



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

**NIST Interagency Report
NIST IR 8473 ipd**

**Cybersecurity Framework Profile
for Electric Vehicle Extreme Fast
Charging Infrastructure**

Initial Public Draft

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

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

21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39

**NIST Interagency Report
NIST IR 8473 ipd**

**Cybersecurity Framework Profile
for Electric Vehicle Extreme Fast
Charging Infrastructure**

Initial Public Draft

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

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

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

July 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

40 Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in
41 this paper in order to specify the experimental procedure adequately. Such identification does not imply
42 recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or
43 equipment identified are necessarily the best available for the purpose.

44 There may be references in this publication to other publications currently under development by NIST in
45 accordance with its assigned statutory responsibilities. The information in this publication, including concepts and
46 methodologies, may be used by federal agencies even before the completion of such companion publications. Thus,
47 until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain
48 operative. For planning and transition purposes, federal agencies may wish to closely follow the development of
49 these new publications by NIST.

50 Organizations are encouraged to review all draft publications during public comment periods and provide feedback
51 to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at
52 <https://csrc.nist.gov/publications>.

53 **NIST Technical Series Policies**

54 [Copyright, Use, and Licensing Statements](#)

55 [NIST Technical Series Publication Identifier Syntax](#)

56 **How to Cite this NIST Technical Series Publication:**

57 McCarthy J, et al. (2023) Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging
58 Infrastructure (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR)
59 8473 ipd. <https://doi.org/10.6028/NIST.IR.8473.ipd>

60 **Author ORCID iDs**

61 Jim McCarthy: 0000-0002-5559-733X

62 Nakia Grayson: 0000-0000-0000-0000

63 Michael Thompson: 0000-0002-0836-244X

64 John Dombrowski: 0000-0002-9408-1838

65 **Public Comment Period**

66 July 14, 2023 - August 28, 2023

67 **Submit Comments**

68 evxfc-nccoe@nist.gov

69 National Institute of Standards and Technology

70 Attn: Applied Cybersecurity Division, Information Technology Laboratory

71 100 Bureau Drive (Mail Stop 2002) Gaithersburg, MD 20899-2002

72 **All comments are subject to release under the Freedom of Information Act (FOIA).**

73 **Abstract**

74 This document is the Cybersecurity Framework Profile (Profile) developed for the Electric
75 Vehicle Extreme Fast Charging (EV/XFC) ecosystem and the subsidiary functions that support
76 each of the four domains: (i) Electric Vehicles (EV); (ii) Extreme Fast Charging (XFC); (iii)
77 XFC Cloud or Third-Party Operations; (iv) and Utility and Building Networks. This Profile
78 provides a foundational profile that relevant parties may use to develop profiles specific to their
79 organization to assess their cybersecurity posture as a part of their risk management process. The
80 profile is intended to supplement, not replace, an existing risk management program or the
81 current cybersecurity standards, regulations, and industry guidelines that are in current use by the
82 EV/XFC industry.

83 **Keywords**

84 Cybersecurity Framework; electric vehicle, EV/XFC ecosystem; extreme fast charging;
85 Framework; Mission Objectives; Profile; risk management; security controls.

86 **Reports on Computer Systems Technology**

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

95 **Acknowledgements**

96 A complete list of contributors and acknowledgements will be released with the final version of
97 this document.

98 **Call for Patent Claims**

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

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

- 107 a) assurance in the form of a general disclaimer to the effect that such party does not hold
108 and does not currently intend holding any essential patent claim(s); or
- 109 b) assurance that a license to such essential patent claim(s) will be made available to
110 applicants desiring to utilize the license for the purpose of complying with the guidance
111 or requirements in this ITL draft publication either:
 - 112 i. under reasonable terms and conditions that are demonstrably free of any unfair
113 discrimination; or
 - 114 ii. without compensation and under reasonable terms and conditions that are
115 demonstrably free of any unfair discrimination.

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

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

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

124	Table of Contents	
125	1. Introduction	1
126	1.1. Purpose	2
127	1.2. Scope	2
128	1.3. Audience	4
129	2. Intended Use	5
130	3. EV/XFC Cybersecurity Mission Objectives	5
131	3.1. Mission Objective 1: Deliver Reliable Performance through Secure Communications.	6
132	3.2. Mission Objective 2: Maintain Resilience of the XFC Infrastructure	6
133	3.3. Mission Objective 3: Build and Maintain Trustworthy Relationships with Partners	
134	and Customers.....	7
135	3.4. Mission Objective 4: Maintain Continuity of Operations.....	8
136	4. Overview of the Cybersecurity Framework	8
137	4.1. The Framework Core	9
138	4.2. Sector-Level Profiles.....	11
139	5. XFC Baseline Profile	11
140	5.1. Identify Function.....	11
141	5.1.1. Asset Management Category	12
142	5.1.2. Business Environment Category	18
143	5.1.3. Governance Category.....	22
144	5.1.4. Risk Assessment Category.....	25
145	5.1.5. Risk Management Category	28
146	5.1.6. Supply Chain Risk Management Category	30
147	5.2. Protect Function Considerations Across the EV/XFC Domains	33
148	5.2.1. Identity Management, Authentication and Access Control Category	33
149	5.2.2. Awareness and Training Category	39
150	5.2.3. Data Security Category.....	42
151	5.2.4. Information Protection and Processes Category.....	48
152	5.2.5. Maintenance Category.....	56
153	5.2.6. Protective Technology Category	57
154	5.3. Detect Function Considerations Across the EV/XFC Domains	62
155	5.3.1. Anomalies and Events	62
156	5.3.2. Security Continuous Monitoring.....	65
157	5.3.3. Detection Processes.....	70
158	5.4. Respond Function Considerations Across the EV/XFC Domains	72
159	5.4.1. Analysis.....	73

160	5.4.2.	Communications	76
161	5.4.3.	Improvements Category	80
162	5.4.4.	Mitigation	81
163	5.4.5.	Response Planning	83
164	5.5.	Recover Function Considerations Across the EV/XFC Domains	84
165	5.5.1.	Communications	84
166	5.5.2.	Improvements	86
167	5.5.3.	Recovery Planning	88
168		References	90
169		Appendix A. List of Symbols, Abbreviations, and Acronyms	96

170 List of Tables

171	Table 1.	Function and Category Unique Identifiers	10
172	Table 2.	Identify: Asset Management Category	13
173	Table 3.	Identify: Business Environment Category	18
174	Table 4.	Identify: Governance Category	22
175	Table 5.	Identify: Risk Assessment Category	25
176	Table 6.	Identify: Risk Management Category	28
177	Table 7.	Identify: Supply Chain Risk Management Category	30
178	Table 8.	Protect: Identity Management, Authentication and Access Control	34
179	Table 9.	Protect: Awareness and Training Category	39
180	Table 10.	Protect: Data Security Category	42
181	Table 11.	Protect: Information Protection Processes and Procedures Category	49
182	Table 12.	Protect: Maintenance Category	56
183	Table 13.	Protect: Protective Technology Category	58
184	Table 14.	Detect: Anomalies and Events Category	63
185	Table 15.	Detect: Security Continuous Monitoring Category	65
186	Table 16.	Detect: Detection Processes Category	70
187	Table 17.	Respond: Analysis Category	73
188	Table 18.	Respond: Communications Category	77
189	Table 19.	Respond: Improvements Category	80
190	Table 20.	Respond: Mitigation Category	81
191	Table 21.	Respond: Response Planning Category	83
192	Table 22.	Recover: Communications Category	84
193	Table 23.	Recover: Improvements Category	87
194	Table 24.	Recover: Recovery Planning Category	88

195 List of Figures

196	Fig. 1.	Charging an EV.	2
197	Fig. 2.	EV/XFC Ecosystem Domains and Profile Scope.	4

198 **1. Introduction**

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

213 Currently, there are approximately 2M electric vehicles (EV) in operation, and the number of EV
214 is projected to be 24.6M by 2030 [\[EEI-2022\]](#). The EV infrastructure was prominently integrated
215 into the Infrastructure Investment and Jobs Act and is also expected to grow. As of 2023, there
216 were over 48,000 public charging stations in the US, and a commitment by the Infrastructure
217 Investment and Jobs Act is in place to increase this number to 500,000 by 2030. The U.S. EV
218 charging infrastructure market size was valued at \$3.15B in 2022 and is expected to grow to
219 \$24B by 2030. [\[Grandview\]](#)

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

226 This document is the result of that effort. The Cybersecurity Framework Profile for Extreme Fast
227 Charging (XFC) Infrastructure (referred to herein as the EV/XFC Cybersecurity Profile) is a
228 sector level profile. The EV/XFC Cybersecurity Profile is an application of the Framework
229 Categories and Subcategories in the context of the EV/XFC cybersecurity ecosystem as provided
230 by the DOE and EPRI. The EV/XFC Cybersecurity Profile provides ecosystem-relevant parties a
231 means to assess and communicate their cybersecurity posture in a manner consistent with the
232 Cybersecurity Framework. The EV/XFC Cybersecurity Profile provides users with an industry
233 level risk-based approach for managing cybersecurity activities and facilitates cross-
234 collaboration between the various industry relevant parties, vendors, and end users.



Fig. 1. Charging an EV.

235

236 1.1. Purpose

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

242 Use of the Profile will help organizations:

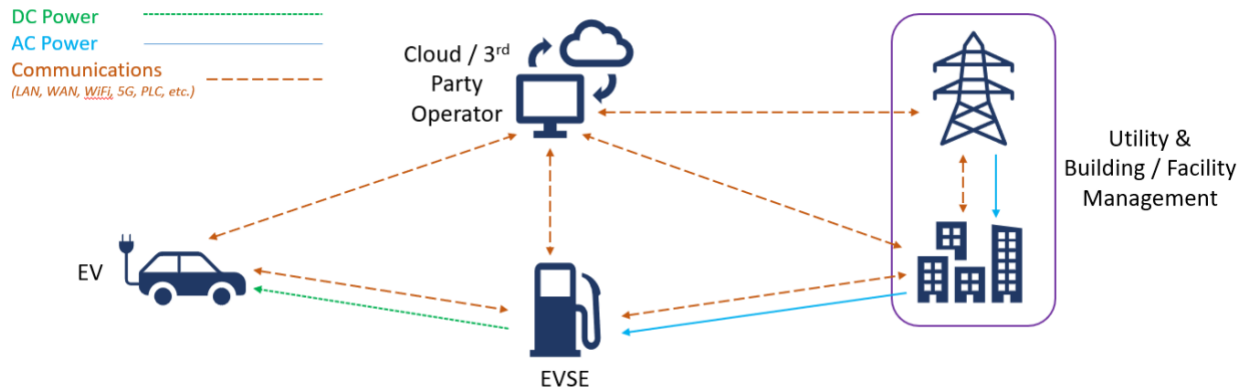
- 243 • Identify key assets and interfaces in each of the ecosystem domains.
- 244 • Address cybersecurity risk in the management and use of EV/XFC services.
- 245 • Identify the threats, vulnerabilities, and associated risks to EV/XFC services, equipment,
246 and data.
- 247 • Apply protection mechanisms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

251 1.2. Scope

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

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

- 260 through a physical connector. The vehicle communicates with vendor cloud/third-party
261 organizations via Bluetooth, wi-fi, or cellular.
- 262 • **XFC/EVSE.** Electric Vehicle Supply Equipment (EVSE) are systems that provide
263 electric power to the vehicle to recharge the vehicle’s batteries. EVSE systems include
264 electrical conductors, related equipment such as Battery Energy Storage Systems (BESS),
265 software, and communications protocols that deliver energy efficiently and safely to the
266 vehicle. Extreme Fast Charging (XFC) is a type of EVSE that is capable of recharging
267 vehicles in a manner of minutes rather than hours. [\[Energies-2019\]](#) In addition to
268 connecting to the EV, the XFC/EVSE and related equipment must connect and
269 communicate with cloud providers and third-party vendors for providing EVSE location
270 information, billing, and other services.
 - 271 • **Cloud/Third-Party Organizations.** The EV/XFC ecosystem consists of independently
272 owned and operated domains, and most charging stations are operated by a charging
273 network with business models that blend station, electricity, and vehicle charging sales
274 together. Third parties are individuals or entities that facilitate transactions but are not
275 one of the primary parties within the exchange. The EV/XFC ecosystem typically uses
276 cloud service providers for these transactions because they are suitable for sensitive data
277 exchanges that involve financial information, personally identifiable information, and
278 other potentially sensitive data.
 - 279 • **Utilities/Building Systems.** Utilities provide the power necessary to fuel the EV/XFC
280 ecosystem. Building and facility management systems may be present in installations
281 where energy management is required, such as EVSE installed at shopping centers, as
282 well as where distributed energy resources (DER) may be present or where physical
283 security control is required. Both utilities and building/facility management systems
284 include equipment to monitor power utilization, communicate with networked devices
285 and supervisory systems, and help control on-site energy demands.
- 286 The scope of cybersecurity and enterprise risk management includes operational technology
287 (OT) in addition to information technology (IT). While managing cybersecurity risks is equally
288 important to IT and OT processes, there are considerable operational differences between the
289 two, which may impact the implementation of risk management techniques for IT vs OT.
290 Despite these differences, the interdependencies between IT and OT are increasing which leads
291 to increasing reliance of OT on IT processes and possibly inherited vulnerabilities and risks
292 between the two technologies.
- 293 The EV/XFC ecosystem has always relied on a combination of IT and OT processes. Integrated
294 risk management includes a collaboration of IT and OT professionals to generate integrated
295 assessments, mitigations, and recovery plans.
- 296 The foundational concepts used to define the EV/XFC Cybersecurity Profile’s scope were
297 derived from previous research and documentation developed by the Electric Power Research
298 Institute (EPRI) [\[EPRI-2023\]](#) as illustrated in Fig. 2 below. Power generation and
299 communications within the utility is outside the scope of the EV/XFC Cybersecurity Profile.



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

301 **1.3. Audience**

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

- 305 • EV owners (including individuals in the general public and fleet owners)
- 306 • EV manufacturers
- 307 • EVSE owners/operators
- 308 • EVSE manufacturers
- 309 • Cloud/third-party providers
- 310 • Utility owner/operators
- 311 • Building Network Owners/Providers
- 312 • Suppliers/Vendors

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

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

323 The EV/XFC Cybersecurity Profile is intended for a general audience and is broadly applicable.

324 The Profile applies to organizations that:

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

330 **2. Intended Use**

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

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

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

354 **3. EV/XFC Cybersecurity Mission Objectives**

355 The EV/XFC Cybersecurity Mission Objectives (MOs) provide the context for an organization to
356 manage its cybersecurity risk as it relates to its specific mission needs. The following MOs can
357 serve as a starting point for a particular organization to define their own cybersecurity MOs.

358 **3.1. Mission Objective 1: Deliver Reliable Performance through Secure**
359 **Communications**

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

367 The rationale for this Mission Objective includes:

- 368 • **EV.** Communication between the EV (battery management system) and the charging
369 station is necessary to facilitate the EV battery charging process. The EV connects to
370 cloud/third-party applications to manage the transactions and collect data. EV user
371 systems (e.g., infotainment) also may communicate with other vehicle systems, such as
372 the charge controller and battery management systems. The interface between these
373 applications presents a potential attack surface for malicious actors to cause damage.
- 374 • **XFC/EVSE.** The charging station requires secure communication to the cloud to
375 facilitate financial transactions, provide authorization to charge, collect maintenance logs,
376 and receive updates. Additionally, the charging station draws power from the metered
377 utility.
- 378 • **Cloud/Third-Party.** Cloud service providers require reliable secure connections to the
379 EV, charging station, and the utility to facilitate the charging process. Secure reliable
380 communications allow for validation of financial transactions, protect personal
381 information, and allow for maintenance updates and logs to be transmitted quickly and
382 economically.
- 383 • **Utility/Building Management Systems.** Utilities provide power to the charging station.
384 Coordination between the XFC chargers and utilities are required for various smart grid
385 applications such as peak shaving/load shifting or forecasting. Where this communication
386 exists, it must be reliable and secure.

387 **3.2. Mission Objective 2: Maintain Resilience of the XFC Infrastructure**

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

393 The rationale for this Mission Objective includes:

- 394 • **EV.** EV owners want assurance that their vehicle is protected before they are willing to
395 participate in the charging ecosystem. Batteries are a significant expense, and a
396 compromised XFC ecosystem could potentially lead to physical damage to the battery,

397 EV components, and other nearby equipment. Thus, implemented safeguards will ease
398 the minds of users and encourage them to use the charging stations.

399 • **XFC/EVSE.** Due to the unique position of charging stations in the ecosystem, its
400 geographical dispersion, and its general lack of physical security, charging stations have
401 become an appealing target for threat actors. EVSE infrastructures should be protected,
402 both cyber and physical, to prevent attacks like ransomware or damage to the charging
403 infrastructure itself.

404 • **Cloud/Third-Party.** The cloud/third-party environment facilitates connectivity between
405 domains of the infrastructure. It should be protected to maintain operations.

406 • **Utility/Building Management Systems.** Utilities should have protection systems in
407 place to prevent manipulation of utility components to maintain safe operations.

408 **3.3. Mission Objective 3: Build and Maintain Trustworthy Relationships with** 409 **Partners and Customers**

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

419 The rationale for this mission objective includes:

420 • **EV.** EV owners trust that charging stations will be available and operable, will not be
421 damaged while charging, and will protect their information during transactions.

422 • **XFC/EVSE.** EVSEs are the most visible representation of the EV/XFC ecosystem, and a
423 cyber incident can have broad impact leaving the public uncertain of the safety and
424 reliability of EVs, potentially impacting future sales.

425 • **Cloud/Third-Party.** Cloud and third-party providers capture and maintain sensitive
426 financial information for transactions across the EV/XFC ecosystem. Inadvertent release
427 of this sensitive information can result in a loss of trust from all ecosystem relevant
428 parties as well as result in high costs to the cloud/third-party providers due to fines, civil
429 lawsuits, or compensation to customers.

430 • **Utility/Building Management Systems.** Disruptions in the power supply may leave EV
431 owners stranded and others in the EV/XFC ecosystem unable to perform their business
432 functions. These types of disruptions erode trust in the EV/XFC ecosystem.

433 **3.4. Mission Objective 4: Maintain Continuity of Operations**

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

441 The rationale for this mission objective includes:

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

454 **4. Overview of the Cybersecurity Framework**

455 This section was derived from Version 1.1 of the NIST Cybersecurity Framework (CSF), and the
456 reader is advised to consult the CSF and its corresponding quick start guide for additional details
457 [\[NIST-CSF\]](#) [\[NIST-SP1271\]](#). The CSF assists organizations in better managing and reducing
458 cybersecurity risk in a way that responds to the industry’s unique cybersecurity needs, risks,
459 threats, and/or cyber sophistication (regardless of its size). The Framework provides an approach
460 to analyzing cybersecurity risk, enabling enterprises to understand their cybersecurity challenges,
461 and selecting appropriate mitigation strategies. The Framework emphasizes the risk management
462 process for cybersecurity by stating that “the Framework focuses on using business drivers to
463 guide cybersecurity activities and considering cybersecurity risks as part of the organization’s
464 risk management process” [\[NIST-CSF\]](#).

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

- 470 • Describe their current cybersecurity posture.
- 471 • Describe their target state for cybersecurity.

- 472 • Identify and prioritize opportunities for improvement within the context of a continuous
473 and repeatable process.
- 474 • Assess progress toward the target state.
- 475 • Communicate among internal and external relevant parties about cybersecurity risk.

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

483 **4.1. The Framework Core**

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

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

496 When considered together, these functions provide a high-level, strategic view for managing
497 cybersecurity risk. The Framework further identifies underlying key categories and subcategories
498 for each function and matches them with example informative references such as existing
499 standards, guidelines, and practices for each Subcategory. As stated previously, the informative
500 references are meant to be used as examples of best practices and to provide relevant information
501 and are by no means any type of regulatory or compliance mandate from the perspective of this
502 guidance

503 **Table 1** illustrates the alignment of Categories to Functions.
504

505

Table 1. Function and Category Unique Identifiers.

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

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

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

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

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

528 **4.2. Sector-Level Profiles**

529 Sector-level profiles, though not formally defined in the CSF, emerged as a concept after the
530 development of the CSF. Sector-level profiles can act as a starting point for members of the
531 sector to develop their organization’s “current” or “target” profile. Sector-level profiles provide a
532 basis for sub-sectors and individual organizations to facilitate conversations and discuss security
533 activities using consistent terminology. Sector-level profiles are intended to:

- 534 • Provide a foundational profile for organizations to augment or tailor specific to their
535 organizational needs.
- 536 • Decrease the chance that organizations overlook a Category or Subcategory.
- 537 • Encourage consistent analysis of cybersecurity-risk in the sector ecosystem/environment.
- 538 • Align sector and regulatory cybersecurity requirements or needs.

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

542 **5. XFC Baseline Profile**

543 The XFC Baseline Profile was created by using the Cybersecurity Framework as described in
544 [Sec. 4](#). The baseline profile consists of tables for each Category that summarize how each
545 associated Subcategory applies generally to the EV/XFC ecosystem with informative references
546 for additional guidance. The tables provide domain specific considerations as appropriate.

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

552 **5.1. Identify Function**

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

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

561 The objectives of the Identify function include:

- 562 • Identifying the business or operational environment and organization’s purpose
- 563 • Identifying all assets, including hardware, software, personnel, roles, and responsibilities,
564 and assets’ criticality
- 565 • Identifying infrastructure that provides ground segment functionality
- 566 • Identifying the current and trending vulnerabilities, threats, and impacts should the threat
567 be realized to assess the risk.

568 The Identify Function consists of six Categories:

- 569 • Asset Management
- 570 • Business Environment
- 571 • Governance
- 572 • Risk Assessment
- 573 • Risk Management
- 574 • Supply Chain Risk Management

575 Each of these Categories and associated Subcategories are summarized in [Sec. 5.1.1](#) through [Sec.](#)
576 [5.1.6](#).

577 **5.1.1. Asset Management Category**

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

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

Table 2. Identify: Asset Management Category.

Subcategory Domain	Applicability	Informative References
<p>AM-1: Physical devices and systems within the organization are inventoried.</p>	<p>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 the 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 the granularity of the inventory include information such as the manufacturer, model number, serial number, version, its function, or its enabled (or disabled) capabilities. The inventory should include rented or leased equipment 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.</p>	<p>NIST SP 800-53 Rev 5 CM-8, PM-5 NERC CIP 002-5.1a-R1</p>
<p>AM-1 EV</p>	<p>Not directly applicable 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.</p> <p>EV owners may consider being aware of the basic information about their vehicle, such as voltage ratings, rated charging current, charging method (AC or DC) and charging connector type.</p>	<p>[NIST SP 800-53 Rev 5] CM-8, PM-5</p>
<p>AM-1 XFC/EVSE</p>	<p>Applicable, no domain specific considerations.</p>	<p>NIST SP 800-53 Rev 5 CM-8, PM-5 ISA 62443-2-1:D4E1 CM 1.1 ISA 62443-3-3:2013 SR 7.8 NIST Handbook 44 1.10 G-S.1(a)-(c), G-S.2, G-S.6 [OIML D31:2019] 6.2.2.1.1 [OIML G22:2022] 4.1, 5.1</p>
<p>AM-1 Cloud/Third-Party</p>	<p>Applicable, no domain specific considerations.</p>	<p>NIST SP 800-53 Rev 5 CM-8, PM-5</p>

Subcategory Domain	Applicability	Informative References
AM-1 Utility/Building Management System	Applicable, no domain specific considerations.	NIST SP 800-53 Rev 5 CM-8, PM-5 ISA 62443-2-1:D4E1 CM 1.1 ISA 62443-3-3:2013 SR 7.8
AM-2: 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 will track 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 800-53 Rev 5 CM-5, CM-8, CA-9, SA-8 NERC CIP 002-5.1a-R1
AM-2 EV	Applicable. EV manufacturers should consider routinely pushing or providing software updates and patches to EV owners and relevant third parties.	NIST SP 800-53 Rev 5 SA-8
AM-2 XFC/EVSE	Applicable. 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 NIST SP 800-53 Rev 5 SA-8 [OIML D31:2019] 6.1.1, 6.2.2.2.2, 6.2.8.4 [OIML G22:2022] 4.4.2, 4.4.7, 5.1 ISA 62443-2-1:D4E1 CM 1.1 ISA 62443-3-3:2013 SR 7.8
AM-2 Cloud/Third-Party	Applicable. Cloud/third-party owners/operators may consider including any external third-party software hosted on or connected to the systems.	NIST SP 800-53 Rev 5 SA-8
AM-2 Utility/Building Management System	Applicable. Utility/Building management owners/may consider including external third-party software hosted on their systems in the software inventory.	NIST SP 800-53 Rev 5 CM-5, SA-8 ISA 62443-2-1:D4E1 CM 1.1 ISA 62443-3-3:2013 SR 7.8

Subcategory Domain	Applicability	Informative References
<p>AM-3: Organizational communication and data flows are mapped.</p>	<p>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 will show 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.</p>	<p>NIST SP 800-53 Rev 5 AC-4, CA-3, CA-6, CA-9, PM-10, PL-8, SA-17, AC-20</p> <p>NERC CIP 002-5.1a-R1,011-2-R1</p>
<p>AM-3 EV</p>	<p>This mapping will include communication and data relating to vehicle ID, system information, battery statistics, payment information, accounts, etc. Data path/flow diagrams should consider including the EV wire harness and each relevant 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.</p>	<p>NIST SP 800-53 Rev 5 CA-3, CA-6, CA-9</p>
<p>AM-3 XFC/EVSE</p>	<p>Directly applicable. XFC/EVSE interfaces will ensure that only necessary data is sent or received to fulfill its task. This domain may consider measures to avoid an indirect exchange of information between the EV and the Utility domain. This process will include EVSE and EV specific interfacing, as well as any communication to any cloud/third-party systems or utility/building management systems.</p>	<p>ISA 62443-2-1:D4E1 NET 1.01</p> <p>[OIML D31:2019] 7.1.2, 7.3.2.4</p> <p>[OIML G22:2022] 5.1</p>
<p>AM-3 Cloud/Third-Party</p>	<p>Directly applicable. This should include 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. Particular attention should be paid to PCI data flows and data flows to and from data lakes.</p>	<p>NIST SP 800-53 Rev 5 CA-3, CA-6, CA-9</p>
<p>AM-3 Utility/Building Management System</p>	<p>Particular attention should be paid to data lakes. Data path/flow diagrams will show relevant utility/substation SCADA system layouts including PLCs, HMIs, and the equipment they control. Diagrams should consider showing how the cloud network communicates information to the utility. The diagrams can show how information flows and the communication protocols they use.</p>	<p>ISA 62443-2-1:D4E1 NET 1.01</p> <p>NIST SP 800-53 Rev 5 CA-3, CA-6, CA-9</p>
<p>AM-4: External information systems are catalogued.</p>	<p>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.</p>	<p>NIST SP 800-53 Rev 5 AC-20, PM-5, SA-9</p> <p>NERC CIP 011-2-R1</p>

Subcategory Domain	Applicability	Informative References
AM-4 EV	Directly applicable. This should 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 also be included.	NIST SP 800-53 Rev 5 AC-20, PM-5, SA-9
AM-4 XFC/EVSE	External information systems that EVSE interface 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 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 800-53 Rev 5 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 62443-2-1:D4E1 ORG 1.1
AM-5: 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 is a pre-requisite for allocation of resources and enables 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 given to user safety, financial, and privacy/personally identifiable information security during prioritization.	[NIST-SP800-37r2] [NIST-SP800-53r5] AC-20, CP-2, CP-8, RA-2, RA-9, SA-20, SC-6
AM-5 EV	Directly applicable. 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

Subcategory Domain	Applicability	Informative References
AM-5 XFC/EVSE	<p>Directly applicable. 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.</p> <p>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.</p>	<p>ISA 62443-2-1:D4E1 DATA 1.1</p> <p>[OIM D31:2019] 6.2.2.2.4</p>
AM-5 Cloud/Third-Party	<p>Directly applicable with an understanding that the criticality to customer and partners organizations should be part of the prioritization.</p>	<p>[NIST-SP800-53r5] AC-20, RA-2, RA-9, SA-20, SC-6</p>
AM-5 Utility/Building Management System	<p>Applicable with the additional consideration that some of their 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.</p>	<p>ISA 62443-2-1:D4E1 DATA 1.1</p> <p>[NIST-SP800-53r5] AC-20, RA-2, RA-9, SA-20, SC-6</p>
AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	<p>Ecosystem: Clear definition of roles and responsibilities enables the coordinator 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 will include 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.</p>	<p>[NIST-SP800-53r5] CP-2, PM-2, PM-11 PM-29, PS-2, PS-7</p> <p>NERC CIP 004-6-R4, 004-6-R2</p>
AM-6 EV	<p>Directly applicable. Additional relevant parties for EV manufactures include elements of the workforce involved in vehicle design, and pre/post-sales support. EV owners should 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.</p>	<p>[ISO 21434] RQ-07-04</p>

Subcategory Domain	Applicability	Informative References
AM-6 XFC/EVSE	Additional relevant parties for EVSE manufactures will include elements of the workforce involved in equipment design/usage, pre/post-sales support, and those involved during EVSE installation design and construction.	ISA 62443-2-1:D4E1 ORG 1.3
AM-6 Cloud/Third-Party	Applicable. 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	Applicable. 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 62443-2-1:D4E1 ORG 1.3

587 **5.1.2. Business Environment Category**

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

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

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

Subcategory Domain	Applicability	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 is a prerequisite 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 which may impact supply chain positions and agreements. Subcomponents (e.g., microcontrollers, sensors, electrical wiring, connectors, etc.) 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
BE-1 EV	EV manufacturers’ role in the supply chain includes relationships and interfaces with suppliers, customers, EVSE manufacturers/operators, and cloud/third-party operators.	[ISO 21434] RQ-07-04, WP-07-01

Subcategory Domain	Applicability	Informative References
BE-1 XFC/EVSE	EVSE manufacturers' role in the supply chain includes 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 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-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.	[ISO 21434] RQ-10-03 [NIST-SP800-161] [NIST-SP800-53r5] PM-8
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
BE-2 Cloud/Third-Party	Additionally, identified dependencies and requirements may be communicated internally and with impacted business partners. EVSE booking and alternative billing options to cloud/third-party use will be defined for use in the event of degradation or an outage.	[NIST-SP800-161] [NIST-SP800-53r5] PM-8

Subcategory Domain	Applicability	Informative References
<p>BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.</p>	<p>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.</p>	<p>[NIST-SP800-53r5] PM-11</p>
<p>BE-3 EV</p>	<p>Applicable, no EV specific considerations.</p>	<p>[NIST-SP800-53r5] PM-11</p>
<p>BE-3 XFC/EVSE</p>	<p>Applicable. EVSE manufacturers and owners/operators should consider emphasizing the cybersecurity and operational requirements of partners within the EV/XFC ecosystem in the prioritization process.</p>	<p>[NIST-SP800-53r5] PM-11</p>
<p>BE-3 Cloud/Third-Party</p>	<p>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.</p>	<p>[NIST-SP800-53r5] PM-11</p>
<p>BE-3 Utility/Building Management System</p>	<p>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.</p>	<p>[NIST-SP800-53r5] PM-11</p>
<p>BE-4: Dependencies and critical functions for delivery of critical services are established.</p>	<p>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.</p>	<p>[NIST-SP800-53r5] CP-2, CP-8, PE-9, PE-11, PM-8, RA-9, SA-20, SR-2</p>
<p>BE-4 EV</p>	<p>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 PII, or cause harm to the EV, EVSE, utility/building infrastructure, or user/owner.</p>	<p>[ISO 21434] RQ-15-01, RQ-15-02</p>

Subcategory Domain	Applicability	Informative References
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 will recognize that providing safe and reliable patches as well as support to operators, is a critical function. 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 EV via Cloud apps, and effective collaboration with third parties to charge EV owners for purchase.	ISA 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 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 is preferable to complete failure during attack and recovery. Resilience plans will include details for how operating states are defined, operational adjustments in each state, and necessary communications.	IEC61850-90-4 12.2, 14.2.4 [NIST-SP800-53r5] CP-2, CP-11, RA-9, SA-8, SA-20 NERC CIP 009-6-R1
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.	IEC61850-90-4 12.2, 14.2.4 [NIST-SP800-53r5] CP-2, CP-11

Subcategory Domain	Applicability	Informative References
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.	ISA 62443-2-1:D4E1 AVAIL 1.1 NIST Handbook 44 3.40 S.2.1, S.2.2, S.2.3 [OIML D31:2019] 6.2.5.3 [OIML G22:2022] 4.4.9.3.1, 4.49.3.2
BE-5 Cloud/Third-Party	Applicable, no Cloud/Third-Party specific considerations.	IEC61850-90-4 12.2, 14.2.4 [NIST-SP800-53r5] CP-2, CP-11
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 62443-2-1:D4E1 AVAIL 1.1

594 **5.1.3. Governance Category**

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

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

602 **Table 4.** Identify: Governance Category.

Subcategory Domain	Applicability	Informative References
GV-1: Organizational cybersecurity policy is established and communicated.	Ecosystem: The policies should be developed collaboratively with external organizations within the domain to ensure consistency and should consider inputs from partner companies within the ecosystem to ensure interoperability. Additionally, policies may consider defining activities, roles, and responsibilities to manage operational systems, regulatory requirements, update and maintenance strategies, or applicable industry standards among other considerations.	[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 ISO/SAE 21434 NERC CIP 004-6-R2

Subcategory Domain	Applicability	Informative References
GV-1 EV	Applicable, but no EV specific considerations.	[ISO 21434] RQ-05-01, RQ-05-02, RQ-05-03, RQ-05-04, RQ-05-05, WP-05-01
GV-1 XFC/EVSE	Applicable, but no XFC/EVSE specific considerations.	ISA 62443-2-1:D4E1 ORG 1.1
GV-1 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] 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 Utilities/Building management specific considerations.	ISA 62443-2-1:D4E1 ORG 1.1
GV-2: 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 SLA, 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] 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 21434] RQ-07-04, WP-07-01
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 62443-2-1:D4E1 ORG 1.3
GV-2 Cloud/Third-Party	Applicable, no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] PM-1, PM-2, PM-29
GV-2 Utility/Building Management System	Applicable, no Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 ORG 1.3

Subcategory Domain	Applicability	Informative References
<p>GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.</p>	<p>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.</p>	<p>[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</p>
<p>GV-3 EV</p>	<p>Applicable, but no EV specific considerations.</p>	<p>[NIST-SP800-53r5] SA-1, SC-1, SI-1, SR-1</p>
<p>GV-3 XFC/EVSE</p>	<p>Applicable, but no XFC/EVSE specific considerations.</p>	<p>ISA 62443-2-1:D4E1 ORG 1.1</p>
<p>GV-3 Cloud/Third-Party</p>	<p>Applicable, but no Cloud/Third-Party specific considerations.</p>	<p>[NIST-SP800-53r5] SA-1, SC-1, SI-1, SR-1</p>
<p>GV-3 Utility/Building Management System</p>	<p>Applicable, but no Utilities/Building management specific considerations.</p>	<p>ISA 62443-2-1:D4E1 ORG 1.1</p>
<p>GV-4: Governance and risk management processes address cybersecurity risks.</p>	<p>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.</p>	<p>[NIST-SP800-53r5] PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, RA-1, RA-2, RA-3, SA-2 [NIST-SP800-160V1] 3.3.8 ISO/SAE 21434</p>
<p>GV-4 EV</p>	<p>Applicable, but no EV specific considerations.</p>	<p>[ISO 21434] RQ-05-01, RQ-05-02, RQ-05-03, RQ-05-04, RQ-05-05, WP-05-01</p>
<p>GV-4 XFC/EVSE</p>	<p>Applicable, but no XFC/EVSE specific considerations.</p>	<p>ISA 62443-2-1:D4E1 ORG 2.1</p>
<p>GV-4 Cloud/Third-Party</p>	<p>Applicable, but no Cloud/Third-Party specific considerations.</p>	<p>[NIST-SP800-53r5] PM-3, PM-7, PM-9, PM-10, PM-11, PM-28 [NIST-SP800-160V1] 3.3.8</p>
<p>GV-4 Utility/Building Management System</p>	<p>Applicable, but no Utilities/Building management specific considerations.</p>	<p>ISA 62443-2-1:D4E1 ORG 2.1</p>

603 **5.1.4. Risk Assessment Category**

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

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

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

Subcategory Domain	Applicability	Informative References
RA-1: Asset vulnerabilities are identified and documented.	Ecosystem: 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. 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 [Auto-ISAC] [E-ISAC] NERC CIP 007-6-R2
RA-1 EV	Applicable. Consider participation in forums such as Auto-ISAC to gain information regarding vulnerabilities. Known asset vulnerabilities may include accessible connector ports, ...	[ISO 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 62443-2-1:D4E1 EVENT 1.9
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	Applicable. 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 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 [NIST-SP800-150] NERC CIP 007-6-R2
RA-2 EV	Applicable. EV manufactures may consider participation in Auto-ISAC for industry specific intelligence.	[ISO 21434] RQ-08-01, WP-08-01

Subcategory Domain	Applicability	Informative References
RA-2 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 ORG 1.1
RA-2 Cloud/Third Party	Applicable, but no Cloud/Third Party specific considerations.	[NIST-SP800-53r5] PM-15, PM-16, RA-10, SI-5 [NIST-SP800-150]
RA-2 Utility/Building Management System	Applicable. Utility/Building Management Systems may consider participation in 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 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] [NIST-SP800-37r2] [NIST-SP800-53r5] PM-12, PM-16, RA-3, RA-10, SI-5 [NIST-SP800-154] [NIST-SP800-160V1] 2.3 NERC CIP 007-6-R4
RA-3 EV	Applicable, but no EV specific considerations.	[ISO 21434] RQ-15-04, RQ-15-06
RA-3 XFC/EVSE	Applicable, but no XFC-EVSE specific considerations.	[NIST-SP800-53r5] PM-12, PM-16, RA-3, RA-10, SI-5
RA-3 Cloud/Third-Party	Applicable, but no 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 Utility/Building Management Systems 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 NERC CIP 002-5.1a-R1
RA-4 EV	Applicable, but no EV specific considerations.	[ISO 21434] Clause 15

Subcategory Domain	Applicability	Informative References
RA-4 XFC/EVSE	Applicable, but no XFC/EVSE specific considerations.	ISA 62443-2-1:D4E1 ORG 2.1
RA-4 Cloud/Third-Party	Possible impacts on charge station availability and PII should be 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 be identified.	ISA 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] [NIST-SP800-53r5] CA-2, CA-7, PM-16, PM-28, RA-2, RA-3 [NIST-SP800-160V1] 2.3, 2.4 NERC CIP 007-6-R2
RA-5 EV	Applicable, but no EV specific considerations.	[ISO 21434] [WP-15-04], [WP-15-05], [WP-15-06], [WP-15-07]
RA-5 XFC/EVSE	Applicable, but no XFC/EVSE specific considerations.	ISA 62443-2-1:D4E1 ORG 2.1
RA-5 Cloud/Third-Party	Applicable, but no 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 Utility/Building management specific considerations.	ISA 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 should consider 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 EV specific considerations.	[ISO 21434] WP-13-01
RA-6 XFC/EVSE	Applicable, but no XFC/EVSE specific considerations.	ISA 62443-2-1:D4E1 ORG 2.1

Subcategory Domain	Applicability	Informative References
RA-6 Cloud/Third-Party	Applicable, but no 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 Utilities/Building management specific considerations.	ISA 62443-2-1:D4E1 ORG 2.1

610 **5.1.5. Risk Management Category**

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

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

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

Subcategory Domain	Applicability	Informative References
RM-1: 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] PM-9, PM-28 ISA 62443-2-1:D4E1 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 21434] WP-05
RM-1 XFC/EVSE	Risk management processes should potentially include accounting for EV/XFC partners, suppliers and organizations like NERC and FERC.	ISA 62443-2-1:D4E1 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] 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 62443-2-1:D4E1 ORG 2.1

Subcategory Domain	Applicability	Informative References
<p>RM-2: Organizational risk tolerance is determined and clearly expressed.</p>	<p>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 will include special considerations for any safety, safety-critical, financial, or regulatory aspects. Organizations may communicate their risk tolerance to the other domains within the ecosystem.</p>	<p>[NIST-SP800-53r5] PM-9</p>
<p>RM-2 EV</p>	<p>Applicable, but no EV specific considerations</p>	<p>[NIST-SP800-53r5] PM-9</p>
<p>RM-2 XFC/EVSE</p>	<p>Applicable, but no EVSE specific considerations.</p>	<p>[NIST-SP800-53r5] PM-9</p>
<p>RM-2 Cloud/Third-Party</p>	<p>Applicable, but no Cloud/Third-Party specific considerations</p>	<p>ISA 62443-2-1:D4E1 ORG 2.1</p>
<p>RM-2 Utility/Building Management System</p>	<p>Applicable, but no Utility/Building Management specific considerations</p>	<p>ISA 62443-2-1:D4E1 ORG 2.1</p>
<p>RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.</p>	<p>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.</p>	<p>[NIST-SP800-53r5] PM-8, PM-9, PM-11, RA-9</p>
<p>RM-3 EV</p>	<p>Applicable, but no EV specific considerations</p>	<p>[NIST-SP800-53r5] PM-8, PM-9, PM-11, RA-9</p>
<p>RM-3 XFC/EVSE</p>	<p>Applicable, but no EVSE specific considerations.</p>	<p>ISA 62443-2-1:D4E1 ORG 2.1</p>
<p>RM-3 Cloud/Third-Party</p>	<p>Applicable, but no Cloud/Third-Party specific considerations</p>	<p>[NIST-SP800-53r5] PM-8, PM-9, PM-11, RA-9</p>
<p>RM-3 Utility/Building Management System</p>	<p>Applicable, but no Utility/Building Management specific considerations</p>	<p>ISA 62443-2-1:D4E1 ORG 2.1</p>

616 **5.1.6. Supply Chain Risk Management Category**

617 The organization’s priorities, constraints, risk tolerances, and assumptions are established and
618 used to support risk decisions associated with managing supply chain risk. The organization has
619 established and implemented processes to identify, assess, and manage supply chain risks.

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

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

Subcategory Domain	Applicability	Informative References
<p>SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.</p>	<p>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. Roles and responsibilities may be established and consistently implemented across the organization. The supply chain should consider being assessed 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.</p>	<p>[NIST-SP800-53r5] PM-30, SA-9, SR-1, SR-2, SR-3, SR-5 [NIST-SP800-161]</p>
<p>SC-1 EV</p>	<p>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, etc.) critical to the function of onboard controllers and management systems should be included in the evaluation of cyber supply chain risk.</p>	<p>[ISO 21434] RQ-07-04, WP-07-01</p>
<p>SC-1 XFC/EVSE</p>	<p>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, etc.) critical to the function of onboard controllers and management systems should be included in the evaluation of cyber supply chain risk.</p>	<p>[NIST-SP800-53r5] SR-1, SR-2, SR-3, SR-5 [NIST-SP800-161]</p>

Subcategory Domain	Applicability	Informative References
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, etc.) 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] SR-1, SR-2, SR-3, SR-5 [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, etc.) critical to the function of onboard controllers and management systems should be included in the evaluation of cyber supply chain risk.	[NIST-SP800-53r5] SR-1, SR-2, SR-3, SR-5 [NIST-SP800-161]
SC-2: Suppliers and third-party partners of information systems, components and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	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. Risks should consider being assessed 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 [NIST-SP800-161] 2.2, 3
SC-2 EV	Applicable, but no EV specific considerations.	[ISO 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 Cloud/Third-Party specific considerations.	[NIST-SP800-161] 2.2, 3
SC-2 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NIST-SP800-161] 2.2, 3

Subcategory Domain	Applicability	Informative References
<p>SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.</p>	<p>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 will include security control, monitoring, and incident response requirements.</p>	<p>[NIST-SP800-53r5] SA-4, SA-9, SR-2, SR-3, SR-5</p>
<p>SC-3 EV</p>	<p>Applicable, but no EV specific considerations.</p>	<p>[ISO 21434] RQ-07-04, WP-07-01</p>
<p>SC-3 XFC/EVSE</p>	<p>Applicable, but no EVSE specific considerations.</p>	<p>[NIST-SP800-53r5] SA-4, SA-9</p>
<p>SC-3 Cloud/Third-Party</p>	<p>Applicable, but no Cloud/Third-Party specific considerations.</p>	<p>[NIST-SP800-53r5] SA-4, SA-9</p>
<p>SC-3 Utility/Building Management System</p>	<p>Applicable, but no Utility/Building Management specific considerations.</p>	<p>[NIST-SP800-53r5] SA-4, SA-9</p>
<p>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.</p>	<p>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. Formal procedures and contingency plans should be established to manage and enforce contractual obligations within the ecosystem.</p>	<p>[NIST-SP800-53r5] AU-6, CA-2, CA-7, PS-7, SA-9, SA-11</p>
<p>SC-4 EV</p>	<p>Applicable, but no EV specific considerations.</p>	<p>[NIST-SP800-53r5] AU-6</p>
<p>SC-4 XFC/EVSE</p>	<p>Applicable, but no EVSE specific considerations.</p>	<p>ISA 62443-3-3:2013 SR 6.1</p>
<p>SC-4 Cloud/Third-Party</p>	<p>Applicable, but no Cloud/Third-Party specific considerations.</p>	<p>[NIST-SP800-53r5] AU-6</p>
<p>SC-4 Utility/Building Management System</p>	<p>Applicable, but no Utility/Building Management specific considerations.</p>	<p>ISA 62443-3-3:2013 SR 6.1</p>

Subcategory Domain	Applicability	Informative References
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 EV specific considerations.	[NIST-SP800-53r5] IR-3, IR-4, IR-8, IR-9
SC-5 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 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 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 Utility/Building Management specific considerations.	ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4

625 **5.2. Protect Function Considerations Across the EV/XFC Domains**

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

629 The Protect Function consists of six Categories:

- 630 • Identity Management, Authentication, and Access Control
- 631 • Awareness and Training
- 632 • Data Security
- 633 • Information Protection Processes and Procedures
- 634 • Maintenance
- 635 • Protective Technology

636 **5.2.1. Identity Management, Authentication and Access Control Category**

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

643

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

Subcategory Domain	Applicability	Informative References
<p>AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.</p>	<p>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 & validation certificates, software certificates, and system administration credentials. Credentials will be promptly accredited and decommissioned when issued and revoked.</p>	<p>[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</p> <p>NERC CIP 004-6-R4, 007-6-R5</p>
<p>AC-1 EV</p>	<p>Applicable, no domain specific considerations.</p>	<p>[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</p>
<p>AC-1 XFC/EVSE</p>	<p>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.</p>	<p>ISA 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</p> <p>ISA 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</p>
<p>AC-1 Cloud/Third-Party</p>	<p>Applicable, no domain specific considerations.</p>	<p>[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</p>
<p>AC-1 Utility/Building Management System</p>	<p>Utility/building management devices/systems specific identities/credentials may include control system credentials, energy management system credentials, and building access credentials.</p>	<p>ISA 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</p> <p>ISA 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</p>

Subcategory Domain	Applicability	Informative References
<p>AC-2: Physical access to assets is managed and protected.</p>	<p>Ecosystem: Physical connections to communication ports must be protected, and if unnecessary, removed or disabled.</p>	<p>[NIST-IR8320] [NIST-SP800-53r5] PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9 NERC CIP 007-6-R5</p>
<p>AC-2 EV</p>	<p>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.</p>	<p>[NIST-SP800-53r5] PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9</p>
<p>AC-2 XFC/EVSE</p>	<p>Physical access may include (but are 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.</p>	<p>ISA 62443-2-1:D4E1 ORG 3.1, AVAIL 1.1, AVAIL 1.2 NIST Handbook 44 1.10 G-S.8, 1.10 G-S.8.2, 3.40 S.3.1, 3.40 S.3.3 [OIML D31:2019] 6.1.3.2.1, 6.1.3.2.4, [OIML G22:2022] 4.4.3.2</p>
<p>AC-2 Cloud/Third-Party</p>	<p>Applicable, but no Cloud/Third-Party specific considerations.</p>	<p>[NIST-SP800-53r5] PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9</p>
<p>AC-2 Utility/Building Management System</p>	<p>Applicable, but no Utility/Building Management specific considerations.</p>	<p>ISA 62443-2-1:D4E1 ORG 3.1, AVAIL 1.1, AVAIL 1.2</p>
<p>AC-3: Remote access is managed.</p>	<p>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.</p>	<p>[NIST-SP800-53r5] AC-1, AC-2, AC-17, AC-19, AC-20, SC-7 SC-15 NERC CIP 004-6-R4, 004-6-R5</p>
<p>AC-3 EV</p>	<p>This may include (but are not limited to) authorized over the air (OTA) updates, vehicle status/usage information, and customer remote access features.</p>	<p>[NIST-SP800-53r5] AC-2, AC-17, AC-19, AC-20</p>

Subcategory Domain	Applicability	Informative References
AC-3 XFC/EVSE	This may include (but are not limited to) 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, NFC, etc.) that might be necessary to provide remote access to the equipment.	<p>ISA 62443-2-1:D4E1 NET 1.01, NET 1.06, NET 3.3. NET 3.4</p> <p>ISA 62443-3-3:2013 SR 1.13, SR 2.6</p> <p>[OIML D31:2019] 6.2.6.5, 6.2.6.5.3</p> <p>[OIML G22:2022] 4.4, 4.4.3, 4.4.4, 4.4.8</p>
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.	<p>ISA 62443-2-1:D4E1 NET 1.01, NET 1.06, NET 3.3. NET 3.4</p> <p>ISA 62443-3-3:2013 SR 1.13, SR 2.6</p>
AC-4: 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 will be periodically reviewed to remove outdated permissions and may include Role Based Access Control (RBAC) or other access control paradigms.	<p>[NIST-SP800-53r5] AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24</p> <p>[NIST-SP800-160V1] Appendix F.1.14</p> <p>NERC CIP 004-6-R4 004-6-R5 007-6-R5</p>
AC-4 EV	This 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	This 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.	<p>[PCI-DSS v4]</p> <p>ISA 62443-2-1:D4E1 USER 1.04, USER 1.05, USER 1.07, USER 2.1, USER 2.2</p> <p>ISA 62443-3-3:2013 SR 2.1</p> <p>[OIML D31:2019] 6.2.5.2, 6.2.6.6</p>
AC-4 Cloud/Third-Party	This may include access permissions and authorizations from EVs, EVSE systems, web vendors, and utility/building management systems.	[PCI-DSS v4]

Subcategory Domain	Applicability	Informative References
AC-4 Utility/Building Management System	This 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 62443-2-1:D4E1 USER 1.04, USER 1.05, USER 1.07, USER 2.1, USER 2.2 ISA 62443-3-3:2013 SR 2.1
AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	Ecosystem: The EV/XFC ecosystem 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 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 will protect 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] ISA 62443-2-1:D4E1 NET 1.01, NET 1.06, USER 1.16 ISA 62443-3-3:2013 SR 3.1, SR 3.8
AC-5 Cloud/Third-Party	This 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 [PCI-DSS v4]
AC-5 Utility/Building Management System	This may include network links to/from EVSE and cloud/third-party systems, as well as other utility/building management systems and assets.	ISA 62443-2-1:D4E1 NET 1.01, NET 1.06, USER 1.16 ISA 62443-3-3:2013 SR 3.1, SR 3.8

Subcategory Domain	Applicability	Informative References
<p>AC-6: Identities are proofed, bound to credentials, and asserted in interactions.</p>	<p>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 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.</p> <p>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.</p>	<p>[ATIS-I-0000070] 2-7</p> <p>[NIST-IR8014]</p> <p>[NIST-SP800-53r5] AC-16, IA-1, IA-2, IA-4, IA-5, IA-8, IA-12, PE-2, PS-3</p> <p>NERC CIP 004-6-R3</p>
<p>AC-6 EV</p>	<p>Applicable. EV-specific considerations include user accounts accessible from the EV and driver identification.</p>	<p>[NIST-SP800-53r5] AC-16, IA-1, IA-2, IA-4, IA-5, IA-8, IA-12</p> <p>[PCI-DSS v4]</p>
<p>AC-6 XFC/EVSE</p>	<p>Applicable, no domain specific considerations.</p>	<p>[PCI-DSS v4]</p> <p>ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1</p>
<p>AC-6 Cloud/Third-Party</p>	<p>Applicable, no domain specific considerations.</p>	<p>[NIST-SP800-53r5] AC-16, IA-1, IA-2, IA-4, IA-5, IA-8, IA-12</p> <p>[PCI-DSS v4]</p>
<p>AC-6 Utility/Building Management System</p>	<p>Applicable, no domain specific considerations.</p>	<p>[PCI-DSS v4]</p> <p>ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1</p>
<p>AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).</p>	<p>Ecosystem: EV/XFC ecosystem may consider the implementation of multi-factor authentication (MFA) where possible. Assets may include data, hardware, software, networks, and facilities.</p>	<p>[IETF-RFC4082] 2-5</p> <p>[NIST-SP800-53r5] AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10</p> <p>NERC CIP 007-6-R5</p>

Subcategory Domain	Applicability	Informative References
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] 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 62443-3-3:2013 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] 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 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10

644 **5.2.2. Awareness and Training Category**

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

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

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

Subcategory Domain	Applicability	Informative References
AT-1: 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] 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] 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 62443-2-1:D4E1 ORG 1.4

Subcategory Domain	Applicability	Informative References
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] AT-2, PM-14
AT-1 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	ISA 62443-2-1:D4E1 ORG 1.4
AT-2: 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. Awareness levels should be continually tested, reevaluated, and retrained to help maintain system security. Privileged user-specific training will emphasize elevated attacker desire to compromise privileged accounts and the consequences of breaches.	[NIST-SP800-53r5] AT-3, PM-13 [NIST-SP800-161] Appendix E
AT-2 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] AT-3, PM-13
AT-2 XFC/EVSE	Applicable, but no EVSE specific considerations.	[NIST-SP800-53r5] AT-3, PM-13
AT-2 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] AT-3, PM-13
AT-2 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NIST-SP800-53r5] AT-3, PM-13
AT-3: 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 should 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] AT-3, PS-7, SA-9
AT-3 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] AT-3, PS-7
AT-3 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 ORG 1.3, ORG 1.4
AT-3 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] AT-3, PS-7

Subcategory Domain	Applicability	Informative References
AT-3 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	ISA 62443-2-1:D4E1 ORG 1.3, ORG 1.4
AT-4: 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 will emphasize elevated attacker desire to compromise executive accounts and the consequences of breaches.	[NIST-SP800-53r5] AT-3, PM-2, PM-13, PM-29
AT-4 EV	Applicable, but no EVSE specific considerations.	[NIST-SP800-53r5] PM-2, PM-13, PM-29
AT-4 XFC/EVSE	Applicable, but no EV specific considerations.	ISA 62443-2-1:D4E1 ORG 1.3, ORG 1.4
AT-4 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] PM-2, PM-13, PM-29
AT-4 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	ISA 62443-2-1:D4E1 ORG 1.3, ORG 1.4
AT-5: 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 should be continually tested, reevaluated, and retrained to maintain system security. Physical/cybersecurity personnel-specific training should emphasize the best practices to adopt and how to identify and report cybersecurity risks. This should include 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 EV specific considerations.	[NIST-SP800-53r5] AT-3, IR-2, PM-13
AT-5 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 ORG 1.3, ORG 1.4
AT-5 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] AT-3, IR-2, PM-13

Subcategory Domain	Applicability	Informative References
AT-5 Utility/Building Management System	Applicable. Utility/Building Management Systems may consider existing physical security requirements and/or regulations.	ISA 62443-2-1:D4E1 ORG 1.3, ORG 1.4

652 **5.2.3. Data Security Category**

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

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

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

Subcategory Domain	Applicability	Informative References
DS-1: Data-at-rest is protected.	<p>Ecosystem: Ecosystem members can consider having increased protections for sensitive, PII, or transactional data. Data-at-rest protections may be provided through measures such as:</p> <ul style="list-style-type: none"> • Securing and tamper-resistant data storage. • Encrypting all data. • Restricting access to all data around a strict need and for a specified time period. • Monitoring and conducting regular security audits of protection mechanisms. • Regularly updating the software and firmware of all onboard electronic management and control systems. <p>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.</p>	<p>[NIST-SP800-37r2]</p> <p>[NIST-SP800-53r5] MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28</p> <p>[NIST-SP800-175Br1]</p> <p>[NIST-SP800-209]</p> <p>NERC CIP 004-6-R4, 004-6-R5, 011-2-R1</p>
DS-1 EV	Data at rest includes any information that is stored onboard electronic management and control systems within the EV. This data may include information on vehicle performance, battery performance, charging history, location history, associated accounts, and charging profiles from EV/XFC partners, and suppliers/vendors.	<p>[NIST-SP800-53r5] MP-3, MP-4, SC-28</p> <p>[NIST-SP800-175Br1]</p> <p>[NIST-SP800-209]</p>

Subcategory Domain	Applicability	Informative References
DS-1 XFC/EVSE	Data at rest 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.	<p>ISA 62443-2-1:D4E1 CM 1.3, DATA 1.2</p> <p>ISA 62443-3-3:2013 SR 3.4, SR 4.1</p> <p>[OIML D31:2019] 6.2.3.4</p> <p>NIST Handbook 44 3.40 S.3.4(a)</p>
DS-1 Cloud/Third-Party	Data at rest 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. Information database access should be protected from unauthorized access and security breaches.	<p>[NIST-SP800-53r5] MP-3, MP-4, SC-28</p> <p>[NIST-SP800-175Br1]</p> <p>[NIST-SP800-209]</p>
DS-1 Utility/Building Management System	Data at rest 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.	<p>ISA 62443-2-1:D4E1 CM 1.3, DATA 1.2</p> <p>ISA 62443-3-3:2013 SR 3.4, SR 4.1</p>
DS-2: Data-in-transit is protected.	<p>Ecosystem: Ecosystem members may consider having increased protections for sensitive, PII, or transactional data. DIT protections may be provided through measures such as:</p> <ul style="list-style-type: none"> • Securing and tamper-resistant communication systems and protocols for all transmitted data. • Encrypting data transmitted over wired or wireless communication channels. • Monitoring and conducting regular security audits of protection mechanisms. • Error detecting/correcting protocols. <p>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.</p>	<p>[NIST-SP800-53r5] SC-8, SC-11, SC-12</p> <p>NERC CIP 004-6-R4, 004-6-R5</p>
DS-2 EV	Data-in-transit includes any information that is transmitted over wired or wireless communication channels onboard electronic management and control systems within 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.	<p>[NIST-SP800-53r5] SC-8, SC-11, SC-12</p>

Subcategory Domain	Applicability	Informative References
DS-2 XFC/EVSE	EVSE owners/operators should consider encrypting all traffic leaving the EVSE.	<p>[PCI-DSS v4]</p> <p>ISA 62443-2-1:D4E1 NET 1.01, NET 1.06, NET 1.08, DATA 1.2, DATA 1.6, USER 1.16</p> <p>ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2</p> <p>[OIML D31:2019] 6.2.5.2</p> <p>[OIML D22:2022] 4.4.9</p>
DS-2 Cloud/Third-Party	Data in transit 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.	<p>[NIST-SP800-53r5] SC-8, SC-11, SC-12</p> <p>[PCI-DSS v4]</p>
DS-2 Utility/Building Management System	Data in transit 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.	<p>ISA 62443-2-1:D4E1 NET 1.01, NET 1.06, NET 1.08, DATA 1.2, DATA 1.6, USER 1.16</p> <p>ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2</p>
DS-3: 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.	<p>[NIST-SP800-53r5] CM-8, MP-6, PE-16, PE-20</p> <p>NERC CIP 011-2-R2</p>
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 include encryption and authentication protocols and should only be 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. Procedures should include guidelines for data retention, backup, and secure disposal.	<p>[NIST-SP800-53r5] CM-8, MP-6, PE-16, PE-20</p>
DS-3 XFC/EVSE	Associated data may include information from EV owners, EV/XFC partners, and suppliers/vendors.	<p>ISA 62443-2-1:D4E1 COMP 1.1, USER 1.04, USER 1.05</p> <p>ISA 62443-3-3:2013 SR 4.2</p>

Subcategory Domain	Applicability	Informative References
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 62443-2-1:D4E1 COMP 1.1, USER 1.04, USER 1.05 ISA 62443-3-3:2013 SR 4.2
DS-4: Adequate capacity to ensure availability is maintained.	Ecosystem: Measures to augment capacity may include: <ul style="list-style-type: none"> • Formal procedures and activities to monitor system performance • Redundant transmission systems • Alternate transmission systems (such as RF, wired or optical systems) Methods such as load balancing address abnormal server loads due to elevated traffic from user activity, incorrect server configurations, or cybersecurity events.	IEC62439-3 4, 5, Appendix P.2.3, 4.6, 4.8, 4.9, 4.12, 4.13 [NIST-SP800-53r5] AU-4, CP-2, CP-6, CP-7, PE-11, SC-5 [NIST-SP800-160V1] Appendix F.4 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 [NIST-SP800-160V1] Appendix F.4
DS-4 XFC/EVSE	This may include information from EV owners, EV/XFC partners, and suppliers/vendors.	ISA 62443-3-3:2013 SR 7.1, SR 7.2 NIST Handbook 44 3.40 S.3.4 (c) [OIML G22:2022] 4.4.9.2.2 [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 [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 62443-3-3:2013 SR 7.1, SR 7.2

Subcategory Domain	Applicability	Informative References
<p>DS-5: Protections against data leaks are implemented.</p>	<p>Ecosystem: Ecosystem members may consider initially identifying what is classified as sensitive data, where it is 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.</p>	<p>[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</p> <p>NERC CIP 004-6-R4, 004-6-R5, 007-6-R3, 007-6-R4, 007-6-R5, 011-2-R2</p>
<p>DS-5 EV</p>	<p>Data leak protections may apply to information on vehicle performance, battery performance, charging information and history, 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.</p>	<p>[NIST-SP800-53r5] AC-4, AC-5, AC-6, PS-6, SC-7, SC-8, SC-13</p>
<p>DS-5 XFC/EVSE</p>	<p>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.</p>	<p>ISA 62443-2-1:D4E1 NET 1.01, NET 1.06, NET 1.08, DATA 1.1, DATA 1.2</p> <p>ISA 62443-3-3:2013 SR 5.2</p>
<p>DS-5 Cloud/Third-Party</p>	<p>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 APIs.</p>	<p>[NIST-SP800-53r5] AC-4, AC-5, AC-6, PS-6, SC-7, SC-8, SC-13</p>
<p>DS-5 Utility/Building Management System</p>	<p>Data leak protections may apply to information from EV/XFC partners, utility/building management partners, and suppliers/vendors.</p>	<p>ISA 62443-2-1:D4E1 NET 1.01, NET 1.06, NET 1.08, DATA 1.1, DATA 1.2</p> <p>ISA 62443-3-3:2013 SR 5.2</p>
<p>DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.</p>	<p>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., OCPP or other standards), may be simple CRCs, or more advanced cryptographic mechanisms, such as digital signatures to validate the integrity of the firmware or software.</p>	<p>[NIST-SP800-53r5] SI-7, SI-10</p> <p>[NIST-SP800-160V1] 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F</p> <p>[NIST-SP800-161]</p> <p>[NIST-SP800-193]</p> <p>[NIST-SP800-218] PO.3.3, PS.1</p>

Subcategory Domain	Applicability	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.	<p>[NIST-SP800-160V1] 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F</p> <p>[NIST-SP800-193]</p> <p>[NIST-SP800-218] PO.3.3, PS.1</p>
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.	<p>ISA 62443-2-1:D4E1 ORG 2.2, DATA 1.2, USER 1.16</p> <p>[OIML D31:2019] 6.1.1, 6.2.2.1.1, 6.2.2.1.2</p> <p>[OIML G22:2022] 4.4.2, 4.4.5.1</p> <p>NIST Handbook 44 1.10 G-S.1 (c), (d)</p> <p>ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8</p>
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.	<p>[NIST-SP800-160V1] 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F</p> <p>[NIST-SP800-193]</p> <p>[NIST-SP800-218] PO.3.3, PS.1</p>
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.	<p>ISA 62443-2-1:D4E1 ORG 2.2, DATA 1.2, USER 1.16</p> <p>ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8</p>
DS-7: 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.	<p>[NIST-SP800-53r5] CM-2, SA-3</p> <p>[NIST-SP800-160V1] 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F</p>
DS-7 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] CM-2, SA-3
DS-7 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 NET 1.01
DS-7 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CM-2, SA-3

Subcategory Domain	Applicability	Informative References
DS-7 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	ISA 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.	FIPS 140-3 NIST-IR800-8320 [NIST-SP800-53r5] AC-25, SA-10, SI-7, SR-9, SR-10 [NIST-SP1800-19] [NIST-SP1800-34]
DS-8 EV	EV-specific hardware under evaluation may include the battery system, charge controller, propulsion and control systems, electrical wiring, and connectors.	FIPS 140-3 [NIST-SP800-53r5] AC-25, SA-10, SI-7, SR-9, SR-10
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.	FIPS 140-3 [NIST-SP800-53r5] AC-25, SA-10, SI-7, SR-9, SR-10
DS-8 Cloud/Third-Party	Applicable, but no domain specific considerations.	FIPS 140-3 [NIST-SP800-53r5] AC-25, SA-10, SI-7, SR-9, SR-10
DS-8 Utility/Building Management System	This may include periodic testing of breaker functionality and regular maintenance and monitoring of energy infrastructure.	FIPS 140-3 [NIST-SP800-53r5] AC-25, SA-10, SI-7, SR-9, SR-10

660 **5.2.4. Information Protection and Processes Category**

661 Security policies (that address purpose, scope, roles, responsibilities, management commitment,
662 and coordination among organizational entities), processes, and procedures are maintained and
663 used to manage protection of information systems and assets.

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

666

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

Subcategory Domain	Applicability	Informative References
<p>IP-1: A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).</p>	<p>Ecosystem: The components within the IT and ICS systems should be configured in 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.</p>	<p>[NIST-SP800-53r5] CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10</p> <p>[NIST-SP800-137] Section D</p> <p>[NIST-SP800-160V1] 3.4.9, 3.4.10, 3.4.11, Appendix F, Appendix G</p> <p>NERC CIP 012-1-R1</p>
<p>IP-1 EV</p>	<p>Applicable, no domain specific considerations.</p>	<p>[NIST-SP800-53r5] CM-3, CM-5, CM-6, CM-7, CM-9</p> <p>[NIST-SP800-160V1] 3.4.9, 3.4.10, 3.4.11, Appendix F, Appendix G</p>
<p>IP-1 XFC/EVSE</p>	<p>Applicable, no domain specific considerations.</p>	<p>ISA 62443-2-1:D4E1 CM 1.3, CM 1.4</p> <p>ISA 62443-3-3:2013 SR 7.6</p> <p>OIML D 31 6.1.4.1</p>
<p>IP-1 Cloud/Third-Party</p>	<p>Applicable, no domain specific considerations.</p>	<p>[NIST-SP800-53r5] CM-3, CM-5, CM-6, CM-7, CM-9</p> <p>[NIST-SP800-160V1] 3.4.9, 3.4.10, 3.4.11, Appendix F, Appendix G</p>
<p>IP-1 Utility/Building Management System</p>	<p>Applicable, no domain specific considerations.</p>	<p>ISA 62443-2-1:D4E1 CM 1.3, CM 1.4</p> <p>ISA 62443-3-3:2013 SR 7.6</p>
<p>IP-2: A System Development Life Cycle to manage systems is implemented.</p>	<p>Ecosystem: SDLC planning may consider including security requirements, failure analyses, and preventative measures.</p>	<p>[NIST-SP800-53r5] SA-3, SA-4, SA-8, SA-10, SA-11</p> <p>[NIST-SP800-160V1] 3.2.1, Appendix F.3</p>

Subcategory Domain	Applicability	Informative References
IP-2 EV	This may include development systems and assets, OEM/owner information assets, and recommended/required replacement schedules.	[NIST-SP800-53r5] SA-3, SA-4, SA-8, SA-10, SA-11 [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 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 [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 62443-2-1:D4E1 ORG 1.1, ORG 2.3
IP-3: Configuration change control processes are in place.	Ecosystem: The ecosystem will employ configuration change control for the domain and elements that are 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. Organizations will provide 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 [NIST-SP800-137] Section D NERC CIP 007-6-R2 [NIST-SP800-160V1] 3.3.5, 3.8.3, 3.8.4
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
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 62443-2-1:D4E1 CM 1.3, CM 1.4 ISA 62443-3-3:2013 SR 7.6
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 62443-2-1:D4E1 CM 1.3, CM 1.4 ISA 62443-3-3:2013 SR 7.6

Subcategory Domain	Applicability	Informative References
<p>IP-4: Backups of information are conducted, maintained, and tested.</p>	<p>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 based on their business needs or compliance requirements.</p>	<p>[NIST-SP800-53r5] CP-4, CP-6, CP-9 NERC CIP 009-6-R1, 009-6-R2</p>
<p>IP-4 EV</p>	<p>Applicable, no domain specific considerations.</p>	<p>[NIST-SP800-53r5] CP-4, CP-6, CP-9</p>
<p>IP-4 XFC/EVSE</p>	<p>Applicable, no domain specific considerations.</p>	<p>ISA 62443-2-1:D4E1 AVAIL 2.1 ISA 62443-3-3:2013 SR 7.3, SR 7.4</p>
<p>IP-4 Cloud/Third-Party</p>	<p>Applicable, no domain specific considerations.</p>	<p>[NIST-SP800-53r5] CP-4, CP-6, CP-9</p>
<p>IP-4 Utility/Building Management System</p>	<p>Applicable, no domain specific considerations.</p>	<p>ISA 62443-2-1:D4E1 AVAIL 2.1 ISA 62443-3-3:2013 SR 7.3, SR 7.4</p>
<p>IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.</p>	<p>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.</p>	<p>[NIST-SP800-53r5] PE-1, PE-12, PE-13, PE-14 ISO/SAE 21434</p>
<p>IP-5 EV</p>	<p>This may include assets connected to, or accessible from, EVSE or Utility/Building assets (e.g., BESS, charging ports, system temperature/safety thresholds).</p>	<p>[NIST-SP800-53r5] PE-1, PE-12, PE-13, PE-14 ISO/SAE 21434</p>
<p>IP-5 XFC/EVSE</p>	<p>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.</p>	<p>ISA 62443-2-1:D4E1 ORG 3.1, AVAIL 1.2 NIST Handbook 44 3.40 S.3.3</p>
<p>IP-5 Cloud/Third-Party</p>	<p>This may include Cloud/Third-Party assets connected to utility/building assets.</p>	<p>[NIST-SP800-53r5] PE-1, PE-12, PE-13, PE-14</p>
<p>IP-5 Utility/Building Management System</p>	<p>This may include physical status indications (e.g., tamper alarms) for deployed equipment and panels.</p>	<p>ISA 62443-2-1:D4E1 ORG 3.1, AVAIL 1.2</p>

Subcategory Domain	Applicability	Informative References
<p>IP-6: Data is destroyed according to policy.</p>	<p>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 will conduct audits and reviews to ensure that data is destroyed according to policy. Consider reviewing data sanitization procedures and component disposal.</p>	<p>[NIST-SP800-53r5] MP-6, SR-12 NERC CIP 011-2-R2</p>
<p>IP-6 EV</p>	<p>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.</p>	<p>[NIST-SP800-53r5] MP-6, SR-12</p>
<p>IP-6 XFC/EVSE</p>	<p>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.</p>	<p>ISA 62443-2-1:D4E1 DATA 1.6 ISA 62443-3-3:2013 SR 4.2</p>
<p>IP-6 Cloud/Third-Party</p>	<p>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)).</p>	<p>[NIST-SP800-53r5] MP-6, SR-12</p>
<p>IP-6 Utility/Building Management System</p>	<p>Applicable, but no Utility/Building Management specific considerations.</p>	<p>ISA 62443-2-1:D4E1 DATA 1.6 ISA 62443-3-3:2013 SR 4.2</p>
<p>IP-7: Protection processes are improved.</p>	<p>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). Protection processes related to sensitive user data may be considered at a higher priority.</p>	<p>[NIST-SP800-53r5] CA-2, CA-7, CA-8, CP-2, CP-4, IR-3, IR-8, PL-2, PM-6 NERC CIP 009-6-R3</p>
<p>IP-7 EV</p>	<p>Protection processes related to safety critical systems may be considered at a higher priority. Manufacturers may consider implementing a database of past events to better track and manage events and corresponding improvement processes.</p>	<p>[NIST-SP800-53r5] CA-2, CA-7, CA-8</p>
<p>IP-7 XFC/EVSE</p>	<p>Protection processes related to safety critical systems may be considered at a higher priority. Owners/operators/manufacturers may consider implementing a database of past events to better track and manage events and corresponding improvement processes.</p>	<p>ISA 62443-2-1:D4E1 ORG 1.1</p>

Subcategory Domain	Applicability	Informative References
IP-7 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CA-2, CA-7, CA-8
IP-7 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	ISA 62443-2-1:D4E1 ORG 1.1
IP-8: Effectiveness of protection technologies is shared.	Ecosystem: Consider participation in collaborative forums such as the Electricity-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 [NIST-SP800-150] NERC CIP 009-6-R3
IP-8 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] IR-6 [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 62443-2-1:D4E1 ORG 1.1
IP-8 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] IR-6 [NIST-SP800-150]
IP-8 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	ISA 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.	IEC61850-90-12 5.8, 4.12-4.14 [NIST-SP800-53r5] CM-3, CM-4, SA-10 [NIST-SP800-61r2] Section D [NIST-SP800-160V1] 6.5, 6.6, Appendix F.2 NERC CIP 009-6-R1, 009-6-R3

Subcategory Domain	Applicability	Informative References
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.	<p>IEC61850-90-12 5.8, 4.12-4.14</p> <p>[NIST-SP800-53r5] CM-3, CM-4, SA-10</p> <p>[NIST-SP800-61r2] Section D</p> <p>[NIST-SP800-160V1] 6.5, 6.6, Appendix F.2</p>
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.	<p>ISA 62443-2-1:D4E1 EVENT 1.8, AVAIL 1.1</p> <p>NIST Handbook 44 3.40 S.2.3</p>
IP-9 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	<p>[NIST-SP800-53r5] CM-3, CM-4, SA-10</p> <p>[NIST-SP800-61r2] Section D</p> <p>[NIST-SP800-160V1] 6.5, 6.6, Appendix F.2</p>
IP-9 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	<p>ISA 62443-2-1:D4E1 EVENT 1.8, AVAIL 1.1</p>
IP-10: 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.	<p>IEC61850-90-4 14.2.4, 5.4.2.5</p> <p>[NERCGridEx]</p> <p>[NIST-SP800-53r5] CP-4, IR-3, PM-14</p> <p>[NIST-SP800-115]</p> <p>NISTIR-8270</p> <p>NERC CIP 009-6-R2</p>
IP-10 EV	Applicable, but no EV specific considerations.	<p>[NIST-SP800-53r5] CP-4, IR-3, PM-14</p> <p>[NIST-SP800-115]</p>
IP-10 XFC/EVSE	Applicable, but no EVSE specific considerations.	<p>ISA 62443-2-1:D4E1 EVENT 1.8, AVAIL 1.1</p> <p>ISA 62443-3-3:2013 SR 3.3</p>

Subcategory Domain	Applicability	Informative References
IP-10 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CP-4, IR-3, PM-14 [NIST-SP800-115]
IP-10 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 EVENT 1.8, AVAIL 1.1 ISA 62443-3-3:2013 SR 3.3
IP-11: 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] PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21 NERC CIP 004-6-R2, 004-6-R3, 004-6-R4, 004-6-R5
IP-11 EV	Applicable, but no EV 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 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 ORG 1.1, ORG 1.2
IP-11 Cloud/Third-Party	Applicable, but no 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 Utility/Building Management Systems specific considerations.	ISA 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)).	[CISA-CIVR-PB] Appendix A [NIST-SP800-53r5] RA-1, RA-3, RA-5, SI-2 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
IP-12 XFC/EVSE	This may include development systems, operational systems, and IT/ICS systems.	ISA 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

Subcategory Domain	Applicability	Informative References
IP-12 Utility/Building Management System	This may include development systems, operational systems, and IT/ICS systems.	ISA 62443-2-1:D4E1 EVENT 1.9

667 **5.2.5. Maintenance Category**

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

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

673 **Table 12.** Protect: Maintenance Category.

Subcategory Domain	Applicability	Informative References
MA-1: 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] MA-1, MA-2, MA-3, MA-5, MA-6 NERC CIP 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] 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 62443-2-1:D4E1 AVAIL 1.2
MA-1 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] MA-1, MA-2, MA-3, MA-5, MA-6
MA-1 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	ISA 62443-2-1:D4E1 AVAIL 1.2

Subcategory Domain	Applicability	Informative References
MA-2: 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 consider safety aspects of all systems that depend on or interact with the asset being worked on.	[NIST-SP800-53r5] MA-4 [NIST-SP800-161] V1 Appendix F1.14 NERC CIP 006-6-R3
MA-2 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] 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 62443-2-1:D4E1 ORG 3.1 [OIML D31:2019] 6.2.8.3
MA-2 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] MA-4
MA-2 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	ISA 62443-2-1:D4E1 ORG 3.1

674 **5.2.6. Protective Technology Category**

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

677 Much of the technology within the EV/XFC ecosystem is single purpose or unique to the
678 domains within the ecosystem. COTS security solutions may need modification or tuning to
679 function properly and avoid unintended consequences.

Table 13. Protect: Protective Technology Category.

Subcategory Domain	Applicability	Informative References
<p>PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.</p>	<p>Ecosystem: These logs may include information regarding asset access, modification, communications, data, or use.</p> <p>Logging all events is not practical; therefore, Audit logging should be 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.</p> <p>Wherever practical, logging and audit mechanisms should produce data elements in accordance with standard data formats to facilitate parsing and consumption by analytic teams.</p> <p>Consider maintaining audit logs for extended periods to support forensic analysis. Audit logging should be determined by risk tolerance and tailored by industry best practices.</p>	<p>[NIST-SP800-53r5] AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16</p> <p>[NIST-SP800-92]</p> <p>[NIST-SP800-161] 3.3.2, 3.3.5</p> <p>NERC CIP 006-6-R1</p>
<p>PT-1 EV</p>	<p>EV manufacturers can consider logging system status and health over time, including indicators such as battery health.</p>	<p>[NIST-SP800-53r5] AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16</p> <p>[NIST-SP800-92]</p>
<p>PT-1 XFC/EVSE</p>	<p>Logging calibration parameters, access, maintenance, and updates may be considered.</p>	<p>ISA 62443-2-1:D4E1 NET 1.10, DATA 1.1, EVENT 1.4, EVENT 1.7</p> <p>ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12</p> <p>NIST Handbook 44 3.40 S.3.3</p> <p>[OIML D31:2019] 6.2.8.4.6</p>
<p>PT-1 Cloud/Third-Party</p>	<p>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.</p>	<p>[NIST-SP800-53r5] AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16</p> <p>[NIST-SP800-92]</p>
<p>PT-1 Utility/Building Management System</p>	<p>Logging system historical demand as a function of time and location may be considered.</p>	<p>ISA 62443-2-1:D4E1 NET 1.10, DATA 1.1, EVENT 1.4, EVENT 1.7</p> <p>ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12</p>

Subcategory Domain	Applicability	Informative References
<p>PT-2: Removable media is protected, and its use restricted according to policy.</p>	<p>Ecosystem: Removable media includes hard drives, flash drives, CDs, DVDs, and SD cards. Authorized use practices will include encryption, access management, sanitization, and malware scanning when utilizing removable media to limit cybersecurity risks. Both physical and wireless access methods can be considered for removable media.</p>	<p>[NIST-SP800-53r5] MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 NERC CIP 006-6-R2, 007-6-R1</p>
<p>PT-2 EV</p>	<p>Removable media may include connections made through EV specific ports or hardware (e.g., OBD-II, CAN, Infotainment, etc.).</p>	<p>[NIST-SP800-53r5] MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8</p>
<p>PT-2 XFC/EVSE</p>	<p>Removable media may include EVSE specific ports or hardware (e.g., maintenance ports, maintenance service equipment, diagnostic equipment, etc.).</p>	<p>ISA 62443-2-1:D4E1 DATA 1.1, DATA 1.2 ISA 62443-3-3:2013 SR 2.3 NIST Handbook 44 1.10 G-S.8.2 [OIML G22:2022] 4.4.3.2.1, 4.4.3.2.3 [OIML D31:2019] 6.1.3.2.1, 6.1.3.2.4</p>
<p>PT-2 Cloud/Third-Party</p>	<p>Applicable, but no Cloud/Third-Party specific considerations.</p>	<p>[NIST-SP800-53r5] MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8</p>
<p>PT-2 Utility/Building Management System</p>	<p>Applicable, but no Utility/Building Management specific considerations.</p>	<p>ISA 62443-2-1:D4E1 DATA 1.1, DATA 1.2 ISA 62443-3-3:2013 SR 2.3</p>
<p>PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.</p>	<p>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 be deactivated.</p>	<p>NERC CIP 007-6-R1 [NIST-SP800-53r5] AC-2, AC-3, CM-7</p>
<p>PT-3 EV</p>	<p>Applicable, but no EV specific considerations.</p>	<p>[NIST-SP800-53r5] AC-2, AC-3, CM-7</p>

Subcategory Domain	Applicability	Informative References
PT-3 XFC/EVSE	Applicable, but no EVSE specific considerations.	<p>ISA 62443-2-1:D4E1 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</p> <p>ISA 62443-3-3:2013 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</p>
PT-3 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	<p>[NIST-SP800-53r5] AC-2, AC-3, CM-7</p>
PT-3 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	<p>ISA 62443-2-1:D4E1 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</p> <p>ISA 62443-3-3:2013 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</p>

Subcategory Domain	Applicability	Informative References
<p>PT-4: Communications and control networks are protected.</p>	<p>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.</p> <p>Implementing some security measures can lead to performance degradation. Organizations may verify that protective measures will not adversely affect overall system performance requirements.</p> <p>These network protections may consider following common IT or OT network protections, including firewalls, encryption, antivirus, etc.</p>	<p>NERC CIP 006-6-R1</p> <p>[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</p> <p>[NIST-SP800-160V1] Appendix F</p>
<p>PT-4 EV</p>	<p>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 networks 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.</p>	<p>[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</p>
<p>PT-4 XFC/EVSE</p>	<p>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 IoT, IIoT and Mesh networks.</p>	<p>ISA 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</p> <p>ISA 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</p> <p>[OIML D31:2019] 6.2.2.1.1, 6.2.5.2.d</p>
<p>PT-4 Cloud/Third-Party</p>	<p>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.</p>	<p>[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</p>

Subcategory Domain	Applicability	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 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 ISA 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: 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 EV specific considerations.	[NIST-SP800-53r5] CP-7, CP-8, CP-11, CP-12, CP-13
PT-5 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-3-3:2013 SR 7.1, SR 7.2
PT-5 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CP-7, CP-8, CP-11, CP-12, CP-13
PT-5 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	ISA 62443-3-3:2013 SR 7.1, SR 7.2

681 **5.3. Detect Function Considerations Across the EV/XFC Domains**

682 Develop and implement the appropriate activities to identify the occurrence of a cybersecurity
683 event. The activities in the Detect Function enable timely discovery of cybersecurity events.

- 684 • Anomalies and Events
- 685 • Security Continuous Monitoring
- 686 • Detection Processes

687 **5.3.1. Anomalies and Events**

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

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

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

Subcategory Domain	Applicability	Informative References
AE-1: 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 [NIST-SP800-92] [NIST-SP800-161] 3.3.2, 3.3.5
AE-1 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] AC-4, CA-3, CM-2, SC-16, SI-4
AE-1 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 NET 1.01
AE-1 Cloud/Third-Party	Cloud and third-party applications may consider 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 Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 NET 1.01
AE-2: Detected events are analyzed to understand attack targets and methods.	Ecosystem: Event analysis may utilize Cyber Threat Intelligence (CTI) sources, such as ISACs or vulnerability databases, to better understand and determine the impacts and attack vectors or vulnerabilities used during the event.	NERC CIP 007-6-R4 [NIST-SP800-53r5] AU-6, CA-7, IR-4, RA-5, SI-4 [NIST-SP800-128]
AE-2 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] AU-6, CA-7, IR-4, RA-5, SI-4
AE-2 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 EVENT 1.7 ISA 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

Subcategory Domain	Applicability	Informative References
AE-2 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] AU-6, CA-7, IR-4, RA-5, SI-4 [NIST-SP800-128]
AE-2 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 EVENT 1.7 ISA 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. Event data should be collected from all networks, systems, and communication ns effected 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.	NERC CIP 007-6-R4 [NIST-SP800-53r5] AU-6, CA-7, CP-2, IR-4, IR-5, IR-8, SI-4 [NIST-SP800-160V1] 3.3.7, Appendix G.2, Appendix G.3
AE-3 EV	Important EV-specific data collected may include 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 62443-2-1:D4E1 EVENT 1.7 ISA 62443-3-3:2013 SR 6.1
AE-3 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] IR-4, IR-5, IR-8
AE-3 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 EVENT 1.7 ISA 62443-3-3:2013 SR 6.1
AE-4: 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 [NIST-SP800-61r2]
AE-4 EV	Applicable, but no EV specific considerations.	ISO/SAE 21434 15.1
AE-4 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 EVENT 1.8

Subcategory Domain	Applicability	Informative References
AE-4 Cloud/Third-Party	Applicable, but no 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 Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 EVENT 1.8
AE-5: 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. This should include the creation and updating of threshold criteria. EV/XFC ecosystem members can consider integrating operational limits into alert thresholds.	NERC CIP 007-6-R4, 007-6-R5 [NIST-SP800-53r5] IR-4, IR-5, IR-8
AE-5 EV	Applicable, but no EV specific considerations.	ISO/SAE 21434 Clause 8 and clause 12
AE-5 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 EVENT 1.1, EVENT 1.7
AE-5 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] IR-4, IR-5, IR-8
AE-5 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 EVENT 1.1, EVENT 1.7

693 **5.3.2. Security Continuous Monitoring**

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

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

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

Subcategory Domain	Applicability	Informative References
CM-1: 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.	NERC CIP 006-6-R1, 006-6-R2 [NIST-IR7800] [NIST-SP800-53r5] AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16

Subcategory Domain	Applicability	Informative References
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 62443-2-1:D4E1 EVENT 1.1 ISA 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 62443-2-1:D4E1 EVENT 1.1 ISA 62443-3-3:2013 SR 6.2
CM-2: 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, etc.) critical to the function of onboard controllers and management systems may be included in the continuous monitoring of the physical environment.	[NIST-SP800-53r5] 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] PE-6, PE-20

Subcategory Domain	Applicability	Informative References
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 62443-2-1:D4E1 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] PE-6, PE-20
CM-2 Utility/Building Management System	This may include monitoring 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 62443-2-1:D4E1 EVENT 1.1
CM-3: 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.	NERC CIP 006-6-R1, 007-6-R4, 007-6-R5 [NIST-SP800-53r5] AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
CM-3 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] AC-2, AU-12, AU-13
CM-3 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 EVENT 1.1 ISA 62443-3-3:2013 SR 6.2
CM-3 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] AC-2, AU-12, AU-13
CM-3 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 EVENT 1.1 ISA 62443-3-3:2013 SR 6.2
CM-4: Malicious code is detected.	Ecosystem: Detection activities may incorporate commonly used Tactics, Techniques, and Procedures (TTPs), unauthorized code execution, and/or unusual system activity.	NERC CIP 007-6-R3 [NIST-SP800-53r5] SC-44, SI-3, SI-4, SI-8 [NIST-SP800-218]
CM-4 EV	EV manufacturers can consider providing means or ensuring the ability to analyze and detect malicious code affecting software and firmware on EV computer systems that may include the vehicle's control units, communication modules, charging systems, and battery management systems.	[NIST-SP800-53r5] SI-3, SI-4, SI-8

Subcategory Domain	Applicability	Informative References
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 62443-2-1:D4E1 COMP 2.2 ISA 62443-3-3:2013 SR 3.2
CM-4 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] SI-3, SI-4, SI-8
CM-4 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 COMP 2.2 ISA 62443-3-3:2013 SR 3.2
CM-5: Unauthorized mobile code is detected.	Ecosystem: Mobile code include 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.	NERC CIP 007-6-R3 [NIST-SP800-53r5] SC-18, SC-44, SI-4
CM-5 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] SC-18, SC-44
CM-5 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 USER 1.06, EVENT 1.1 ISA 62443-3-3:2013 SR 2.4
CM-5 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] SC-18, SC-44
CM-5 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 USER 1.06, EVENT 1.1 ISA 62443-3-3:2013 SR 2.4
CM-6: External service provider activity is monitored to detect potential cybersecurity events.	Ecosystem: Directly applicable to the EV/XFC ecosystem. The ecosystem comprises of four distinct domains that require a level of service from each other to function.	NERC CIP 006-6-R1, 007-6-R4, 007-6-R5 [NIST-SP800-53r5] CA-7, PS-7, SA-4, SA-9, SI-4
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

Subcategory Domain	Applicability	Informative References
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 62443-2-1:D4E1 ORG 1.1, ORG 1.3
CM-6 Cloud/Third-Party	Applicable, but no 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 Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 ORG 1.1, ORG 1.3
CM-7: 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.	NERC CIP 006-6-R1, 007-6-R3, 005-6-R4, 007-6-R5 [NIST-SP800-53r5] AU-12, CA-7, CM-3, CM-8, PE-6, PE-20, SI-4
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] CM-3, CM-8, PE-6, PE-20
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 62443-2-1:D4E1 ORG 2.2, EVENT 1.1
CM-7 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CM-3, CM-8, PE-6, PE-20
CM-7 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 ORG 2.2, EVENT 1.1
CM-8: 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] RA-5 [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] RA-5 [NIST-SP800-115]

Subcategory Domain	Applicability	Informative References
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 62443-2-1:D4E1 ORG 2.2, EVENT 1.1
CM-8 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] RA-5 [NIST-SP800-115]
CM-8 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 ORG 2.2, EVENT 1.1

699 **5.3.3. Detection Processes**

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

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

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

Subcategory Domain	Applicability	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 EV specific considerations.	[NIST-SP800-53r5] CA-2, CA-7
DP-1 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 ORG 1.3
DP-1 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CA-2, CA-7
DP-1 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 ORG 1.3

Subcategory Domain	Applicability	Informative References
<p>DP-2: Detection activities comply with all applicable requirements.</p>	<p>Ecosystem: Activities and requirements include (but are not limited to) policy, contractual, regulation, and legal requirements.</p>	<p>NERC CIP 007-6-R4</p> <p>[NIST-SP800-53r5] 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</p> <p>[NIST-SP800-61r2]</p>
<p>DP-2 EV</p>	<p>Applicable, but no EV specific considerations.</p>	<p>[NIST-SP800-53r5] SI-1, SI-4, SR-1, SR-9, SR-10</p>
<p>DP-2 XFC/EVSE</p>	<p>Applicable, but no EVSE specific considerations.</p>	<p>ISA 62443-2-1:D4E1 EVENT 1.1</p>
<p>DP-2 Cloud/Third-Party</p>	<p>Applicable, but no Cloud/Third-Party specific considerations.</p>	<p>[NIST-SP800-53r5] SI-1, SI-4, SR-1, SR-9, SR-10</p>
<p>DP-2 Utility/Building Management System</p>	<p>Applicable, but no Utility/Building Management Systems specific considerations.</p>	<p>ISA 62443-2-1:D4E1 EVENT 1.1</p>
<p>DP-3: Detection processes are tested.</p>	<p>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.</p>	<p>NERC CIP 006-6-R3</p> <p>[NIST-SP800-53r5] CA-2, CA-7. PM-14, SI-3, SI-4</p>
<p>DP-3 EV</p>	<p>Applicable, but no EV specific considerations.</p>	<p>[NIST-SP800-53r5] CA-2, CA-7. PM-14, SI-3, SI-4</p>
<p>DP-3 XFC/EVSE</p>	<p>Applicable, but no EVSE specific considerations.</p>	<p>ISA 62443-2-1:D4E1 EVENT 1.1</p> <p>ISA 62443-3-3:2013 SR 3.3</p>
<p>DP-3 Cloud/Third-Party</p>	<p>Applicable, but no Cloud/Third-Party specific considerations.</p>	<p>[NIST-SP800-53r5] CA-2, CA-7. PM-14, SI-3, SI-4</p>
<p>DP-3 Utility/Building Management System</p>	<p>Applicable, but no Utility/Building Management Systems specific considerations.</p>	<p>ISA 62443-2-1:D4E1 EVENT 1.1</p> <p>ISA 62443-3-3:2013 SR 3.3</p>

Subcategory Domain	Applicability	Informative References
DP-4: 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.	NERC CIP 008-6-R4 [NIST-SP800-53r5] AU-6, CA-2, CA-7, RA-5, SI-4
DP-4 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] AU-6, CA-2, CA-7
DP-4 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 EVENT 1.2 ISA 62443-3-3:2013 SR 6.1
DP-4 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] AU-6, CA-2, CA-7
DP-4 Utility/Building Management System	Applicable, but no Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 EVENT 1.2 ISA 62443-3-3:2013 SR 6.1
DP-5: 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 EV specific considerations.	[NIST-SP800-53r5] CA-2, CA-7, PL-2, PM-14, RA-5
DP-5 XFC/EVSE	Applicable, but no EVSE specific considerations.	ISA 62443-2-1:D4E1 ORG 1.1
DP-5 Cloud/Third-Party	Applicable, but no 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 Utility/Building Management Systems specific considerations.	ISA 62443-2-1:D4E1 ORG 1.1

706 **5.4. Respond Function Considerations Across the EV/XFC Domains**

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

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

- 713 The objectives of the Response Function are to:
- 714 • Contain events using a verified response procedure.
 - 715 • Communicate the occurrence and impact of the incident to operations and relevant
 - 716 parties.
 - 717 • Develop processes to respond to and mitigate new known or anticipated threats or
 - 718 vulnerabilities.
 - 719 • Evolve response strategies and plans based on lessons learned.

720 **5.4.1. Analysis**

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

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

723 responses.

724 **Table 17.** Respond: Analysis Category.

Subcategory Domain	Applicability	Informative References
AN-1: 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 be used as a tool in system diagnosis, event/incident response and mitigations.	[NIST-SP800-53r5] AU-6, CA-7, IR-4, IR-5, PE-6, RA-5, SI-4
AN-1 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] CA-7, IR-5, SI-4
AN-1 XFC/EVSE	Applicable, but no EVSE specific considerations.	[NIST-SP800-53r5] CA-7, IR-5, SI-4 [ISA 62443-2-1:D4E1] ORG 1.1, EVENT 1.7, EVENT 1.8 [ISA 62443-3-3:2013] SR 6.1
AN-1 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CA-7, IR-5, SI-4
AN-1 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NIST-SP800-53r5] CA-7, IR-5, SI-4 [ISA 62443-2-1:D4E1] ORG 1.1, EVENT 1.7, EVENT 1.8 [ISA 62443-3-3:2013] SR 6.1

Subcategory Domain	Applicability	Informative References
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 [NIST-SP800-61r2] 3
AN-2 EV	Impacts to safety critical systems and components should be treated as high priority or understood in greater detail.	[NIST-SP800-53r5] CP-2, IR-4, RA-3 [NIST-SP800-61r2] 3.2.4
AN-2 XFC/EVSE	Impacts to safety critical systems and components should be treated as high priority or understood in greater detail.	[NIST-SP800-53r5] CP-2, IR-4, RA-3 [NIST-SP800-61r2] 3.2.4 [ISA 62443-2-1:D4E1] ORG 1.1, EVENT 1.7
AN-2 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CP-2, IR-4, RA-3
AN-2 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NIST-SP800-53r5] CP-2, IR-4, RA-3 [ISA 62443-2-1:D4E1] ORG 1.1, EVENT 1.7
AN-3: Forensics are performed.	Ecosystem: Forensics provide information that aids in the selection of response actions and informs improvements for future response plans.	NERC CIP 009-6-R1 [NIST-SP800-53r5] AU-7, IR-4 [NIST-SP800-61r2] 2.4.2, 2.4.3, 3.1.1
AN-3 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] IR-4 [NIST-SP800-61r2] 2.4.2, 2.4.3, 3.1.1
AN-3 XFC/EVSE	Applicable, but no EVSE specific considerations.	[NIST-SP800-53r5] IR-4 [NIST-SP800-61r2] 2.4.2, 2.4.3, 3.1.1 [ISA 62443-2-1:D4E1] EVENT 1.7 [ISA 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 Cloud/Third-Party specific considerations.	[NIST-SP800-61r2] 2.4.2, 2.4.3, 3.1.1

Subcategory Domain	Applicability	Informative References
AN-3 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	<p>[NIST-SP800-61r2] 2.4.2, 2.4.3, 3.1.1</p> <p>[ISA 62443-2-1:D4E1] EVENT 1.7</p> <p>[ISA 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</p>
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.	<p>[NIST-SP800-53r5] CP-2, IR-4, IR-5, IR-8, RA-3</p> <p>[NIST-SP800-61r2] 2, 3.2</p>
AN-4 EV	Applicable, but no EV specific considerations.	<p>[NIST-SP800-53r5] IR-4, IR-5, IR-8, RA-3</p> <p>[NIST-SP800-61r2] 2</p>
AN-4 XFC/EVSE	Applicable, but no EVSE specific considerations.	<p>[NIST-SP800-53r5] IR-4, IR-5, IR-8, RA-3</p> <p>[NIST-SP800-61r2] 2</p> <p>[ISA 62443-2-1:D4E1] EVENT 1.7</p>
AN-4 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	<p>[NIST-SP800-53r5] IR-4, IR-5, IR-8, RA-3</p> <p>[NIST-SP800-61r2] 2</p>
AN-4 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	<p>[NIST-SP800-53r5] IR-4, IR-5, IR-8, RA-3</p> <p>[NIST-SP800-61r2] 2</p> <p>[ISA 62443-2-1:D4E1] EVENT 1.7</p>

Subcategory Domain	Applicability	Informative References
<p>AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).</p>	<p>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.</p>	<p>[DHS-NCCIC] NERC CIP 007-6-R2 [NIST-SP800-53r5] CA-1, CA-2, PM-4, PM-15, RA-1, RA-7, SI-5, SR-6 [NIST-SP800-61r2] 3, 3.2 [NIST-SP800-160V1] 3.4.9, 3.4.11</p>
<p>AN-5 EV</p>	<p>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.</p>	<p>[DHS-NCCIC] [NIST-SP800-53r5] CA-1, CA-2, RA-1, RA-7, SI-5, SR-6 [NIST-SP800-61r2] 3</p>
<p>AN-5 XFC/EVSE</p>	<p>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.</p>	<p>[NIST-SP800-53r5] CA-1, CA-2, RA-1, RA-7, SI-5, SR-6 [NIST-SP800-61r2] 3</p>
<p>AN-5 Cloud/Third-Party</p>	<p>Applicable, but no Cloud/Third-Party specific considerations.</p>	<p>[DHS-NCCIC] [NIST-SP800-53r5] CA-1, CA-2, RA-1, RA-7, SI-5, SR-6 [NIST-SP800-61r2] 3</p>
<p>AN-5 Utility/Building Management System</p>	<p>Applicable, but no Utility/Building Management specific considerations.</p>	<p>[DHS-NCCIC] [NIST-SP800-53r5] CA-1, CA-2, RA-1, RA-7, SI-5, SR-6 [NIST-SP800-61r2] 3</p>

725 **5.4.2. Communications**

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

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

Table 18. Respond: Communications Category.

Subcategory Domain	Applicability	Informative References
<p>CO-1: Personnel know their roles and order of operations when a response is needed.</p>	<p>Ecosystem: The efficacy and timeliness of the response depends on how well the 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.</p>	<p>NERC CIP 009-6-R2 [NIST-SP800-34r1] [NIST-SP800-53r5] CP-2, CP-3, IR-3, IR-8 [NIST-SP800-61r2] Appendix A, 2.4</p>
<p>CO-1 EV</p>	<p>Applicable, no EV specific considerations.</p>	<p>[NIST-SP800-53r5] CP-3, IR-8 [NIST-SP800-61r2] Appendix A, 2.4</p>
<p>CO-1 XFC/EVSE</p>	<p>Applicable, no EVSE specific considerations.</p>	<p>[NIST-SP800-53r5] CP-3, IR-8 [NIST-SP800-61r2] Appendix A, 2.4 [ISA 62443-2-1:D4E1] ORG 1.3, EVENT 1.8</p>
<p>CO-1 Cloud/Third-Party</p>	<p>Applicable, no Cloud/Third-Party specific considerations.</p>	<p>[NIST-SP800-53r5] CP-3, IR-8</p>
<p>CO-1 Utility/Building Management System</p>	<p>Utility/Building Management Systems: Applicable, no Utility/Building Management specific considerations.</p>	<p>[NIST-SP800-34r1] [NIST-SP800-53r5] CP-3, IR-8 [NIST-SP800-61r2] Appendix A [ISA 62443-2-1:D4E1] ORG 1.3, EVENT 1.8</p>
<p>CO-2: Incidents are reported, consistent with established criteria.</p>	<p>Ecosystem: The reporting typically includes internal and the appropriate external relevant parties. The reporting can be done in a manner that is consistent with pre-defined thresholds and will initiate the response in a timely manner.</p>	<p>[NERC-CIP-008-6] [NIST-SP800-53r5] AU-6, IR-6, IR-8 [NIST-SP800-61r2] 4</p>
<p>CO-2 EV</p>	<p>Applicable, no EV specific considerations.</p>	<p>[NERC-CIP-008-6] [NIST-SP800-53r5] IR-6, IR-8</p>
<p>CO-2 XFC/EVSE</p>	<p>Applicable, no EVSE specific considerations.</p>	<p>[NERC-CIP-008-6] [NIST-SP800-53r5] IR-6, IR-8 [ISA 62443-2-1:D4E1] ORG 1.1, EVENT 1.2</p>

Subcategory Domain	Applicability	Informative References
CO-2 Cloud/Third-Party	Applicable, no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] IR-6, IR-8 [NIST-SP800-61r2] Appendix A
CO-2 Utility/Building Management System	Applicable, no Utility/Building Management specific considerations.	[NIST-SP800-53r5] IR-6, IR-8 [NIST-SP800-61r2] Appendix A [ISA 62443-2-1:D4E1] ORG 1.1, EVENT 1.2
CO-3: 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. Organizations may coordinate with law enforcement and regulatory officials where applicable. Consider sharing with industry groups, ISAC, or other consortia to increase cyber situational awareness.	[NIST-SP800-53r5] CP-2, IR-4, IR-8 [NIST-SP800-61r2] 2.4
CO-3 EV	Applicable, no EV specific considerations.	[NIST-SP800-53r5] CP-2, IR-4 [NIST-SP800-61r2] 2.4
CO-3 XFC/EVSE	Applicable, no EVSE specific considerations.	[NIST-SP800-53r5] CP-2, IR-4 [NIST-SP800-61r2] 2.4 [ISA 62443-2-1:D4E1] EVENT 1.2
CO-3 Cloud/Third-Party	Applicable, no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CP-2, IR-4
CO-3 Utility/Building Management System	Applicable, no Utility/Building Management specific considerations.	[NIST-SP800-53r5] CP-2, IR-4 [ISA 62443-2-1:D4E1] EVENT 1.2
CO-4: 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 [NIST-SP800-61r2] 2.3.4

Subcategory Domain	Applicability	Informative References
CO-4 EV	Applicable, no EV specific considerations.	[NIST-SP800-53r5] CP-2, IR-8 [NIST-SP800-61r2] 2.3.4
CO-4 XFC/EVSE	Applicable, no EVSE specific considerations.	[NIST-SP800-53r5] CP-2, IR-8 [NIST-SP800-61r2] 2.3.4 [ISA 62443-2-1:D4E1] EVENT 1.2
CO-4 Cloud/Third-Party	Applicable, no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CP-2, IR-8 [NIST-SP800-61r2] 2.3.4
CO-4 Utility/Building Management System	Applicable, no Utility/Building Management specific considerations.	[NIST-SP800-53r5] CP-2, IR-8 [NIST-SP800-61r2] 2.3.4 [ISA 62443-2-1:D4E1] EVENT 1.2
CO-5: 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 EV specific considerations.	[NIST-SP800-53r5] PM-15, PM-16, SI-5
CO-5 XFC/EVSE	Applicable, but no EVSE specific considerations.	[NIST-SP800-53r5] PM-15, PM-16, SI-5
CO-5 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] PM-15, PM-16, SI-5
CO-5 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NIST-SP800-53r5] PM-15, PM-16, SI-5

731 **5.4.3. Improvements Category**

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

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

736 **Table 19.** Respond: Improvements Category.

Subcategory Domain	Applicability	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 [NIST-SP800-61r2] 3.4.1
IM-1 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] CP-2, IR-4, IR-8 [NIST-SP800-61r2] 3.4.1
IM-1 XFC/EVSE	Applicable, but no EVSE specific considerations.	[NIST-SP800-53r5] CP-2, IR-4, IR-8 [NIST-SP800-61r2] 3.4.1 [ISA 62443-2-1:D4E1] EVENT 1.8
IM-1 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CP-2, IR-4, IR-8 [NIST-SP800-61r2] 3.4.1
IM-1 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NIST-SP800-53r5] CP-2, IR-4, IR-8 [NIST-SP800-61r2] 3.4.1 [ISA 62443-2-1:D4E1] EVENT 1.8
IM-2: Response strategies are updated.	Ecosystem: This may include updating response plans periodically, around major events, or an initial update.	[NIST-SP800-53r5] CP-2, IR-4, IR-8
IM-2 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] CP-2, IR-4, IR-8
IM-2 XFC/EVSE	Applicable, but no EVSE specific considerations.	[NIST-SP800-53r5] CP-2, IR-4, IR-8 [ISA 62443-2-1:D4E1] EVENT 1.8

Subcategory Domain	Applicability	Informative References
IM-2 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CP-2, IR-4, IR-8
IM-2 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NIST-SP800-53r5] CP-2, IR-4, IR-8 [ISA 62443-2-1:D4E1] EVENT 1.8

737 **5.4.4. Mitigation**

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

739 Mitigation is not unique to the EV/XFC ecosystem, and like other ecosystems, timely mitigation

740 will minimize the overall impact of the incident.

741 **Table 20.** Respond: Mitigation Category.

Subcategory Domain	Applicability	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 [NIST-SP800-61r2] 3.4.1
MI-1 EV	Applicable, but no EVSE specific considerations.	[NIST-SP800-53r5] IR-4 [NIST-SP800-61r2] 3.3, 3.3.1
MI-1 XFC/EVSE	Applicable, but no EVSE specific considerations.	[NIST-SP800-53r5] IR-4 [NIST-SP800-61r2] 3.3, 3.4.1 [ISA 62443-2-1:D4E1] NET 1.01, NET 1.04, NET 1.06, EVENT 1.8 [ISA 62443-3-3:2013] SR 5.1, SR 5.2, SR 5.4
MI-1 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] IR-4 [NIST-SP800-61r2] 3.3, 3.4.1

Subcategory Domain	Applicability	Informative References
MI-1 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	<p>[NIST-SP800-53r5] IR-4</p> <p>[NIST-SP800-61r2] 3.3, 3.4.1</p> <p>[ISA 62443-2-1:D4E1] NET 1.01, NET 1.04, NET 1.06, EVENT 1.8</p> <p>[ISA 62443-3-3:2013] SR 5.1, SR 5.2, SR 5.4</p>
MI-2: 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.	<p>[NIST-SP800-53r5] IR-4</p> <p>[NIST-SP800-61r2] 3.3.1</p>
MI-2 EV	Applicable, but no EVSE specific considerations.	<p>[NIST-SP800-53r5] IR-4</p> <p>[NIST-SP800-61r2] 3.3.1</p>
MI-2 XFC/EVSE	Applicable, but no EVSE specific considerations.	<p>[NIST-SP800-53r5] IR-4</p> <p>[NIST-SP800-61r2] 3.3.1</p> <p>[ISA 62443-2-1:D4E1] NET 1.01, NET 1.05, NET 1.06, COMP 2.2</p>
MI-2 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	<p>[NIST-SP800-53r5] IR-4</p> <p>[NIST-SP800-61r2] 3.3.1</p>
MI-2 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	<p>[NIST-SP800-53r5] IR-4</p> <p>[NIST-SP800-61r2] 3.3.1</p> <p>[ISA 62443-2-1:D4E1] NET 1.01, NET 1.05, NET 1.06, COMP 2.2</p>
MI-3: 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.	<p>[NIST-SP800-53r5] CA-2, CA-7, RA-3, RA-5, RA-7</p> <p>[NIST-SP800-61r2] 3.4</p>

Subcategory Domain	Applicability	Informative References
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 [NIST-SP800-61r2] 3.4
MI-3 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, priority updates.	[NIST-SP800-53r5] CA-2, RA-3, RA-5, RA-7 [NIST-SP800-61r2] 3.4 [ISA 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 [NIST-SP800-61r2] 3.4
MI-3 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NIST-SP800-53r5] CA-2, RA-3, RA-5, RA-7 [NIST-SP800-61r2] 3.4 [ISA 62443-2-1:D4E1] EVENT 1.9

742 **5.4.5. Response Planning**

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

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

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

Subcategory Domain	Applicability	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, no EV specific considerations.	[NIST-SP800-53r5] CP-10, IR-4

Subcategory Domain	Applicability	Informative References
RP-1 XFC/EVSE	Applicable, no EVSE specific considerations.	[NIST-SP800-53r5] CP-2, CP-10, IR-4
RP-1 Cloud/Third-Party	Applicable, no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CP-10, IR-4
RP-1 Utility/Building Management System	Applicable, no Utility/Building Management specific considerations.	[NIST-SP800-34r1] [NIST-SP800-53r5] CP-2, CP-10, IR-4

749 **5.5. Recover Function Considerations Across the EV/XFC Domains**

750 Develop and implement the appropriate activities to maintain plans for resilience and to restore
751 any capabilities or services that were impaired due to a cybersecurity event. The activities in the
752 Recover Function support timely recovery to normal operations to reduce the impact from a
753 cybersecurity event. Examples of outcome categories within this function include:

- 754 • Recovery Planning
- 755 • Improvements
- 756 • Communications

757 **5.5.1. Communications**

758 Restoration activities are coordinated with internal and external parties (e.g., coordinating
759 centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and
760 vendors).

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

764 **Table 22.** Recover: Communications Category.

Subcategory Domain	Applicability	Informative References
CO-1: 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 [NIST-SP800-61r2] 4.1

Subcategory Domain	Applicability	Informative References
CO-1 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] IR-4 [NIST-SP800-61r2] 4.1
CO-1 XFC/EVSE	Applicable, but no EVSE specific considerations.	[NIST-SP800-53r5] IR-4 [NIST-SP800-61r2] 4.1
CO-1 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] IR-4 [NIST-SP800-61r2] 4.1
CO-1 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NIST-SP800-53r5] IR-4 [NIST-SP800-61r2] 4.1
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.	[NERC-CIP-008-6] [NIST-SP800-53r5] AU-6, IR-6, IR-8 [NIST-SP800-61r2] 4
CO-2 EV	Applicable, but no EV specific considerations.	[NERC-CIP-008-6] [NIST-SP800-53r5] AU-6, IR-6, IR-8 [NIST-SP800-61r2] 4
CO-2 XFC/EVSE	Applicable, but no EVSE specific considerations.	[NERC-CIP-008-6] [NIST-SP800-53r5] AU-6, IR-6, IR-8 [NIST-SP800-61r2] 4
CO-2 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NERC-CIP-008-6] [NIST-SP800-53r5] AU-6, IR-6, IR-8 [NIST-SP800-61r2] 4

Subcategory Domain	Applicability	Informative References
CO-2 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NERC-CIP-008-6] [NIST-SP800-53r5] AU-6, IR-6, IR-8 [NIST-SP800-61r2] 4
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.	NERC CIP 009-6-R3 [NIST-SP800-53r5] CP-2, IR-4, IR-8 [NIST-SP800-61r2] 3.4
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
CO-3 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CP-2, IR-4, IR-8 [NIST-SP800-61r2] 3.4
CO-3 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NIST-SP800-53r5] CP-2, IR-4, IR-8 [NIST-SP800-61r2] 3.4

765 **5.5.2. Improvements**

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

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

Table 23. Recover: Improvements Category.

Subcategory Domain	Applicability	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.	NERC CIP 009-6-R3 [NIST-SP800-53r5] CP-2, IR-4, IR-8 [NIST-SP800-61r2] 3.4.1
IM-1 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] CP-2, IR-4 [NIST-SP800-61r2] 3.4.1
IM-1 XFC/EVSE	Applicable, but no EVSE specific considerations.	[NIST-SP800-53r5] CP-2, IR-4 [NIST-SP800-61r2] 3.4.1 [ISA 62443-2-1:D4E1] EVENT 1.8, AVAIL 1.1
IM-1 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CP-2, IR-4 [NIST-SP800-61r2] 3.4.1
IM-1 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NIST-SP800-53r5] CP-2, IR-4 [NIST-SP800-61r2] 3.4.1 [ISA 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 [NIST-SP800-61r2] 3.4, 3.4.1
IM-2 EV	Applicable, but no EV specific considerations.	[NIST-SP800-53r5] CP-2, IR-4 [NIST-SP800-61r2] 3.4.1
IM-2 XFC/EVSE	Applicable, but no EVSE specific considerations.	[NIST-SP800-53r5] CP-2, IR-4 [NIST-SP800-61r2] 3.4.1 [ISA 62443-2-1:D4E1] EVENT 1.8, AVAIL 1.1

Subcategory Domain	Applicability	Informative References
IM-2 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] CP-2, IR-4 [NIST-SP800-61r2] 3.4.1
IM-2 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NIST-SP800-53r5] CP-2, IR-4 [NIST-SP800-61r2] 3.4.1 [ISA 62443-2-1:D4E1] EVENT 1.8, AVAIL 1.1

771 **5.5.3. Recovery Planning**

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

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

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

Subcategory Domain	Applicability	Informative References
RP-1: 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] [NIST-SP800-53r5] CP-10, IR-4, IR-8 [NIST-SP800-160V1] 3.4.11, Appendix F.2.6 [NIST-SP800-184] 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 [NIST-SP800-184]
RP-1 XFC/EVSE	Recovery plans may consider including 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 [NIST-SP800-184] [ISA 62443-2-1:D4E1] EVENT 1.8

Subcategory Domain	Applicability	Informative References
RP-1 Cloud/Third-Party	Applicable, but no Cloud/Third-Party specific considerations.	[NIST-SP800-53r5] IR-4, IR-8 [NIST-SP800-184]
RP-1 Utility/Building Management System	Applicable, but no Utility/Building Management specific considerations.	[NIST-SP800-34r1] [NIST-SP800-53r5] IR-4, IR-8 [NIST-SP800-184] [ISA 62443-2-1:D4E1] EVENT 1.8

778 **References**

- 779 [ATIS-I-0000070] Alliance for Telecommunications Industry Solutions (2018) *Context-*
780 *Aware Identity Management Framework*, ATIS-I-0000070 (ATIS,
781 Washington, DC). Available at
782 [https://access.atis.org/apps/group_public/download.php/43565/ATIS-](https://access.atis.org/apps/group_public/download.php/43565/ATIS-I0000070.pdf)
783 [I0000070.pdf](https://access.atis.org/apps/group_public/download.php/43565/ATIS-I0000070.pdf)
- 784 [Auto-ISAC] Automotive Information Sharing and Analysis Center. Available at:
785 <https://automotiveisac.com/>
- 786 [CISA-CIVR-PB] Cybersecurity and Infrastructure Security Agency (2021) *Cybersecurity*
787 *Incident & Vulnerability Response Playbooks: Operational Procedures*
788 *for Planning and Conducting Cybersecurity Incident and Vulnerability*
789 *Response Activities in FCEB Information Systems*. (CISA, Washington,
790 DC). Available at
791 [https://www.cisa.gov/sites/default/files/publications/Federal Governmen](https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf)
792 [t_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508](https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf)
793 [C.pdf](https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf)
- 794 [CISA-ICS] Cybersecurity and Infrastructure Security Agency (2020) *Industrial*
795 *Control Systems*. (CISA, Washington, DC). Available at [https://us-](https://us-cert.cisa.gov/ics)
796 [cert.cisa.gov/ics](https://us-cert.cisa.gov/ics)
- 797 [CISA-RFI-BPG] Cybersecurity and Infrastructure Security Agency and
798 SAFECOM/National Council of Statewide Interoperability Coordinators
799 (2020) *Radio Frequency Interference Best Practices Guidebook*. (CISA,
800 Washington, DC). Available at
801 [https://www.cisa.gov/sites/default/files/publications/safecom-](https://www.cisa.gov/sites/default/files/publications/safecom-ncswic_rf_interference_best_practices_guidebook_2.7.20_-_final_508c.pdf)
802 [ncswic_rf_interference_best_practices_guidebook_2.7.20 -](https://www.cisa.gov/sites/default/files/publications/safecom-ncswic_rf_interference_best_practices_guidebook_2.7.20_-_final_508c.pdf)
803 [_final_508c.pdf](https://www.cisa.gov/sites/default/files/publications/safecom-ncswic_rf_interference_best_practices_guidebook_2.7.20_-_final_508c.pdf)
- 804 [DHS-NCCIC] Department of Homeland Security (2012) *National Cybersecurity &*
805 *Communications Integration Center (NCCIC) Overview*. (DHS,
806 Washington, DC). Available at
807 [https://csrc.nist.gov/CSRC/media/Events/ISPAB-OCTOBER-](https://csrc.nist.gov/CSRC/media/Events/ISPAB-OCTOBER-2012MEETING/documents/ispab_oct2012_lzelvin_nccic-overview.pdf)
808 [2012MEETING/documents/ispab_oct2012_lzelvin_nccic-overview.pdf](https://csrc.nist.gov/CSRC/media/Events/ISPAB-OCTOBER-2012MEETING/documents/ispab_oct2012_lzelvin_nccic-overview.pdf)
- 809 [EEI-2022] Scruggs T (2022) “EEI Projects 26.4 Million Electric Vehicles Will Be
810 on U.S. Roads in 2030”. Edison Electric Institute. June 20, 2022.
811 Available at: [https://www.eei.org/News/news/All/eei-projects-26-](https://www.eei.org/News/news/All/eei-projects-26-million-electric-vehicles-will-be-on-us-roads-in-2030)
812 [million-electric-vehicles-will-be-on-us-roads-in-2030](https://www.eei.org/News/news/All/eei-projects-26-million-electric-vehicles-will-be-on-us-roads-in-2030)
- 813 [E-ISAC] Electricity information Sharing and Analysis Center. Available at:
814 <https://www.eisac.com/s/>
- 815 [EO.13636] The White House, Office of the Press Secretary. “Executive Order --
816 *Improving Critical Infrastructure Cybersecurity*”. February 12, 2013.
817 Available at: [https://obamawhitehouse.archives.gov/the-press-](https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity)
818 [office/2013/02/12/executive-order-improving-critical-infrastructure-](https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity)
819 [cybersecurity](https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity)

- 820 [Energies-2019] Ronanki, D, Kelkar, A, Williamson, S. “Extreme Fast Charging
821 Technology—Prospects to Enhance Sustainable Electric Transportation”.
822 *Energies*2019,12, 3721. <https://doi.org/10.3390/en12193721>
- 823 [EPRI-2023] Cybersecurity Platform and Certification Framework Development for
824 Extreme Fast Charging (XFC)-Integrated Charging Ecosystem. EPRI,
825 Palo Alto, CA: 2023. 3002027649
- 826 [Grandview] Grand View Research. “U.S. Electric Vehicle (EV) Charging
827 Infrastructure Market Size, Share & Trends Analysis Report By Charger
828 Type, By Connector Type, By Level of Charging, By Connectivity, By
829 Application, And Segment Forecasts, 2023 – 2030” Report ID: GVR-3-
830 68038-309-6. Available at:
831 [https://www.grandviewresearch.com/industry-analysis/us-electric-
832 vehicle-charging-infrastructure-evci-market](https://www.grandviewresearch.com/industry-analysis/us-electric-vehicle-charging-infrastructure-evci-market)
- 833 [IEC61850-90-4] International Electrotechnical Commission (2020) *IEC TR 61850-90-
834 4:2020 Communication networks and systems for power utility
835 automation - Part 90-4: Network engineering guidelines* (IEC, Geneva,
836 Switzerland). Available at <https://webstore.iec.ch/publication/64801>
- 837 [IEC61850-90-12] International Electrotechnical Commission (2020) *IEC TR 61850-90-
838 12:2020 Communication networks and systems for power utility
839 automation - Part 90-12: Wide area network engineering guidelines.*
840 (IEC, Geneva, Switzerland). Available at
841 <https://webstore.iec.ch/publication/63706>
- 842 [IEC62439-3] International Electrotechnical Commission (2021) *IEC 62439-3
843 Industrial communication networks - High availability automation
844 networks - Part 3: Parallel Redundancy Protocol (PRP) and High-
845 availability Seamless Redundancy (HSR).* (IEC, Geneva, Switzerland).
846 Available at <https://webstore.iec.ch/publication/64423>
- 847 [IETF-RFC4082] Perrig A, Song D, Canetti R, Tygar JD, Briscoe B (2005) Timed
848 Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast
849 Source Authentication Transform Introduction. (Internet Engineering
850 Task Force (IETF) Network Working Group), IETF Request for
851 Comments (RFC) 4082. <https://doi.org/10.17487/RFC4082>
- 852 [Johnson-Berg] Johnson J, Berg T, Anderson B, Wright, B. (2022). Review of Electric
853 Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and
854 Defenses. *Energies*. 15. 3931. [10.3390/en15113931](https://doi.org/10.3390/en15113931).
- 855 [NERC-CIP-008-6] North American Electric Reliability Corporation (2020) *CIP-008-6 –
856 Cyber Security – Incident Reporting and Response Planning*. Available
857 at [https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-
858 6.pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf)
- 859 [NERC-GridEx] North American Electric Reliability Corporation (2020) *GridEx*.
860 Available at <https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx>

- 861 [NIST-CSF] National Institute of Standards and Technology (2018) Framework for
862 Improving Critical Infrastructure Cybersecurity, Version 1.1. (National
863 Institute of Standards and Technology, Gaithersburg, MD).
864 <https://doi.org/10.6028/NIST.CSWP.04162018>
- 865 [NIST-IR 7298] Paulsen C, Byers R. (2022). *Glossary of Key Information Security*
866 *Terms*. Available at:
867 <https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/final>
- 868 [NIST-IR7800] Waltermire D, Halbardier A, Humenansky A, Mell P (2012) Applying
869 the Continuous Monitoring Technical Reference Model to the Asset,
870 Configuration, and Vulnerability Management Domains. (National
871 Institute of Standards and Technology, Gaithersburg, MD), NIST
872 Interagency or Internal Report (IR) 7800 (Draft). Available at
873 [https://csrc.nist.gov/CSRC/media/Publications/nistir/7800/draft/documen](https://csrc.nist.gov/CSRC/media/Publications/nistir/7800/draft/documents/Draft-NISTIR-7800.pdf)
874 [ts/Draft-NISTIR-7800.pdf](https://csrc.nist.gov/CSRC/media/Publications/nistir/7800/draft/documents/Draft-NISTIR-7800.pdf)
- 875 [NIST-IR8014] Hastings NE, Franklin JM (2015) Considerations for Identity
876 Management in Public Safety Mobile Networks. (National Institute of
877 Standards and Technology, Gaithersburg, MD), NIST Interagency or
878 Internal Report (IR) 8014. <https://doi.org/10.6028/NIST.IR.8014>
- 879 [NIST-IR8179] Paulsen C, Boyens JM, Bartol N, Winkler K (2018) Criticality Analysis
880 Process Model: Prioritizing Systems and Components. (National Institute
881 of Standards and Technology, Gaithersburg, MD), NIST Interagency or
882 Internal Report (IR) 8179. <https://doi.org/10.6028/NIST.IR.8179>
- 883 [NIST-IR8320] Bartock M, Souppaya M, Savino R, Knoll T, Shetty U, Cherfaoui M,
884 Yeluri R, Malhotra A, Banks D, Jordan M, Pendarakis D, Rao JR,
885 Romness P, Scarfone K (2022) Hardware-Enabled Security: Enabling a
886 Layered Approach to Platform Security for Cloud and Edge Computing
887 Use Cases. (National Institute of Standards and Technology,
888 Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8320.
889 <https://doi.org/10.6028/NIST.IR.8320>
- 890 [NIST-SP1271] NIST SP 1271, Getting Started with the NIST Cybersecurity Framework:
891 A Quick Start Guide. <https://doi.org/10.6028/NIST.SP.1271>
- 892 [NIST-SP800-30r1] Joint Task Force Transformation Initiative (2012) Guide for Conducting
893 Risk Assessments. (National Institute of Standards and Technology,
894 Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
895 <https://doi.org/10.6028/NIST.SP.800-30r1>
- 896 [NIST-SP800-34r1] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010)
897 Contingency Planning Guide for Federal Information Systems. (National
898 Institute of Standards and Technology, Gaithersburg, MD), NIST Special
899 Publication (SP) 800-34, Rev. 1, Includes updates as of November 11,
900 2010. <https://doi.org/10.6028/NIST.SP.800-34r1>
- 901 [NIST-SP800-37r2] Joint Task Force (2018) Risk Management Framework for Information
902 Systems and Organizations: A System Life Cycle Approach for Security
903 and Privacy. (National Institute of Standards and Technology,

- 904 Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2.
905 <https://doi.org/10.6028/NIST.SP.800-37r2>
- 906 [NIST-SP800-53r5] Joint Task Force (2020) Security and Privacy Controls for Information
907 Systems and Organizations. (National Institute of Standards and
908 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53,
909 Rev. 5. Includes updates as of December 10, 2020.
910 <https://doi.org/10.6028/NIST.SP.800-53r5>
- 911 [NIST-SP800-61r2] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer
912 Security Incident Handling Guide. (National Institute of Standards and
913 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61,
914 Rev. 2. <https://doi.org/10.6028/NIST.SP.800-61r2>
- 915 [NIST-SP800-92] Kent K, Souppaya MP (2006) Guide to Computer Security Log
916 Management. (National Institute of Standards and Technology,
917 Gaithersburg, MD), NIST Special Publication (SP) 800-92.
918 <https://doi.org/10.6028/NIST.SP.800-92>
- 919 [NIST-SP800-115] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical
920 Guide to Information Security Testing and Assessment. (National
921 Institute of Standards and Technology, Gaithersburg, MD), NIST Special
922 Publication (SP) 800-115. <https://doi.org/10.6028/NIST.SP.800-115>
- 923 [NIST-SP800-128] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide
924 for Security-Focused Configuration Management of Information
925 Systems. (National Institute of Standards and Technology, Gaithersburg,
926 MD), NIST Special Publication (SP) 800-128, Includes updates as of
927 October 10, 2019. <https://doi.org/10.6028/NIST.SP.800-128>
- 928 [NIST-SP800-137] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC,
929 Orebaugh AD, Scholl MA, Stine KM (2011) Information Security
930 Continuous Monitoring (ISCM) for Federal Information Systems and
931 Organizations. (National Institute of Standards and Technology,
932 Gaithersburg, MD), NIST Special Publication (SP) 800-137.
933 <https://doi.org/10.6028/NIST.SP.800-137>
- 934 [NIST-SP800-150] Johnson CS, Waltermire DA, Badger ML, Skorupka C, Snyder J (2016)
935 Guide to Cyber Threat Information Sharing. (National Institute of
936 Standards and Technology, Gaithersburg, MD), NIST Special
937 Publication (SP) 800-150. <https://doi.org/10.6028/NIST.SP.800-150>
- 938 [NIST-SP800-154] Souppaya M, Scarfone K (2016) Guide to Data-Centric System Threat
939 Modeling. (National Institute of Standards and Technology,
940 Gaithersburg, MD), NIST Special Publication (SP) 800-154 (Draft).
941 Available at <https://csrc.nist.gov/publications/detail/sp/800-154/draft>
- 942 [NIST-SP800-160V1] Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering:
943 Considerations for a Multidisciplinary Approach in the Engineering of
944 Trustworthy Secure Systems. (National Institute of Standards and
945 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-

- 946 160, Vol. 1, Includes updates as of March 21, 2018.
947 <https://doi.org/10.6028/NIST.SP.800-160v1>
- 948 [NIST-SP800-161] Boyens J, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk
949 Management Practices for Federal Information Systems and
950 Organizations. (National Institute of Standards and Technology,
951 Gaithersburg, MD), NIST Special Publication (SP) 800-161.
952 <https://doi.org/10.6028/NIST.SP.800-161>
- 953 [NIST-SP800-175Br1] Barker EB (2020) Guideline for Using Cryptographic Standards in the
954 Federal Government: Cryptographic Mechanisms. (National Institute of
955 Standards and Technology, Gaithersburg, MD), NIST Special
956 Publication (SP) 800-175B, Rev. 1.
957 <https://doi.org/10.6028/NIST.SP.800-175Br1>
- 958 [NIST-SP800-184] Bartock MJ, Scarfone KA, Smith MC, Witte GA, Cichonski JA,
959 Souppaya MP (2016) Guide for Cybersecurity Event Recovery.
960 (National Institute of Standards and Technology, Gaithersburg, MD),
961 NIST Special Publication (SP) 800-184.
962 <https://doi.org/10.6028/NIST.SP.800-184>
- 963 [NIST-SP800-193] Regenscheid AR (2018) Platform Firmware Resiliency Guidelines.
964 (National Institute of Standards and Technology, Gaithersburg, MD),
965 NIST Special Publication (SP) 800-193.
966 <https://doi.org/10.6028/NIST.SP.800-193>
- 967 [NIST-SP800-209] Chandramouli R, Pinhas D (2020) Security Guidelines for Storage
968 Infrastructure. (National Institute of Standards and Technology,
969 Gaithersburg, MD), NIST Special Publication (SP) 800-209.
970 <https://doi.org/10.6028/NIST.SP.800-209>
- 971 [NIST-SP800-218] Souppaya M, Scarfone K, Dodson D (2022) Secure Software
972 Development Framework (SSDF) Version 1.1: Recommendations for
973 Mitigating the Risk of Software Vulnerabilities. (National Institute of
974 Standards and Technology, Gaithersburg, MD), NIST Special
975 Publication (SP) 800-218. <https://doi.org/10.6028/NIST.SP.800-218>
- 976 [NIST-SP1800-19] Bartock M, Souppaya M, Dodson D, Carroll D, Masten R, Scinta G,
977 Massis P, Prafullchandra H, Malnar J, Singh H, Ghandi R, Storey L,
978 Yeluri R, Shea T, Dalton M, Weber R, Scarfone K, Phoenix C, Dukes A,
979 Haskins J, Swarts B (2022) Trusted Cloud: Security Practice Guide for
980 VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments.
981 (National Institute of Standards and Technology, Gaithersburg, MD),
982 NIST Special Publication (SP) 1800-19. Available at
983 <https://doi.org/10.6028/NIST.SP.1800-19>
- 984 [NIST-SP1800-34] Diamond T, Grayson N, Polk W, Regenscheid A, Souppaya M, Brown
985 C, Deane C, Scarfone K (2021) Validating the Integrity of Computing
986 Devices. (National Institute of Standards and Technology, Gaithersburg,
987 MD), NIST Special Publication (SP) 1800-34 (Preliminary Draft).
988 Available at <https://csrc.nist.gov/publications/detail/sp/1800-34/draft>

- 989 [RTCA-DO-235] Radio Technical Commission for Aeronautics (2008) *RTCA DO-235A*
990 *Assessment of Radio Frequency Interference Relevant to the GNSS L1*
991 *Frequency Band*. (RTCA, Washington, DC). Available at
992 <https://standards.globalspec.com/std/1090607/RTCA%20DO-235>
- 993 [S.1353] S.1353 - 113th Congress (2013-2014): Cybersecurity Enhancement Act
994 of 2014, S.1353, 113th Cong. (2014),
995 <https://www.congress.gov/bill/113th-congress/senate-bill/1353/text>.

996 **Appendix A. List of Symbols, Abbreviations, and Acronyms**

997	AAR
998	After Action Report
999	AC
1000	Alternating Current
1001	API
1002	Application Programming Interface
1003	BESS
1004	Battery Energy Storage System
1005	BMS
1006	Battery Management System
1007	CAN
1008	Control Area Network
1009	CD
1010	Compact Disc
1011	COI
1012	Community of Interest
1013	CRC
1014	Cyclic Redundancy Check
1015	CSF
1016	Cyber Security Framework
1017	CTI
1018	Cyber Threat Intelligence
1019	CVE
1020	Common Vulnerabilities and Exposures
1021	CVSS
1022	Common Vulnerability Scoring System
1023	CWE
1024	Common Weakness Enumeration
1025	DAR
1026	Data-At-Rest
1027	DC
1028	Direct Current
1029	DE
1030	Detect
1031	DER
1032	Distributed Energy Resources
1033	DIT
1034	Data-In-Transit

1035	DOE
1036	Department of Energy
1037	DVD
1038	Digital Versatile Disc
1039	ECU
1040	Electronic Control Unit
1041	EO
1042	Executive Order
1043	EPRI
1044	Electric Power Research Institute
1045	EV
1046	Electric Vehicle
1047	EVSE
1048	Electric Vehicle Supply Equipment
1049	EVTOLS
1050	Electric Vehicle Take-Off and Landing
1051	FERC
1052	Federal Energy Regulatory Commission
1053	HMI
1054	Human-Machine Interface
1055	ICS
1056	Industrial Control System
1057	ID
1058	Identify / Identity
1059	IIOT
1060	Industrial Internet of Things
1061	IOT
1062	Internet of Things
1063	IT
1064	Information Technology
1065	IEC
1066	International Electrotechnical Commission
1067	ISAC
1068	Information Sharing and Analysis Center
1069	ISO
1070	International Organization for Standardization
1071	MOU
1072	Memorandum of Understanding
1073	MFA
1074	Multi-Factor Authentication

1075	NERC
1076	North American Electric Reliability Corporation
1077	NFC
1078	Near Field Communication
1079	NIST
1080	National Institute of Standards and Technology
1081	NVD
1082	National Vulnerability Database
1083	OBD-II
1084	On-Board Diagnostic II
1085	OCPI
1086	Open Charge Point Interface
1087	OCPP
1088	Open Charge Point Protocol
1089	OEM
1090	Original Equipment Manufacturer
1091	OT
1092	Operational Technology
1093	OTA
1094	Over the Air
1095	PCI
1096	Payment Card Industry
1097	PII
1098	Personally Identifiable Information
1099	PIN
1100	Personal Identification Number
1101	PLC
1102	Programmable Logic Controller
1103	PR
1104	Protect
1105	RBAC
1106	Role Based Access Control
1107	RC
1108	Recover
1109	RF
1110	Radio Frequency
1111	RS
1112	Respond
1113	SBOM
1114	Software Bill of Material

- 1115 **SCADA**
- 1116 Supervisory Control and Data Acquisition

- 1117 **SCRM**
- 1118 Supply Chain Risk Management

- 1119 **SD**
- 1120 Secure Digital

- 1121 **SLA**
- 1122 Service Level Agreement

- 1123 **TTP**
- 1124 Tactics, Techniques, and Procedures

- 1125 **TTX**
- 1126 Tabletop Exercise

- 1127 **V2G**
- 1128 Vehicle-To-Grid

- 1129 **XFC**
- 1130 Extreme Fast Charging