3, 3.1.1<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.7<br>**ISA/IEC 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 |
| **AN-3 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-61r2]** 2.4.2, 2.4.3, 3.1.1 |
| **AN-3 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-61r2]** 2.4.2, 2.4.3, 3.1.1<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.7<br>**ISA/IEC 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 |
| **AN-4:** Incidents are categorized consistent with response plans. | **Ecosystem:** Categorizing incidents enables a more prompt initiation of response actions and may influence future risk management decisions. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-5, IR-8, RA-3<br>**[NIST-SP800-61r2]** 2, 3.2 |
| **AN-4 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** IR-4, IR-5, IR-8, RA-3<br>**[NIST-SP800-61r2]** 2 |
| **AN-4 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** IR-4, IR-5, IR-8, RA-3<br>**[NIST-SP800-61r2]** 2<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.7 |
| **AN-4 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** IR-4, IR-5, IR-8, RA-3<br>**[NIST-SP800-61r2]** 2 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AN-4 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** IR-4, IR-5, IR-8, RA-3<br>**[NIST-SP800-61r2]** 2<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.7 |
| **AN-5:**<br>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). | **Ecosystem:** EV/XFC ecosystem members can consider establishing processes to receive, analyze and respond to disclosed vulnerabilities from internal or external sources. Responses may include ensuring they are properly protected against the vulnerability and updating policy, practices, or guidance correspondingly. | **[NIST-SP800-53r5]** CA-1, CA-2, PM-4, PM-15, RA-1, RA-7, SI-5, SR-6<br>**[NIST-SP800-61r2]** 3, 3.2<br>**[NIST-SP800-160V1]** 3.4.9, 3.4.11<br>**DHS-NCCIC**<br>**NERC CIP** 007-6-R2 |
| **AN-5 \| EV** | Vulnerabilities impacting safety critical systems may be given higher priority or cause increased responses. Responses may include, but are not limited to, testing mitigation effectiveness, component recalls, and priority updates. | **[NIST-SP800-53r5]** CA-1, CA-2, RA-1, RA-7, SI-5, SR-6<br>**[NIST-SP800-61r2]** 3<br>**DHS-NCCIC**<br>**ISO/SAE 21434** RQ-08-01, RQ-08-03, RQ-08-05, RQ-08-07, RQ-08-08<br>**ISO 24089:20233** |
| **AN-5 \| XFC/EVSE** | Vulnerabilities impacting safety critical systems may be given higher priority or cause increased responses. Responses may include, but are not limited to, testing mitigation effectiveness, component recalls, and priority updates. | **[NIST-SP800-53r5]** CA-1, CA-2, RA-1, RA-7, SI-5, SR-6<br>**[NIST-SP800-61r2]** 3 |
| **AN-5 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CA-1, CA-2, RA-1, RA-7, SI-5, SR-6<br>**[NIST-SP800-61r2]** 3<br>**DHS-NCCIC** |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **AN-5 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** CA-1, CA-2, RA-1, RA-7, SI-5, SR-6<br>**[NIST-SP800-61r2]** 3<br>**DHS-NCCIC** |

### 5.4.2. Communications

Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).

Relative to other ecosystems, the EV/XFC ecosystem's response is likely to need more inter-organization communications to enable a coordinated response to incidents.

**Table 18.** Respond: Communications Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **CO-1:** Personnel know their roles and order of operations when a response is needed. | **Ecosystem:** The efficacy and timeliness of the response depends on how well responders understand the recovery time objectives and recovery point objectives, restoration priorities, task sequences, and other tasks in a manner that is consistent with the continuity plans. | **[NIST-SP800-34r1]**<br>**[NIST-SP800-53r5]** CP-2, CP-3, IR-3, IR-8<br>**[NIST-SP800-61r2]** Appendix A, 2.4<br>**NERC CIP** 009-6-R2 |
| **CO-1 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CP-3, IR-8<br>**[NIST-SP800-61r2]** Appendix A, 2.4 |
| **CO-1 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** CP-3, IR-8<br>**[NIST-SP800-61r2]** Appendix A, 2.4<br>**ISA/IEC 62443-2-1:D4E1** ORG 1.3, EVENT 1.8 |
| **CO-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CP-3, IR-8 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **CO-1 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-34r1]**<br>**[NIST-SP800-53r5]** CP-3, IR-8<br>**[NIST-SP800-61r2]** Appendix A<br>**ISA/IEC 62443-2-1:D4E1** ORG 1.3, EVENT 1.8 |
| **CO-2:**<br>Incidents are reported, consistent with established criteria. | **Ecosystem:** The reporting typically includes internal and the appropriate external relevant parties. Reporting can be done in a manner that is consistent with pre-defined thresholds and should consider initiating the response in a timely manner. | **[NIST-SP800-53r5]** AU-6, IR-6, IR-8<br>**[NIST-SP800-61r2]** 4<br>**NERC-CIP-008-6** |
| **CO-2 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** IR-6, IR-8<br>**NERC-CIP-008-6** |
| **CO-2 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** IR-6, IR-8<br>**NERC-CIP-008-6**<br>**ISA/IEC 62443-2-1:D4E1** ORG 1.1, EVENT 1.2 |
| **CO-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** IR-6, IR-8<br>**[NIST-SP800-61r2]** Appendix A |
| **CO-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System specific considerations. | **[NIST-SP800-53r5]** IR-6, IR-8<br>**[NIST-SP800-61r2]** Appendix A<br>**ISA/IEC 62443-2-1:D4E1** ORG 1.1, EVENT 1.2 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **CO-3:**<br>Consistent information is shared with response plans. | **Ecosystem:** The information shared may include the creation or updating of information sharing response plan actions and activities. Information may be shared with all effected entities, both internal and external, and may include information related to incident analysis, mitigation/recovery efforts and plans, or paths forward.<br>Organizations may coordinate with law enforcement and regulatory officials where applicable.<br>Consider sharing with industry groups, ISAC, or other consortia to increase cyber situational awareness. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**[NIST-SP800-61r2]** 2.4 |
| **CO-3 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4<br>**[NIST-SP800-61r2]** 2.4 |
| **CO-3 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4<br>**[NIST-SP800-61r2]** 2.4<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.2 |
| **CO-3 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4 |
| **CO-3 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.2 |
| **CO-4:**<br>Coordination with stakeholders occurs consistent with response plans. | **Ecosystem:** Consider defining the terms and conditions associated with the coordination in advance. Coordination may take the form of communications, plans, activities, or responsibilities. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**[NIST-SP800-61r2]** 2.3.4 |
| **CO-4 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-8<br>**[NIST-SP800-61r2]** 2.3.4 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **CO-4 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-8<br>**[NIST-SP800-61r2]** 2.3.4<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.2 |
| **CO-4 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-8<br>**[NIST-SP800-61r2]** 2.3.4 |
| **CO-4 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-8<br>**[NIST-SP800-61r2]** 2.3.4<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.2 |
| **CO-5:**<br>Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness. | **Ecosystem:** The domains are independent organizations that may impact other domains. Information sharing assists the domains by enabling proactive response actions, which benefits the whole ecosystem. This information may include cybersecurity risk positions or response actions. | **[NIST-SP800-53r5]** PM-15, PM-16, SI-5 |
| **CO-5 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** PM-15, PM-16, SI-5 |
| **CO-5 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** PM-15, PM-16, SI-5 |
| **CO-5 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** PM-15, PM-16, SI-5 |
| **CO-5 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** PM-15, PM-16, SI-5 |

### 5.4.3. Improvements Category

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

In the context of the EV/XFC ecosystem, the sharing of lessons learned between domains can result in ecosystem wide improvements.

**Table 19.** Respond: Improvements Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **IM-1:** Response plans incorporate lessons learned. | **Ecosystem:** Lessons learned may include past incidents, other industries responding to a similar incident, or from external information sources. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**[NIST-SP800-61r2]** 3.4.1 |
| **IM-1 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**[NIST-SP800-61r2]** 3.4.1 |
| **IM-1 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**[NIST-SP800-61r2]** 3.4.1<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.8 |
| **IM-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**[NIST-SP800-61r2]** 3.4.1 |
| **IM-1 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**[NIST-SP800-61r2]** 3.4.1<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.8 |
| **IM-2:** Response strategies are updated. | **Ecosystem:** Response strategies may include updating response plans periodically either around major events or an initial update. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8 |
| **IM-2 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**ISO/SAE 21434** RQ-08-07, RQ-08-08, RQ-13-01 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **IM-2 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.8 |
| **IM-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8 |
| **IM-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.8 |

### 5.4.4. Mitigation

Activities are performed to contain an event, mitigate its effects, and resolve the incident.

Mitigation is not unique to the EV/XFC ecosystem, and, like other ecosystems, timely mitigation will minimize the overall impact of the incident.

**Table 20.** Respond: Mitigation Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **MI-1:** Incidents are contained. | **Ecosystem:** Timely containment can minimize the impact of the incident and hastens the response and recovery. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 3.4.1 |
| **MI-1 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 3.3, 3.3.1 |
| **MI-1 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 3.3, 3.4.1<br>**ISA/IEC 62443-2-1:D4E1** NET 1.01, NET 1.04, NET 1.06, EVENT 1.8<br>**ISA/IEC 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **MI-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 3.3, 3.4.1 |
| **MI-1 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 3.3, 3.4.1<br>**ISA/IEC 62443-2-1:D4E1** NET 1.01, NET 1.04, NET 1.06, EVENT 1.8<br>**ISA/IEC 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 |
| **MI-2:**<br>Incidents are mitigated. | **Ecosystem:** Mitigation efforts may occur in response to newly learned cyber threat intelligence, in response to an incident, or as vulnerabilities become known, as part of an automated security tool/program, or in accordance with policies and contractual agreements. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 3.3.1 |
| **MI-2 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 3.3.1 |
| **MI-2 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 3.3.1<br>**ISA/IEC 62443-2-1:D4E1** NET 1.01, NET 1.05, NET 1.06, COMP 2.2 |
| **MI-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 3.3.1 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **MI-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 3.3.1<br>**ISA/IEC 62443-2-1:D4E1** NET 1.01, NET 1.05, NET 1.06, COMP 2.2 |
| **MI-3:**<br>Newly identified vulnerabilities are mitigated or documented as accepted risks. | **Ecosystem:** Vulnerabilities may be considered as general classes or types instead of treating each specific vulnerability separately. | **[NIST-SP800-53r5]** CA-2, CA-7, RA-3, RA-5, RA-7<br>**[NIST-SP800-61r2]** 3.4 |
| **MI-3 \| EV** | Vulnerabilities impacting safety-critical systems may be given higher priority or cause increased responses. Responses may include, but are not limited to, testing mitigation effectiveness, component recalls, priority updates. | **[NIST-SP800-53r5]** CA-2, RA-3, RA-5, RA-7<br>**[NIST-SP800-61r2]** 3.4<br>**ISO/SAE 21434** RQ-08-07, RQ-08-08, RQ-13-01<br>**ISO 24089:2021** |
| **MI-3 \| XFC/EVSE** | Vulnerabilities impacting critical systems may be given higher priority or cause increased responses. Responses may include, but are not limited to, testing mitigation effectiveness, component recalls, priority updates. | **[NIST-SP800-53r5]** CA-2, RA-3, RA-5, RA-7<br>**[NIST-SP800-61r2]** 3.4<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.9 |
| **MI-3 \| Cloud/Third-Party** | Applicable, but no Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CA-2, RA-3, RA-5, RA-7<br>**[NIST-SP800-61r2]** 3.4 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **MI-3 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** CA-2, RA-3, RA-5, RA-7<br>**[NIST-SP800-61r2]** 3.4<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.9 |

### 5.4.5. Response Planning

Response processes and procedures are executed and maintained after detected cybersecurity incidents.

Response processes and procedures are not unique to the EV/XFC ecosystem, and like other cyber-ecosystems, need to be pre-defined for a timely response to an incident and avoid ambiguities.

**Table 21.** Respond: Response Planning Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **RP-1:** Response plan is executed during or after an incident. | **Ecosystem:** The domains may consider executing response plans during or after an incident in accordance with the pre-defined threshold and document the steps and results of the response plan as it is being executed. | **[NIST-SP800-53r5]** CP-2, CP-10, IR-4, IR-8 |
| **RP-1 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CP-10, IR-4<br>**ISO 24089:2023** |
| **RP-1 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** CP-2, CP-10, IR-4 |
| **RP-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CP-10, IR-4 |
| **RP-1 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-34r1]**<br>**[NIST-SP800-53r5]** CP-2, CP-10, IR-4 |

## 5.5. Recover Function Considerations Across the EV/XFC Domains

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. The activities in the Recover function support timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this function include:

- Recovery Planning
- Improvements
- Communications

### 5.5.1. Communications

Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, internet service providers, owners of attacking systems, victims, other computer security incident response teams, and vendors).

The communications category is not unique to the EV/XFC ecosystem, and like other ecosystems, timely communications and coordinated restoration will lead to more timely recovery.

**Table 22.** Recover: Communications Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **CO-1:**<br>Public relations are managed. | **Ecosystem:** Management of public relations may include different recipients such as shareholders, partners, users, and the public. The message and communications may need to be tailored in accordance with the recipients' interests. Communication in this regard may include disclosure of the event/incident, recovery plans or activities, coordination with external partners or entities. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 4.1 |
| **CO-1 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 4.1 |
| **CO-1 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 4.1 |
| **CO-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 4.1 |
| **CO-1 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** IR-4<br>**[NIST-SP800-61r2]** 4.1 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **CO-2:** Reputation is repaired after an incident. | **Ecosystem:** This repair may take the form of public outreach, policy or activity reform, or coordination with external partners or entities. | **[NIST-SP800-53r5]** AU-6, IR-6, IR-8 **[NIST-SP800-61r2]** 4 **NERC-CIP-008-6** |
| **CO-2 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** AU-6, IR-6, IR-8 **[NIST-SP800-61r2]** 4 **NERC-CIP-008-6** |
| **CO-2 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** AU-6, IR-6, IR-8 **[NIST-SP800-61r2]** 4 **NERC-CIP-008-6** |
| **CO-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** AU-6, IR-6, IR-8 **[NIST-SP800-61r2]** 4 **NERC-CIP-008-6** |
| **CO-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** AU-6, IR-6, IR-8 **[NIST-SP800-61r2]** 4 **NERC-CIP-008-6** |
| **CO-3:** Recovery activities are communicated to internal and external stakeholders as well as executive and management teams. | **Ecosystem:** Communications may consist of recovery timelines, future mitigation/prevention strategies, and incident or root-cause analysis. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8 **[NIST-SP800-61r2]** 3.4 **NERC CIP** 009-6-R3 |
| **CO-3 \| EV** | Applicable, but no EV-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8 **[NIST-SP800-61r2]** 3.4 |
| **CO-3 \| XFC/EVSE** | Applicable, but no EVSE-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8 **[NIST-SP800-61r2]** 3.4 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **CO-3 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**[NIST-SP800-61r2]** 3.4 |
| **CO-3 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**[NIST-SP800-61r2]** 3.4 |

### 5.5.2. Improvements

Recovery planning and processes are improved by incorporating lessons learned into future activities.

In the context of the EV/XFC ecosystem, sharing lessons learned between domains can result in ecosystem wide improvements.

**Table 23.** Recover: Improvements Category.

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **IM-1:** Recovery plans incorporate lessons learned. | **Ecosystem:** Updated recovery plans may include updated, new, or increased activities to reduce the likelihood of the event occurring. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**[NIST-SP800-61r2]** 3.4.1<br>**NERC CIP** 009-6-R3 |
| **IM-1 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4<br>**[NIST-SP800-61r2]** 3.4.1<br>**ISO/SAE 21434** RG-05-08 |
| **IM-1 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4<br>**[NIST-SP800-61r2]** 3.4.1<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.8, AVAIL 1.1 |

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **IM-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4<br>**[NIST-SP800-61r2]** 3.4.1 |
| **IM-1 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4<br>**[NIST-SP800-61r2]** 3.4.1<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.8, AVAIL 1.1 |
| **IM-2:** Recovery strategies are updated. | **Ecosystem:** Updates to the strategy may include updating response plans periodically, around major events, or an initial update. | **[NIST-SP800-53r5]** CP-2, IR-4, IR-8<br>**[NIST-SP800-61r2]** 3.4, 3.4.1 |
| **IM-2 \| EV** | Applicable, but no additional EV-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4<br>**[NIST-SP800-61r2]** 3.4.1 |
| **IM-2 \| XFC/EVSE** | Applicable, but no additional EVSE-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4<br>**[NIST-SP800-61r2]** 3.4.1<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.8, AVAIL 1.1 |
| **IM-2 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4<br>**[NIST-SP800-61r2]** 3.4.1 |
| **IM-2 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-53r5]** CP-2, IR-4<br>**[NIST-SP800-61r2]** 3.4.1<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.8, AVAIL 1.1 |

### 5.5.3. Recovery Planning

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

Recovery processes and procedures are not unique to the EV/XFC ecosystem, but the prioritization of recovery operations may be informed by the impact of the assets to other domains.

**Table 24.** Recover: Recovery Planning Category

| Subcategory \| Domain | Specific Considerations | Informative References |
|---|---|---|
| **RP-1:**<br>Recovery plan is executed during or after an incident. | **Ecosystem:** A recovery plan may include an evaluation and updating processes to the recovery plan. | **[NIST-SP800-34r1]**<br>**[NIST-SP800-53r5]** CP-10, IR-4, IR-8<br>**[NIST-SP800-160V1]** 3.4.11, Appendix F.2.6<br>**[NIST-SP800-184]**<br>**NERC CIP** 009-6-R1, 009-6-R2 |
| **RP-1 \| EV** | Recovery plans may potentially include proliferation of any software, hardware and policy updates, mitigation implementations, or recalls to all affected EV production centers and individual EVs. | **[NIST-SP800-53r5]** IR-4, IR-8<br>**[NIST-SP800-184]**<br>**ISO/SAE 21434** RQ-13-01, RQ-13-02 |
| **RP-1 \| XFC/EVSE** | Consider having recovery plans include proliferation of any software, hardware and policy updates, mitigation implementations, or recalls to all affected EVSE production centers and individual EVSE devices. | **[NIST-SP800-53r5]** IR-4, IR-8<br>**[NIST-SP800-184]**<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.8 |
| **RP-1 \| Cloud/Third-Party** | Applicable, but no additional Cloud/Third-Party-specific considerations. | **[NIST-SP800-53r5]** IR-4, IR-8<br>**[NIST-SP800-184]** |
| **RP-1 \| Utility/Building Management System** | Applicable, but no additional Utility/Building Management System-specific considerations. | **[NIST-SP800-34r1]**<br>**[NIST-SP800-53r5]** IR-4, IR-8<br>**[NIST-SP800-184]**<br>**ISA/IEC 62443-2-1:D4E1** EVENT 1.8 |

## References

[ATIS-I-0000070] Alliance for Telecommunications Industry Solutions (2018) *Context-Aware Identity Management Framework,* ATIS-I-0000070 (ATIS, Washington, DC). Available at https://access.atis.org/apps/group_public/download.php/43565/ATIS-I0000070.pdf

[Auto-ISAC] Automotive Information Sharing and Analysis Center. Available at: https://automotiveisac.com/

[CISA-CIVR-PB] Cybersecurity and Infrastructure Security Agency (2021) Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems. (CISA, Washington, DC). Available at https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

[CISA-ICS] Cybersecurity and Infrastructure Security Agency (2020) *Industrial Control Systems.* (CISA, Washington, DC). Available at https://us-cert.cisa.gov/ics

[CISA-RFI-BPG] Cybersecurity and Infrastructure Security Agency and SAFECOM/National Council of Statewide Interoperability Coordinators (2020) Radio Frequency Interference Best Practices Guidebook. (CISA, Washington, DC). Available at https://www.cisa.gov/sites/default/files/publications/safecom-ncswic_rf_interference_best_practices_guidebook_2.7.20_-_final_508c.pdf

[DHS-NCCIC] Department of Homeland Security (2012) National Cybersecurity & Communications Integration Center (NCCIC) Overview. (DHS, Washington, DC). Available at https://csrc.nist.gov/CSRC/media/Events/ISPAB-OCTOBER-2012MEETING/documents/ispab_oct2012_lzelvin_nccic-overview.pdf

[EEI-2022] Scruggs T (2022) “EEI Projects 26.4 Million Electric Vehicles Will Be on U.S. Roads in 2030”. Edison Electric Institute. June 20, 2022. Available at: https://www.eei.org/News/news/All/eei-projects-26-million-electric-vehicles-will-be-on-us-roads-in-2030

[E-ISAC] Electricity information Sharing and Analysis Center. Available at: https://www.eisac.com/s/

[EO.13636] The White House, Office of the Press Secretary. “Executive Order -- Improving Critical Infrastructure Cybersecurity”. February 12, 2013. Available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[Energies-2019] Ronanki, D, Kelkar, A, Williamson, S. "Extreme Fast Charging Technology—Prospects to Enhance Sustainable Electric Transportation". Energies 2019,12, 3721. https://doi.org/10.3390/en12193721

[EPRI-2023] Cybersecurity Platform and Certification Framework Development for Extreme Fast Charging (XFC)-Integrated Charging Ecosystem. EPRI, Palo Alto, CA: 2023. 3002027649. Available at: https://www.epri.com/research/products/000000003002027649

[Grandview] Grand View Research. "U.S. Electric Vehicle (EV) Charging Infrastructure Market Size, Share & Trends Analysis Report By Charger Type, By Connector Type, By Level of Charging, By Connectivity, By Application, And Segment Forecasts, 2023 – 2030" Report ID: GVR-3-68038-309-6. Available at: https://www.grandviewresearch.com/industry-analysis/us-electric-vehicle-charging-infrastructure-evci-market

[IEC 61850-90-4] International Electrotechnical Commission (2020) *IEC TR 61850-90-4:2020 Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines* (IEC, Geneva, Switzerland). Available at https://webstore.iec.ch/publication/64801

[IEC61850-90-12] International Electrotechnical Commission (2020) *IEC TR 61850-90-12:2020 Communication networks and systems for power utility automation - Part 90-12: Wide area network engineering guidelines.* (IEC, Geneva, Switzerland). Available at https://webstore.iec.ch/publication/63706

[IEC62439-3] International Electrotechnical Commission (2021) *IEC 62439-3 Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR).* (IEC, Geneva, Switzerland). Available at https://webstore.iec.ch/publication/64423

[IEC62443-2-1] International Electrotechnical Commission (2010) *IEC 62443-2-1:2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program.* (IEC, Geneva, Switzerland). Available at https://webstore.iec.ch/publication/7030

[IEC62443-3-3] International Electrotechnical Commission (2013) *IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels.* (IEC, Geneva, Switzerland). Available at https://webstore.iec.ch/publication/7033

[IETF-RFC4082] Perrig A, Song D, Canetti R, Tygar JD, Briscoe B (2005) Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction. (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 4082. https://doi.org/10.17487/RFC4082

[ISO 24089] International Organizations for Standardization. (2023). Road vehicles-

*Software update engineering.* (24089:2023). Available at https://www.iso.org/standard/77796.html

[ISO-SAE-21434] International Organizations for Standardization/SAE. (2021). *Road vehicles — Cybersecurity engineering.*(21434:2021). Available at https://www.iso.org/obp/ui/en/#iso:std:iso-sae:21434:ed-1:v1:en

[Johnson-Berg] Johnson J, Berg T, Anderson B, Wright, B. (2022). Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses. Energies. 15. 3931. https://doi.org/10.3390/en15113931.

[NERC-CIP-008-6] North American Electric Reliability Corporation (2020) *CIP-008-6 – Cyber Security – Incident Reporting and Response Planning.* Available at https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf

[NERC-GridEx] North American Electric Reliability Corporation (2020) *GridEx.* Available at https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx

[NIST-CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[NIST-IR7298] Paulsen C, Byers R. (2022). *Glossary of Key Information Security Terms.* Available at: https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/final

[NIST-IR7800] Waltermire D, Halbardier A, Humenansky A, Mell P (2012) Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7800 (Draft). Available at https://csrc.nist.gov/CSRC/media/Publications/nistir/7800/draft/documents/Draft-NISTIR-7800.pdf

[NIST-IR8014] Hastings NE, Franklin JM (2015) Considerations for Identity Management in Public Safety Mobile Networks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8014. https://doi.org/10.6028/NIST.IR.8014

[NIST-IR8179] Paulsen C, Boyens JM, Bartol N, Winkler K (2018) Criticality Analysis Process Model: Prioritizing Systems and Components. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8179. https://doi.org/10.6028/NIST.IR.8179

[NIST-IR8320] Bartock M, Souppaya M, Savino R, Knoll T, Shetty U, Cherfaoui M, Yeluri R, Malhotra A, Banks D, Jordan M, Pendarakis D, Rao JR, Romness P, Scarfone K (2022) Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases. (National Institute of Standards and Technology,

Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8320. https://doi.org/10.6028/NIST.IR.8320

[NIST-SP1271] NIST SP 1271, Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide. https://doi.org/10.6028/NIST.SP.1271

[NIST-SP800-30r1] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[NIST-SP800-34r1] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1

[NIST-SP800-37r2] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[NIST-SP800-53r5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[NIST-SP800-61r2] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

[NIST-SP800-92] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-92. https://doi.org/10.6028/NIST.SP.800-92

[NIST-SP800-115] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. https://doi.org/10.6028/NIST.SP.800-115

[NIST-SP800-128] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128, Includes updates as of October 10, 2019. https://doi.org/10.6028/NIST.SP.800-128

[NIST-SP800-137] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security

Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-137

[NIST-SP800-150] Johnson CS, Waltermire DA, Badger ML, Skorupka C, Snyder J (2016) Guide to Cyber Threat Information Sharing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-150. https://doi.org/10.6028/NIST.SP.800-150

[NIST-SP800-154] Souppaya M, Scarfone K (2016) Guide to Data-Centric System Threat Modeling. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-154 (Draft). Available at https://csrc.nist.gov/publications/detail/sp/800-154/draft

[NIST-SP800-160V1] Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[NIST-SP800-161] Boyens J, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. http://doi.org/10.6028/NIST.SP.800-161

[NIST-SP800-175Br1] Barker EB (2020) Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-175B, Rev. 1. https://doi.org/10.6028/NIST.SP.800-175Br1

[NIST-SP800-184] Bartock MJ, Scarfone KA, Smith MC, Witte GA, Cichonski JA, Souppaya MP (2016) Guide for Cybersecurity Event Recovery. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-184. https://doi.org/10.6028/NIST.SP.800-184

[NIST-SP800-193] Regenscheid AR (2018) Platform Firmware Resiliency Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-193. https://doi.org/10.6028/NIST.SP.800-193

[NIST-SP800-209] Chandramouli R, Pinhas D (2020) Security Guidelines for Storage Infrastructure. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-209. https://doi.org/10.6028/NIST.SP.800-209

[NIST-SP800-218] Souppaya M, Scarfone K, Dodson D (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for

Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-218. https://doi.org/10.6028/NIST.SP.800-218

[NIST-SP1800-19] Bartock M, Souppaya M, Dodson D, Carroll D, Masten R, Scinta G, Massis P, Prafullchandra H, Malnar J, Singh H, Ghandi R, Storey L, Yeluri R, Shea T, Dalton M, Weber R, Scarfone K, Phoenix C, Dukes A, Haskins J, Swarts B (2022) Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-19. Available at https://doi.org/10.6028/NIST.SP.1800-19

[NIST-SP1800-34] Diamond T, Grayson N, Polk W, Regenscheid A, Souppaya M, Brown C, Deane C, Scarfone K (2022) Validating the Integrity of Computing Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-34 (Final). Available at https://doi.org/10.6028/NIST.SP.1800-34

[RTCA-DO-235] Radio Technical Commission for Aeronautics (2008) *RTCA DO-235A Assessment of Radio Frequency Interference Relevant to the GNSS L1 Frequency Band.* (RTCA, Washington, DC). Available at https://standards.globalspec.com/std/1090607/RTCA%20DO-235

[S.1353] S.1353 - 113th Congress (2013-2014): Cybersecurity Enhancement Act of 2014, S.1353, 113th Cong. (2014), https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

# Appendix A. List of Symbols, Abbreviations, and Acronyms

**AAR**
After Action Report

**AC**
Alternating Current

**API**
Application Programming Interface

**AUTO-ISAC**
Automotive Information Sharing and Analysis Center

**BESS**
Battery Energy Storage System

**BMS**
Battery Management System

**CAN**
Control Area Network

**CD**
Compact Disc

**COI**
Community of Interest

**COTS**
Commercial Off the Shelf

**CRC**
Cyclic Redundancy Check

**CSF**
Cybersecurity Framework

**CTI**
Cyber Threat Intelligence

**CVE**
Common Vulnerabilities and Exposures

**CVSS**
Common Vulnerability Scoring System

**CWE**
Common Weakness Enumeration

**DAR**
Data-At-Rest

**DC**
Direct Current

**DE**
Detect

**DER**
Distributed Energy Resources

**DIT**
Data-In-Transit

**DOE**
Department of Energy

**DVD**
Digital Versatile Disc

**E-ISAC**
Electricity Information Sharing and Analysis Center

**ECU**
Electronic Control Unit

**EO**
Executive Order

**EPRI**
Electric Power Research Institute

**EV**
Electric Vehicle

**EVSE**
Electric Vehicle Supply Equipment

**EVTOLS**
Electric Vehicle Take-Off and Landing

**FERC**
Federal Energy Regulatory Commission

**HMI**
Human-Machine Interface

**ICS**
Industrial Control System

**ID**
Identify / Identity

**IIOT**
Industrial Internet of Things

**IOT**
Internet of Things

**IT**
Information Technology

**IEC**
International Electrotechnical Commission

**ISAC**
Information Sharing and Analysis Center

**ISO**
International Organization for Standardization

**MOU**
Memorandum of Understanding

**MFA**
Multi-Factor Authentication

**NERC**
North American Electric Reliability Corporation

**NFC**
Near Field Communication

**NIST**
National Institute of Standards and Technology

**NVD**
National Vulnerability Database

**OBD-II**
On-Board Diagnostic II

**OCPI**
Open Charge Point Interface

**OCPP**
Open Charge Point Protocol

**OEM**
Original Equipment Manufacturer

**OT**
Operational Technology

**OTA**
Over the Air

**PCI**
Payment Card Industry

**PII**
Personally Identifiable Information

**PIN**
Personal Identification Number

**PLC**
Programmable Logic Controller

**PR**
Protect

**RBAC**
Role Based Access Control

**RC**
Recover

**RF**
Radio Frequency

**RS**
Respond

**SBOM**
Software Bill of Material

**SDLC**
Software Development Lifecycle

**SCADA**
Supervisory Control and Data Acquisition

**SCRM**
Supply Chain Risk Management

**SD**
Secure Digital

**SLA**
Service Level Agreement

**TTP**
Tactics, Techniques, and Procedures

**TTX**
Tabletop Exercise

**V2G**
Vehicle-To-Grid

**XFC**
Extreme Fast Charging