Government Fleet and Public Sector Electric Vehicle Supply Equipment (EVSE) Cybersecurity Best Practices and Procurement Language Report

Prepared by:
United States Department of Transportation Volpe Center and

Prepared for:
Department of Navy
Naval Facilities Engineering Command (NAVFAC)
Public Works Business Line, Transportation Product Line

Final Report-November 2019

DOT-VNTSC-NAVY-20-01

Prepared for:
Department of Navy
Naval Facilities Engineering Command (NAVFAC)
Public Works Business Line, Transportation Product Line

U.S. Department of Transportation
Volpe Center

Notice

This report is disseminated under the sponsorship of the Department of Transportation and the Naval Facilities Engineering Command (NAVFAC) in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE: November 2019	3. REPORT TYPE AND DATES COVERED Cybersecurity Best Practices Report

4. TITLE AND SUBTITLE	5a. FUNDING NUMBERS
Government Fleet and Public Sector Electric Vehicle Supply Equipment (EVSE) Cybersecurity Best Practices and Procurement Language Report	VXQ4A5/TH094
6. AUTHOR(S) Kevin Harnett, Graham Watson, Gus Brown	5b. CONTRACT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Department of Transportation John A. Volpe National Transportation Systems Center 55 Broadway Cambridge, MA 02142-1093	8. PERFORMING ORGANIZATION REPORT NUMBER DOT-VNTSC-NAVY-20-01
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Department of Navy Naval Facilities Engineering Command (NAVFAC) Public Works Business Line, Transportation Product Line	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES	
12a. DISTRIBUTION/AVAILABILITY STATEMENT This document is available to the public on the National Transportation Library (NTL) Repository and Open Science Access Portal (ROSA P) website at:	12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

Currently there are no cybersecurity standards or guidance for Electrical Vehicle Supply Equipment (EVSE) tailored towards the needs of the Federal Government and the private sector vehicles. This report discusses threats and proposes cybersecurity requirements for the Federal Government and private sector EVSEs.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Electric Vehicle (EV), Electric Vehicle Supply Equipment (EVSE), Cybersecurity, Charging Station, Smart Grid, Utility, Building Energy Management Systems (BEMS), Requirements, Best Practices	62
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASS	UNCLASS	UNCLASS	Unlimited

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18
298-102

Acknowledgments

The Electric Vehicle environment encompasses a wide set of diverse stakeholders whose knowledge and expertise was critical in the information gathering and data analysis necessary for this report. The authors would like to thank these stakeholders for their contributions to this report.

Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Term
A&A	Assessment and Authorization
AFV	Alternative Fuel Vehicle
ATO	Authorization To Operate
AWS	Amazon Web Services
BEV	Battery Electric Vehicles
CCC	Chaos Communication Congress
CGI	Common Gateway Interface
CSD	Cybersecurity Directorate
CVE	Common Vulnerability Exposure
DCFC	Direct Current Fast Charger
DER	Distributed Energy Resources
DFAR	Defense Federal Acquisition Regulation
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
DOE	Department of Energy
EO	Executive Order
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
FAR	Federal Acquisition Regulation
FAST	Federal Automotive Statistical Tool
FEC	Facilities Engineering Command
GSA	General Services Administration
ICS-CERT	Industrial Control Systems – Computer Emergency Response Team
IT	Information Technology
LAN	Local Area Network
LDV	Light-Duty Vehicle
MAC	Media Access Control
NMCI	Navy Marine Corps Intranet
NMFTA	National Motor Freight Traffic Association
OEM	Original Equipment Manufacturer
OP	Office of Policy
OTA	Over-The-Air
PHEV	Plug-in Hybrid Electric Vehicles
RMF	Risk Management Framework
S&T	Science & Technology
SME	Subject Matter Expert
STIG	Security Technology Implementation Guide
VTO	Vehicle Technologies Office
WAN	Wide Area Network
XFC	Extreme Fast Charger

Executive Summary

According to the latest data provided by General Services Administration (GSA) the government employs a total of 1,349 electric vehicles counting both battery electric and plugin hybrid models in various agency fleets. The majority of these vehicles are Ford, General Motors, FCA, and Nissan. There are now over 1 million electric vehicles in the US. The public sector is the part of the economy composed of both public "government" services and public enterprises. Currently there are no standards or guidance for EVSE cybersecurity tailored towards the needs of the Federal Government and the private sector. The EVSE cybersecurity requirements in this report are recommended for use as guidance only for government organizations such as the Department of Defense (DoD), Civil Federal Agencies, Government and public sector fleet managers, State and Local Governments/Municipalities, Law Enforcement agencies and any Public Sector organization such as: EVSE vendors, EVSE Network Operators, Extreme Fast Charging (XFC) Vendors, and Utilities and need to be tailored to each organization's EVSE architecture and environment in the, production, management, evaluation and/or procurement of EVSEs.

In 2017, the U.S. Department of Energy's (DOE) Office of Policy (OP), in collaboration with DOE's Vehicle Technologies Office (VTO), the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), and the U.S. Department of Transportation's (U.S. DOT) John A. Volpe National Transportation Systems Center (Volpe) held a technical meeting on key aspects of Electric Vehicle (EV) and EVSE cybersecurity with a large group of stake holders across multiple industries [1]. The outcome of the workshop identified EVSE for light passenger vehicles and electric trucks as a major vulnerability point in the Federal electric vehicle environment. Add a simple sentence explaining EVSEs for this meeting were L1, L2 and DCFC (add voltages)

In June 2019, the National Motor Freight Transportation Association (NMFTA) and the U.S. DOT Volpe center published a report titled "Extreme Fast Charging Cybersecurity Threats, Use Cases and Requirements for Medium and Heavy Duty Electric Vehicles" [4], the cybersecurity requirements in that report were derived from automotive, EV, and EVSE industry stakeholder collaboration.

Examples of EVSE Vulnerabilities

EVSE have vulnerabilities which can affect not only the device itself, but also the EV fleet and, in some cases, the local power grid. The examples of EVSE vulnerabilities detailed below are **not** for EVSE units currently used by the Navy or any other government agency. They serve as examples of the types of vulnerabilities that EVSE can contain. These are EVSE vulnerabilities that have been reported in the public domain and Section 1.3 provides more details:

- EVSE authentication cards that allowed for the charging and authentication could be copied easily and as often as one would like

- Major vulnerabilities were found in an EVSE remote management mobile application
- An EVSE brand was found to have serious vulnerabilities associated with the use of hard-coded credentials
- An EVSE vulnerability allowed a remote attacker to retrieve credentials stored in clear text.
- Interconnected power grids are being exposed to greater risk as EVSE are deployed.

These examples of EVSE vulnerabilities, demonstrate that the cybersecurity should be a high priority for any Federal, State, or Private organization Fleet Manager considering the acquisition and deployment of these technologies is support of their petroleum reduction and energy security goals.

EVSE Component Decomposition

EVSE are comprised of a number of system components that work together to deliver power to the vehicle for charging while also providing a secure means for user authentication, usage data to be transmitted to the EVSE Vendor, and critical EVSE maintenance and performance information to be monitored. For the purposes of this report, it should be noted that "charging station" is semantically synonymous with "EVSE." Technically, in a level 1 or 2 EVSE, the vehicle's on-board charger recharges the battery pack and is powered by the EVSE, but for all intents and purposes the two terms can be used interchangeably. The functions of the three main elements that make up the EVSE environment are defined in Table 1.

Element	FUNCTIONS
EVSE Owner/Operator, Site Controller, EVSE Network Operator	• Supplies power connection to the EVSE • Authorizes the EV user to charge • Gathers and processes data and measurements • Commands energy limits to control the energy flow between the EVSE and vehicle based on charging station data
EVSE (i.e. Charging Station), Authentication Terminal	• Supplies and controls energy from the Grid Operator to the EV • Collects charge measurements for each EV • Authenticates EV users • Enables remote management of the EVSE via the Charging Station over the WAN
Grid Operator	• Forecasts the available capacity • Ensures power supply stability

Table 1: EVSE Environmental Elements and Functions Description

EVSE Cybersecurity Requirements

The key elements of ESVE's that are relevant when evaluating cybersecurity include the EVSE and/or EVSE Vendors/Network Operators and Grid Operators. The 64 EVSE cybersecurity requirements listed in Section 5 address various aspects of these key elements. The requirements were compiled by the DOT/Volpe Center in collaboration with the Naval Facilities Engineering Command (NAVFAC). The

research and data for this report were acquired through pre-existing EVSE and Electric Vehicle (EV) publications and reports from the following sources:

- Interviews with industry subject matter experts
- Cybersecurity requirement report [2] from the knowledge and innovation center in the field of Smart Charging infrastructure in the Netherlands (ElaadNL)
- National Motor Freight Traffic Association (NMFTA) Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cybersecurity Baseline Reference report [3], and the NMFTA Heavy Vehicle Cybersecurity for Extreme fast Chargers report from June 2019 [4].

The requirements in Section 5 are broken down into ten specification sections. Each requirement within these elements contains the following data:

- **Security Control Area**: Defines the sub-area of the EVSE system addressed by the requirement
- **Name**: The name of the major area of the requirement
- **Charger Type**: The type of charger that the requirement applies to
- **Source**: The source (if any) for the requirement
- **No.**: A reference number for the requirement
- **Devices**: Components in the EVSE system affected by the requirement
- **Requirements**: The requirement itself
- **Assurances**: Demonstrable proof that the requirement has been met

Table 2 below provides an overview of the EVSE requirements listing the requirements specification section and the Security Control Areas:

EVSE Specification Section	Security Control Area
Design	Design Future-Proofing
	Hardware Design
	Remote Firmware Updates
	Secure Over-the-Air Updates
	Secured Versioning
	Segmentation of Functions
	Vehicle Communication & Connection Anonymity
Cryptography	Cryptographic Algorithms and Key Lengths
	Cryptographic Random Number Generation
	Key Management
Logging	Black Box Recorder
	IDS/IPS systems
	Logging Security Events-Local Controllers
	Logging Security Events-Authentication Terminals
Lifecycle and Governance	Vulnerability Disclosure Program
	Information Security Management System (ISMS)
	Configuration Management System
	Vulnerability Management Process
	Security Updates and Patching
	Security Training and

			Awareness
	Cryptographic Versioning		Security Production and Credential Provisioning
Communication	Confidentiality		EVSE Incident Response Plan
			Assessment & Authorization
			FedRAMP Compliance
	Message Integrity	Assurance	Design Evidence (part 1)
	Firmware Integrity		Design Evidence (part 2)
	Replay Attack Detection		Security Testing
	Replay Prevention		Secure Coding Practices
	Authentication		Vulnerability Scanning of Device & Backend
Hardening	Least Functionality		Utility Operator Confidentiality
	Device Hardening		EVSE Operator Message Integrity
	Interface Minimization		Utility Operator Message Integrity
	Account Hardening		EVSE Operator Message Authentication
	Security-enhancing features		Utility Operator Message Authentication
	Protection against Physical Manipulations		EVSE Operator Message Integrity Verification
Resiliency	Message Integrity Verification		Utility Operator Message Integrity Verification
	Fail-Secure Operation	Secure Operation	Cryptographic Key Management
	Fail-Secure Operation		Secure Local Storage of Sensitive Information (PII, VIN, Payment Info, etc.)
Secure Operation	Access Control		Intrusion Detection & Logging of independent power quality and quantity
	User Authentication		Cryptographic Hardware Module Authentication
	End User Authentication		Secure power up /power down for safe grid operation
	Payment System		Ongoing Third-Party Penetration Testing and Security Testing

Table 2: EVSE Requirements Overview

Conclusions

The electrification of vehicle fleets across the government and private sector will continue, leveraging the associated cost savings and emissions improvements. While the rate at which EVs and EVSE are being procured and deployed is steadily increasing, there is still a window of opportunity to get ahead of

the curve in cybersecurity for these systems.

Too often the cybersecurity considerations of a new electronic product or system are overlooked resulting in resource-intensive, time consuming, and less than adequate post-deployment applications of cybersecurity controls. The EVSE cybersecurity requirements and considerations identified in this report are intended to be used as a starting point for those organizations (i.e. DoD, Federal Government, State and Local Governments/Municipalities, Law Enforcement agencies, and Private organizations like Utilities) which procure, operate, or interface with EV and EVSEs. As with any cybersecurity tool, these requirements are not final formal standards but rather an initial step toward the development of a robust and thoroughly vetted standard and guidance documents.

1 Introduction

1.1 Objective

According to the latest data provided by General Services Administration (GSA) the government employs a total of 1,349 electric vehicles counting both battery electric and plugin hybrid models in various agency fleets. The majority of these vehicles are Ford, General Motors, FCA, and NISSAN. There are now over 1 million electric vehicles in the US. This report discusses threats and proposes cybersecurity requirements for Federal Government and public sector Electric Vehicle Supply Equipment (EVSE). Currently there are no standards or guidance for EVSE cybersecurity tailored towards the needs of the Federal Government and the private sector. The EVSE cybersecurity requirements in this report are recommended for use as guidance only for government organizations such as the Department of Defense (DoD), Civil Federal Agencies, Government and public sector fleet managers, State and Local Governments/Municipalities, Law Enforcement agencies and any Private organization such as: EVSE vendors, EVSE Network Operators, Extreme Fast Charging (XFC) Vendors, and Utilities and need to be tailored to each organization's EVSE architecture and environment in the, production, management, evaluation and/or procurement of EVSEs in public sector.

In 2017, the U.S. Department of Energy's (DOE) Office of Policy (OP), in collaboration with DOE's Vehicle Technologies Office (VTO), the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), and the U.S. Department of Transportation's (U.S. DOT) John A. Volpe National Transportation Systems Center (Volpe) held a technical meeting on key aspects of Electric Vehicle (EV) and EVSE cybersecurity with a large group of stake holders across multiple industries [1]. The outcome of the workshop identified EVSE for light passenger vehicles and electric trucks as a major vulnerability point in the Federal electric vehicle environment. In June 2019, the National Motor Freight Transportation Association (NMFTA) and the U.S. DOT Volpe center published a report titled "Extreme Fast Charging Cybersecurity Threats, Use Cases and Requirements for Medium and Heavy Duty Electric Vehicles" [4], the cybersecurity requirements in that report were derived from automotive, EV, and EVSE industry stakeholder collaboration.

An increase in cybersecurity awareness across the EV and EVSE industry, coupled with the government and private sector growing EV and EVSE inventory, is the driving factor behind this report. Government and public sector fleet managers need to understand the criticality of ensuring the proper cybersecurity measures are considered during the acquisition and integration of EVSE across government and public sector installations. Utilizing current EVSE environmental data and in-depth interviews with Subject Matter Experts (SMEs), it is the objective of this report to provide an insightful overview of the current state of EVSE cybersecurity while providing a resource for guidance and best practices that can be used across the DoD and Federal electric vehicle and electric truck sectors.

1.2 EVSE Industry Overview

According to the DOE's Office of Energy Efficiency and Renewable Energy, there were more than 68,000 EVSE deployed in the United States as of May 2019. Driven by emissions regulations, increased environmental awareness, decreasing material and technology costs, and significantly higher vehicle efficiency and performance, EVs and their supporting EVSE are experiencing explosive growth.

Table 3 lists the categories of chargers, based on the maximum power and whether the device's output is alternating current (AC) or direct current (DC). There are three major categories of chargers: Level 1, Level 2 and DCFC. A fourth category is the Extreme Fast Charger (XFC) which supports medium and heavy duty electric trucks and high voltage charging.

Charger Type	Specifications
Level 1	• 120VAC input • Output AC voltage to the EV • Can deliver 2-5 miles of ranger per hour of charging • Often a standard wall electrical outlet • Most commonly used in homes and workplaces
Level 2	• 240VAC or 208VAC input • Output AC voltage to the EV • Requires installation of dedicated charging equipment • Can deliver 10-20 miles of range per hour of charging • Use in homes, workplaces and for long-dwell public EVSE
DC Fast Charger (DCFC)	• 480 AC input • Output up to 150 kW DC voltage to the EV • Requires specialized, high-powered equipment on the charger as well as the vehicle itself. • Can deliver 60-80 miles of range in 20 min of charging. • Use for short-dwell public charging or electrified motor pools
Extreme Fast Charger (XFC)	• Output 350 kW – 1 MW of DC voltage for medium and heavy duty electric trucks. • Highly specialized high-powered equipment. • Over 700 miles of range per hour of charging. • Used for fleet charging of electric trucks
Inductive Charging	• Output up to 200kW DC in use at present time for commercial buses • Specialized equipment for contactless charging typically 6" to12" range

Table 3: EVSE Types

Networks of EVSE are necessary supporting infrastructure to enable a driving range acceptable to organizations and typical consumers. The Office of Energy Efficiency and Renewable Energy estimated in a 2017 report that by the year 2030 [5], the United States would need approximately 600,000 Level 2 EVSE and 25,000 DCFC chargers to support approximately 15 million EVs. Hence, it is prudent to establish and understand the best practices for EVSE cybersecurity is now for the Federal Government and public sector EV sector to potential adverse impacts to physical and environmental safety as well as the power grid and supporting Information Technology (IT) infrastructures.

1.3 EVSE Cybersecurity Overview

A major cybersecurity challenge is the variety of implementations of protocols for communication, network, and user-to-EVSE authentication. The differences in technologies, lack of standards and general urgency to get EVSE systems to market results in a wide array of attack vectors, risks, and potential threats. Threat actors include insider threats, hacking collectives, criminal organizations and nation states. The Microsoft STRIDE threat model (see Appendix A) defines the following cybersecurity vulnerabilities:

- **S**poofing Identity
- **T**ampering with Data
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of Privilege

Networked and network-capable EVSE have potential impact on their fleets, grids, and networks, but also enjoy potential benefits beyond facilitating fleet reporting and utility billing, such as the possibility of vehicle-grid-integration (VGI) for Distributed Energy Resources (DER) and energy management. Thus, best practices and guidelines will be necessary to balance cybersecurity and system availability. Various domestic and foreign organizations are working towards this goal. Nonetheless, there have been several high-risk vulnerabilities identified in EVSE.

1.3.1 Private and Public EVSE Cybersecurity Vulnerabilities

This section illustrates some general industry examples of ESVE cybersecurity vulnerabilities. It is important to note that these are **not** EVSE units currently used by the Federal government.

- In 2018, cybersecurity vulnerabilities were found to be associated with ChargePoint Home EVSE units as detailed in a report by Kaspersky Lab [6]. The report identified major cybersecurity flaws in the charging stations' remote management mobile application that could allow a malicious user to bypass authentication requirements and add new users to the EVSE unit without the

owner's knowledge. These cybersecurity flaws highlighted threats within the information disclosure, escalation of privilege and tampering with data categories of the STRIDE threat model. Once exploited, these vulnerabilities could lead to charging interference and potential financial losses for the owner. Another issue was identified in the ChargePoint Home unit's Common Gateway Interface (CGI) binaries that could allow an intruder to gain access to the charger and tamper with parts of the owner's home electrical system, potentially causing fore or other physical damage. ChargePoint was ultimately able to remediate the vulnerabilities through software and firmware updates.

- Also in 2018, Schneider Electric EVSE units were found to have serious vulnerabilities associated with the use of hard-coded credentials, code injection and SQL injection as detailed by DHS's Industrial Control Systems – Computer Emergency Response Team (ICS-CERT) under the ICS Advisory ICSA-19-031-01 [7]. Specific Common Vulnerabilities and Exposure (CVE) entries for these include CVE-2018-7800, CVE-2018-7801 and CVE-2018-7802, which all have a base vulnerability score of Critical, High and Medium respectively. These vulnerabilities could allow an attacker to tamper with EVSE functions as well as inflict physical and financial damage. Within the STRIDE model, these threats fall within the tampering with data, information disclosure, escalation of privilege, and denial of service categories.
  Schneider Electric has made a software update available to mitigate these vulnerabilities.

1.3.2 Research Community EVSE Cybersecurity Vulnerabilities

The following are EVSE vulnerabilities found by the research community:

- In December 2017, at the Chaos Communication Congress (CCC) conference in Leipzig, Germany cybersecurity researcher Mathias Dalheimer presented findings in NewMotion EVSE deployed on their networks throughout Germany [8]. Dalheimer found that a public card number associated with the authentication cards that allowed for the charging and authentication was publicly stored and could be easily copied. This provided the means for individuals to use cloned cards to charge their own vehicles without having to pay for them. Additionally, Dalheimer demonstrated that the card numbers were transmitted without encryption directly to the provider. This required little technical effort to intercept this communication and harvest card numbers to forge cards or simply simulate charging events. Within the STRIDE model, these vulnerabilities would likely present threats in the spoofing identity, tampering with data and information disclosure categories.

- At the 2019 DEF CON 27 conference, security professional John Kurnaz revealed vulnerabilities in CirCarLife EVSE units that could allow a remote attacker to retrieve credentials stored in clear text and use them to bypass authentication on the EVSE, allowing a hacker access to critical system information. This information is categorized under ICS Advisory ICSA-18-305-03 [9]. Mitigation recommendations have been provided, although this vulnerability has not been fully

addressed in all currently deployed CirCarLife EVSE units. These vulnerabilities fall under the tampering with data, repudiation, escalation of privilege, and potentially denial of service categories of the STRIDE model and have serious cybersecurity implications.

- In August 2019, New York University (NYU) researchers [10] detailed how increasingly-interconnected power grids are being exposed to more risk as EVSE units have been deployed. The report details how cyber-attacks aimed at EVSE could potentially cause blackouts with serious grid impacts, depending on their length and geographic extent.

- In October of 2019 at the October 2019 USENIX conference [11] researchers detailed how design choices in the Combined Charging System (CCS) standard which is in use worldwide in the use of power-line communication (PLC) make the system prone to electromagnetic side-channel attacks.

These examples of current and legacy vulnerabilities demonstrate that the cybersecurity implications of EVSE should be a high priority for any DoD or Federal Fleet Manager considering the acquisition and deployment of EVs and ESVE units in support of their petroleum reduction and energy security goals. In Section 4 of this report we identify additional vulnerabilities that should be of particular interest and deserves substantial consideration from the government and public sector community.

2 EV and EVSE Overview

2.1 EVSE Element Decomposition

The EVSE environment is comprised of system elements that work together to deliver power to the EV for charging. These elements are listed in Table 4. They provide a secure means for user authentication, as well as transmission of usage, maintenance, and performance data to the EVSE network operator.

Element	FUNCTIONS
EVSE Owner/Operator, Site Controller, Network Operator	• Supplies power connection to the EVSE • Authorizes the EV user to charge • Gathers and processes data and measurements • Commands energy limits to control the energy flow between the EVSE and vehicle based on Charging Station data
EVSE Charging Station, Authentication Terminal	• Supplies and controls energy from the Grid Operator to the EV • Collects charge measurements for each EV • Authenticates EV users • Enables remote management of the EVSE via the Charging Station over the WAN
Grid Operator	• Forecasts the available capacity • Ensures power supply stability

Table 4: EVSE Environmental Element and Function Descriptions

2.2 Notional EVSE Environment

A notional EVSE architecture diagram and additional component definitions are provided in Figure 1. Each government and public sector deployment may be slightly different depending on operational priorities. Current Navy EVSE inventory consists of almost entirely of Level 2 chargers deployed within the physical security perimeter of the naval installation.

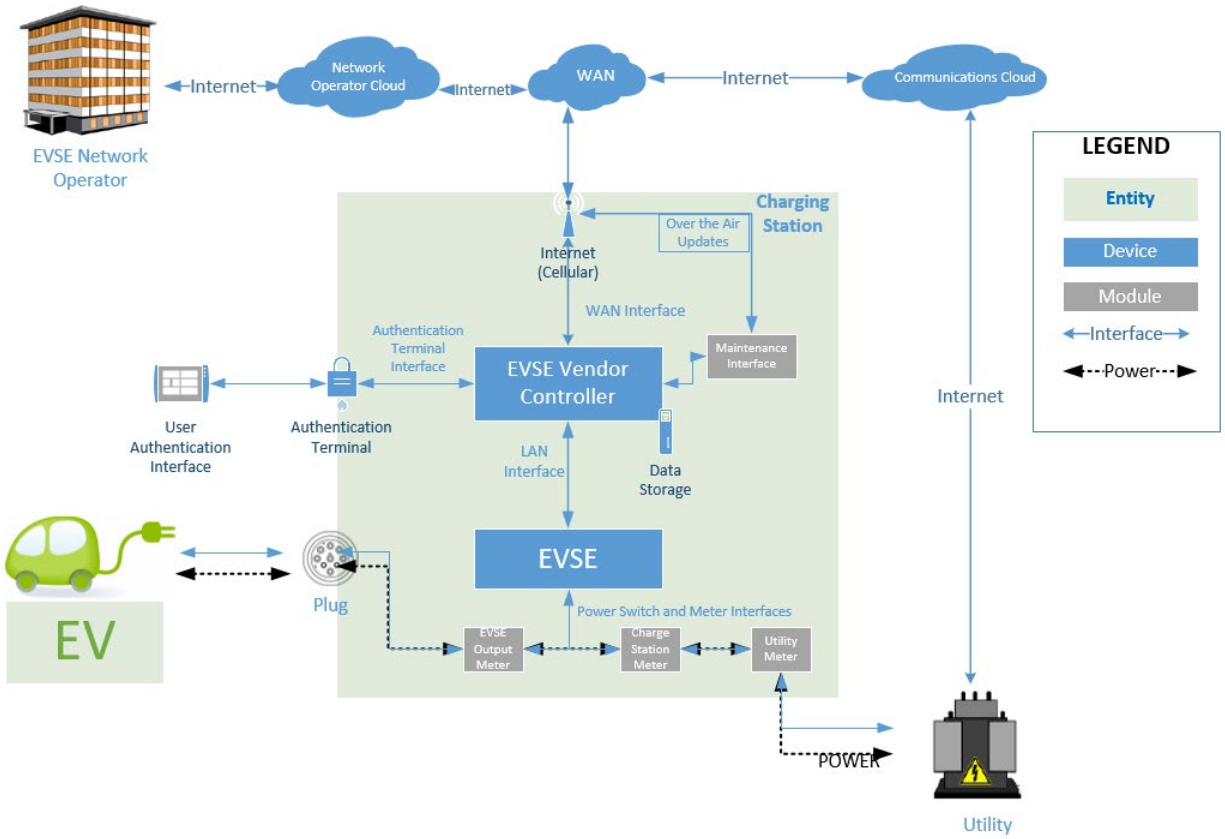

Figure 1: Notional EVSE Environment

The legend in Figure 1 identifies various types of physical components and/or system communication and data transport modes. These components are explained further by the following definitions:

- **Entity -** Represents the EVSE.
- **Device -** Identifies the component within the charging station. A device can have Interfaces to communicate with other devices.
- **Module -** Identifies the physical part of the Device where important functionalities operate
- **Interface -** Defines the communication links between two Devices.

The EVSE Vendor Controller **Core** (*"the core")* includes the operating system, cybersecurity functionality and other system level functionality at the foundation of the EVSE Vendor Controller.

3 EV and EVSE Statistics

3.1 Projections for EVs, Electric Trucks, and Electric Bus Inventories

BloombergNEF reports that global passenger electric vehicle sales surpassed 2 million vehicles in 2018. Sales are expected to top 10 million by 2025 [12]. In the United States, 2019 EV sales were forecast at over 380,000 and expected to reach over 1.5 million by 2025 [13]. This substantial sales growth reflects a significant effort by the automotive industry to promote electric vehicles. The 2019 Bloomberg Electrical Vehicle Outlook report [16] projects price parity for EVs vis-a-vis internal combustion engine vehicles by the mid-2020s. Presumably, the federal government and the private sector vehicle purchases will follow these market trends.

According to a recent report by Lisa Jerram, a principal research analyst for Navigant Research, the number of hybrid-electric and electric trucks is set to grow almost 25% annually, from 1% of the market in 2017 to 7% in 2027, a jump from about 40,000 electric trucks worldwide this year to 371,000. Technavio's market research analyst predicts that the global electric bus market will grow at a CAGR of close to 27% (in terms of units shipped) during the forecast period of 2016-2020. The global electric bus market is primarily dominated by five major vendors who continually compete to gain maximum market share. Key vendors in the market are: New Flyer, Volvo, Novabus, Gillig, BYD, Ebus, Proterra, Wuzhoulong and Yutong. One of the key focus areas for Electric Bus OEMs is working with state and city government agencies. For example, Seattle's Metro Transit has ordered 120 all electric buses, which is the largest purchase of its kind in the nation to date. Metro Transit released a plan to transition its entire fleet to electric buses by 2034 [14].The market is also characterized by rapid innovation and the development of advanced buses to meet the needs of specific regions [15].

The 2019 Bloomberg Electrical Vehicle Outlook report [16] projects price parity for EVs vis-a-vis internal combustion engine vehicles by the mid-2020s.

4 Federal Government EVSE Cybersecurity Considerations

This section of the report is specifically targeted for the Federal Government EV and EVSE environments. The public sector should consider the following EVSE cybersecurity issues and actions when evaluating, procuring and operating EVSEs in their environment:

- EVSE Cyber Security Risk Assessments leveraging the NIST 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach* [17] and NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations [18]
- EVSE secure "cloud" environment and possible leveraging of the Federal Risk and Authorization Management Program (FedRAMP) or other cloud security best practices such as: Cloud Security Alliance (CSA) [19]. FedRAMP is a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services

Through interviews with government transportation and EVSE Subject Matter Experts (SMEs), as well as government cybersecurity personnel, the authors have been able to assess the government's current posture of the EVSE environment from a cybersecurity perspective. We have considered how the government is deploying EVSE units across government installations, how organizations are addressing cybersecurity challenges, and how they are planning for the future. The following EVSE cybersecurity considerations can assist Fleet Managers and IT staff regarding EVSE cybersecurity issues for the DoD and federal fleet managers, in addition to Public Sector organizations:

4.1 Administrative Cybersecurity Considerations

Purchase of EVSE systems

The acquisition, installation, operation, and maintenance of EVSE units across government installations have cybersecurity implications. Some DoD agency acquisition personnel are required to purchase only approved EVSE products, such as those in the February 2017 General Services Administration's (GSA) Blanket Purchase Agreement (BPA) for EVSE [20].

Some DoD ESVE purchases are subject to information security requirements as outlined in the Defense Federal Acquisitions Regulation. Clause 252.204-7012 [21] requires "government contractors to comply with two key information security requirements: (1) adequate cybersecurity and (2) incident reporting." This clause, unlike the Federal Acquisition Regulation (FAR) Final Rule 52.204-21, provides for detailed implementation and reporting standards based on NIST guidelines.

Cybersecurity Risk Assessment

- EVSE devices may not currently be viewed as information systems. Nonetheless, based on cybersecurity research, currently identified vulnerabilities, and possible future connections to government networks, it will be prudent to consider EVSE units to be considered IT systems. As such, serious consideration should be given to DoD Assessment and Authorization (A&A) requirements and/or NIST Federal Information Systems Act (FISMA) compliance, such as NIST 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach* [17] and NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations [18]

Cloud Security (EVSE Back-end Services)

An additional administrative concern is the compliance of an EVSE vendor, network operator, and/or cloud infrastructure vendors for payment and billing information. EVSE units will need cybersecurity authorization through the Risk Management Framework (RMF) to connect to a DoD or Federal network. The vendor's cloud infrastructure will have to be Federal Risk and Authorization Management Program (FedRAMP) [22] approved. FedRAMP is a government-wide program that provides a standardized approach to cybersecurity assessment, authorization, and continuous monitoring for cloud products and services such as EVSE back-end network operators and cloud services.

Today, a large number of government EVSE inventory is manufactured by ChargePoint which uses cloud services provided by Amazon Web Services (AWS). AWS is one of the few cloud services authorized to provide services to the DoD based on FedRAMP compliance. In October 2021 the GSA will require the award of a new GSA BPA. ESVE products without a FedRAMP certification will not likely be purchased by the DoD or other government organization.

Payment Systems

An important consideration involves payment for the potential use of government EVSE units by employees to charge privately owned electric vehicles. The Fixing America's Surface Transportation Act (FAST Act) [23] authorizes the GSA and other Federal agencies to install, operate and maintain electric vehicle charging stations for privately owned EVs. The use of government owned EVSE units for charging private vehicles will require the expansion and implementation of the payment interface on EVSE which will inherently expand the cybersecurity attack surface of the devices.

4.2 Physical Security Considerations

There are many differing types of EVSEs each having their own unique properties. Commercial EVSEs are public facing devices (e.g. public parking lots, garages, rest stops) which have unique physical security challenges. Unlike personal computers and servers, which are usually kept behind locked doors, commercial charging stations are situated in public areas and are frequently left unattended and open to physical damage. Commercial EVSE equipment is often placed in public places with low to zero security. In such instances, there are windows of opportunity for potential attackers to tamper and damage the EVSE equipment physically, such as manipulating the EVSE through open USB ports or

subscriber identification module (SIM) card slots.

Intentional physical attacks on EVSEs can occur to gain access to the EVSE's internal electronics to perform a cyber-based attack, to steal components such as cabling which have a high re-sale value, or to vandalize the equipment. In addition to intentional attacks, unintentional physical damage to EVSEs can be caused by vehicles striking the EVSE, charging cabling being cut or torn out, and miscellaneous damage to user interfaces located on the EVSE such as displays and payment systems. Physical damage to commercial EVSEs can result in non-operational units which could have an adverse effect on consumer confidence in EVs in general. Some types of physical damage whether intentional or not, may expose the public to harmful electric current levels.

Physical security mitigations in the EVSE environment such as anti-tamper hardware, cyber event monitoring, video surveillance hardware and techniques (such as object video), and tamper alert of the EVSE components as well as physical protection considerations for the installation of EVSE equipment such as bollards, frangible fittings, lighting, etc. The physical security of EVSE components needs to be thoughtfully designed so as not to undermine the cybersecurity mechanisms put in place and to also allow for maintenance. For example, EVSE equipment is often placed in public places with low to zero security. In such instances, there is a window of opportunity for a potential attacker to tamper with the EVSE equipment physically which often is enough to undermine cybersecurity defense mechanisms.

EVSE units currently on DoD Installations are inherently subject to physical security and other controls that limit the number of personnel who can access them. Many EVSE units are deployed in general parking areas, parking garages, etc. requiring appropriate credentials. Some EVSE units may be located in areas with additional security, such as motor pool areas or compounds for military operations. EVSE units are typically monitored by security patrols and security cameras.

4.3 Traditional Cybersecurity – IT Based Considerations

If an EVSE unit is not connected to any DoD network, they are not required to obtain an Authority To Operate (ATO) by the DoD nor are they subject to the cybersecurity controls in NIST 800-53 Revision 4 (Security and Privacy Controls for Federal Information Systems and Organization), Committee on National Security Systems (CNSSI) 1253 (Security Categorization and Control Selection for National Security Systems) or other DoD or Federal security compliance requirements. This means that certain cybersecurity assessments such as operating systems (OS) testing or other functional or application security testing are not taking place.

ESVE power is received from the power substation and any communication back to the EVSE vendor takes place over the EVSE unit's built-in cellular network communications card. Over-The-Air (OTA) updates and the associated cellular communication are subject to various cybersecurity vulnerabilities. If a non-networked ESVE unit were compromised, risks associated with the connection to the power grid would remain.

In the future, EVSE might have interfaces to government networks for vehicle-grid-integration purposes. As such, the need for thorough cybersecurity evaluation and/or compliance for an ATO should be considered. The user interaction and payment processes should all be evaluated for their potential cybersecurity impacts. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) provide guidelines for cybersecurity evaluations of various OS and technical devices and could affect tailoring ESVE controls in the future. The NIST 800-53 Security Controls for Risk Management Framework (RMF) allow for controls to be tailored to fit specific technology types such as control systems such as EVSE units.

4.4 Embedded Cybersecurity Considerations

Unlike traditional IT systems, EVSE operates in an embedded environment that is resource constrained and is designed to interface with unknown and untrusted devices. The following paragraphs detail some of the considerations that are unique to this environment.

Penetration Testing

- A key component of cybersecurity is penetration testing which is an ongoing testing process which will test cybersecurity of an EVSE. The best way to accomplish this is through independent testing and verification of the EVSE following government and industry best practices [24, 25, 26, 27]. Such penetration testing should be done by a neutral "third party", to ensure that the EVSE does not have any easily discovered vulnerabilities. Penetration testing (either manually or with automated tools) includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings. The main objective of penetration testing is to determine security weaknesses and fix them before an adversary finds them. There are three main types of penetration testing, white box, grey box, and black box, each having to do with the amount of proprietary data given to the tester on the component/system being tested. In a white box scenario, the tester is given full and complete data on the component/system being tested. In a grey box situation, the tester is given slightly more data than can be obtained from public domain research. In a black box situation the tester can only utilize data on the component/system which is in the public domain.

Over the Air Updates (OTA)

- EVSE needs to be able to quickly and securely apply updates, patches, and enhancements (including cybersecurity patches) to the software and firmware. Attacking OTA updates would provide cybercriminals direct access to multiple EVSsE, and possible manipulation of EVSE functions, so it is critical that Secure OTA (SOTA) is implemented for the EVSE [28]. Some of the challenges facing OTA updates are providing a secure updating method that addresses the

entire chain of back-end servers, wireless links, and the EVSE itself. Additionally, a method to confirm that the patch is unaltered and successfully installed is needed for both the owner of the EVSE and the vendor.

Inductive Charging

Contactless, inductive, or "wireless" charging which is already seeing use among the commercial bus industry is unique in that consists of an EVSE which uses electromagnetic resonance to charge a vehicle rather than a physical cable connection to the vehicle. The EVSE is connected to fixed pad on the ground which contains an electromagnetic coil. The vehicle contains a similar coil, both the charging pad and vehicle use coils of the same physical orientation and resonate frequency to transfer power to the vehicle's batteries eliminating the need for charging cables and plugs. Currently there is no clear guidance on cybersecurity requirements specifically for inductive charging systems.

Inductive charging systems face the same cybersecurity issues as traditional wired charging systems, but because of the wireless aspect, unique issues need to be considered such as:

- Remote attack vectors to the EVSE where a malicious actor could compromise the safety, privacy, or operation of not only charging, but other infrastructure functions without physically interacting with the EVSE.
- The physical and cyber security mitigations used for a traditional, wired charging system will need to be redesigned because the same threat model does not apply. Two-way communication between the EV and EVSE is exposed to eavesdroppers and is vulnerable to attacks over the air.
- Different vulnerabilities than traditional charging systems including influencing the positional information of the vehicle, enabling energy transfer when a vehicle isn't present or when a human is between the vehicle and the fixed coil, and eavesdropping on vehicle charge status or payment information need to be considered.

RFID User Authentication

Interviews with government personnel indicated that some EVs are each assigned a Radio Frequency Identification (RFID) card that allows the operator to be authenticated by the ESVE before charging the vehicle. The RFID information for that vehicle is logged so that the agency can bill the appropriate organization for power consumption. This limited access inhibits cybersecurity attacks related to cloned RFID cards or software issues related to billing.

4.5 Mitigation Resources

Organizations like the Idaho National Laboratory (INL) have published various reports on their cybersecurity evaluations of EV and EVSE technologies that include recommendations cybersecurity requirements and mitigations [29]. The DOE's Federal Energy Management Program (FEMP) has compiled a set of EV- and EVSE-related cybersecurity mitigation resources called the Fleet Cybersecurity Toolkit [30]. A cornerstone in the Fleet Cybersecurity Toolkit is the National Renewable Energy Laboratory's (NREL) Vehicle Cybersecurity Threats and Mitigation Approaches report, specifically Section 5 – EVSE Cybersecurity Threats and Vulnerabilities [20]. The report discusses vehicle cybersecurity considerations including technical approaches to mitigating known EVSE vulnerabilities and appropriate

cybersecurity language for procurements to assure the acquisition of secure EVSE units. The report recommendations include:

"Mitigation Techniques for Physical Threats to all EVSE
EVSE companies can mitigate physical access risks to all EVSE, including SAE J1772 Level 1 and Level 2, by:
• Removing all jacks that are externally accessible from the EVSE unit
• Incorporating strong encryption of the controller boards in the EVSE, including flash memory and board-to-board communication
• Including a tampering alarm or signal to the service provider
• Employing secure coding practices and auditing the source code."

"Procurement Recommendations for Physical Threats to all EVSE
The following procurement recommendations can help federal fleets mitigate EVSE physical access risks:
• EVSE should be constructed without external control board physical access points or with the minimum access points required to function in a given setting o This includes, but is not limited to, RJ45 (ethernet), D-subminiature serial type connections (e.g. video graphics array [VGA]), and all forms of USB o If control board physical access points are required for general operation and maintenance, the ports should be secured from public access or concealed in a lockable enclosure.
• All communication and management of the system board should incorporate high-level encryption o Firmware should be encrypted, locked, or require signatures o All locally stored flash memory should be encrypted o All encryption techniques should use FIPS 197 AES 256 algorithm and cryptographic modules that have been validated under FIPS 140, National Security Agency Type 1 or Type 2 standards, or equivalent standards demonstrated to be acceptable alternatives"

Although Level 2 EVSE units are not as sophisticated as DCFC and XFC chargers, they can still have vulnerabilities such as non-tamper proof access that allows an attacker to gain physical access to the onboard electronics of the EVSE. Physical access might enable installation of malware to render the EVSE inoperable and/or lock the charging cables to the unit. These issues are addressed in the NREL toolkit.

The major challenge for U.S. government fleet managers and procurement personnel is the acquisition of EVSE units that include integrated cybersecurity attributes that require less up front mitigation and requirements that EVSE vendors can be held accountable.

5 EVSE Cybersecurity Best Practices

5.1 EVSE Cybersecurity Best Practices Overview

This section of the report details the intent of the EVSE cybersecurity requirements, identification of the importance of the proper application of current standards, and the EVSE security controls/requirements guidance.

5.1.1 Intent of Use

The cybersecurity requirements section is intended to be used by federal executive agencies as well as state and local municipalities and public sector as a requirement for single purchases of EVSE as well as in the solicitation for future pre-negotiated contracts for the purchase of EVSE, including Level 2, DCFCs, and XFCs. These requirements may be tailored and made applicable to all government EVSE technologies. GSA Office of Fleet Management's awarded an EVSE BPA in 2017 which covers a 5 year period with option years spanning from March 2017 through February 2022. This report will provide input for the cybersecurity requirements section of future solicitations.

5.1.2 Proper application of existing standards

There are references to various cybersecurity standards within the requirements in the tables below. As best practices and standards are always evolving, it is recommended that the most recent version of any standard be applied. For example, a recent cybersecurity study was made of *ISO 15118-2 Standard Road Vehicles – Vehicle-to-Grid Communications Interface - Part 2: Network and Application Protocol Requirements* [31] where the authors of that report listed a series of cybersecurity concerns with the current version of the ISO 15118-2 standard.

5.2 EVSE Cybersecurity Requirements

The tables below contain listings of cybersecurity requirements for an EVSE system. These requirements have been drafted for applicability to Level 2 EVSE, DC Fast Chargers (DCFC) as well as Extreme Fast Chargers (XFC). The requirements are broken down into ten sections. Each requirement listed within these sections contains the following elements:

- **Name**: The name of the major area of the requirement
- **Charger Type**: The type of charger that the requirement applies to
- **Source**: The source (if any) for the requirement

- **No.**: A reference number for the requirement
- **Security Control Area**: Defines the sub-area of the EVSE system addressed by the requirement
- **Devices**: Components in the EVSE system affected by the requirement
- **Requirements**: The requirement itself
- **Assurances**: Demonstrable proof that the requirement has been met

5.2.1 Design

<table>
<tr><td colspan="3">EVSE System Specification Section: Design</td><td>Charger Type(s): L2, DCFC, XFC</td></tr>
<tr><td colspan="4">Source: Elaad/NL-Chapter 2 Section 2.1 Future-Proof Design [2]</td></tr>
<tr><td>Ref #</td><td>Security Control Area</td><td>Devices</td><td>Requirements</td></tr>
<tr><td>SSD-01</td><td>Design future-proofing</td><td>Local Controllers, Authentication Terminals</td><td rowspan="3">The Device SHALL have sufficient reserves in memory and computing power to allow updates to security functions that security experts anticipate are necessary during the Device’s lifecycle.</td></tr>
<tr><td colspan="3">Assurances</td></tr>
<tr><td colspan="3">• Analysis of the design documentation provided by the Vendor.
• Testing the performance of the Device for algorithms and protocols anticipated for future use.</td></tr>
</table>

<table>
<tr><td colspan="3">EVSE System Specification Section: Design</td><td>Charger Type(s): L2, DCFC, XFC</td></tr>
<tr><td colspan="4">Source: ElaadNL-Chapter 2 Section 2.1 Future-Proof Design [2]</td></tr>
<tr><td>Ref #</td><td>Security Control Area</td><td>Devices</td><td>Requirements</td></tr>
<tr><td>SSD-02</td><td>Hardware Design</td><td>EVSE</td><td rowspan="3">The EVSE SHALL support modular replacement of all components that provide wireless access interfaces to the EVSE</td></tr>
<tr><td colspan="3">Assurances</td></tr>
<tr><td colspan="3">• Analysis of the design documentation provided by the Vendor.
• Testing the performance of the Device for algorithms and protocols anticipated for future use.</td></tr>
</table>

EVSE System Specification Section: Design			Charger Type(s): L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.1 Future-Proof Design* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSD-03	Remote Firmware Updates	Local controllers	1. The Device SHALL support updating all security and operational functions through remote firmware updates. 2. The Device SHALL NOT perform updates while charging a vehicle
Assurances			
• Analysis of the design documentation provided by the Vendor.			

EVSE System Specification Section: Design			Charger Type(s): L2, DCFC, XFC
Source: *NMFTA Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cybersecurity Baseline Reference Document-Section 13.2* [3]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSD-04	Secure over the air updates	EVSE	1. If the device supports over the air software/firmware updates the updates SHALL be implemented in a secure fashion through the best practices methodologies such as UPTANE [32], OCPP [33], Internet Engineering Task Force (IETF) [34] IoT Firmware Update Architecture, etc. 2. The Device SHALL NOT perform updates while charging a vehicle
Assurances			

EVSE System Specification Section: Design			Charger Type(s): L2, DCFC, XFC
Source: *NMFTA Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cybersecurity Baseline Reference Document-Section 13.2* [3]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSD-05	Secured Versioning	System wide	1. The Vendor SHALL ensure that all released versions of hardware and firmware of the Device are uniquely identifiable. 2. The Vendor SHALL provide to the Purchaser a cryptographic hash value for each firmware version. 3. The Vendor SHALL be able to reproduce released versions within the contractually agreed product lifecycle, with traceability provided by the hash value(s) as identifier(s). 4. The Vendor SHALL version exchangeable hardware modules separately.
Assurances			

	5. The Vendor SHALL digitally sign each firmware update supplied to the Purchaser. 6. The Vendor SHALL protect the firmware signing keys as highly confidential data. 7. The Vendor SHALL report it to the Purchaser if a firmware signing key is compromised.

EVSE System Specification Section: Design			**Charger Type(s):** L2, DCFC, XFC
Source: NMFTA XFC Working Group			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSD-06	Segmentation of functions	EVSE and local controllers	Memory and processing space for wireless interface controllers SHALL be separated/segmented from the memory and processing space of all other system controllers (e.g., the main system board,).
Assurances			

EVSE System Specification Section: Design			**Charger Type(s):** L2, DCFC, XFC
Source: Volpe - Telematics Cybersecurity Primer for Agencies (AR-7 PRIVACY-ENHANCED SYSTEM DESIGN AND DEVELOPMENT) [36]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSD-07	Vehicle Communication and Connection Anonymity		1. The Utility Operator and ESVE Operator system SHALL implement privacy controls to protect the confidentiality and integrity of vehicle connections and connection requests as well as other Personally Identifiable Information (PII).
Assurances			

5.2.2 Cryptography

EVSE System Specification Section: Cryptography			**Charger Type(s):** L2, DCFC, XFC
Source: ElaadNL-Chapter 2 Section 2.2 Cryptographic Algorithms and Protocols [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSCR-01	Cryptographic Algorithms and key Lengths	Local controllers, EVSE, Authentication Terminals	1. For security functions, the Device SHALL use only cryptographic algorithms for which a description is publicly available, and which have been thoroughly reviewed by independent cryptographers.
Assurances			

• Analysis of the design documentation provided by the Vendor can be used to establish that only allowed cryptographic algorithms, protocols, and parameters are used. • Functional security tests can be used to verify that the algorithms are implemented as described. • Cryptographic primitives can be certified with the NIST Cryptographic Algorithm Validation Program (CAVP).	2. For security functions the Device SHALL not use cryptographic or hashing algorithms, protocols, and parameters if they are known to be vulnerable via e.g. academic research or public vulnerability disclosures (Common Vulnerabilities and Exposures (CVEs), Common Weakness Enumeration (CWEs), etc.) 3. The Device SHALL use only those cryptographic algorithms, and parameters considered suitable for future use. 4. The Device SHALL use the algorithms implemented exactly as they are described in the reviewed literature without any modifications.

EVSE System Specification Section: Cryptography			**Charger Type(s):** L2, DCFC, XFC
Source: ElaadNL-Chapter 2 Section 2.2 Cryptographic Algorithms and Protocols [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSCR-02	Cryptographic Random Number Generation	Local Controllers, Authentication Terminals	The Device SHALL use a dedicated cryptographic pseudo- random number generator, as defined in FIPS 186-4 [36], FIPS 140-2 (Annex C)[37] to generate random numbers used for security functions such as secret key generation and generation of nonces. The Device SHALL use the algorithms implemented exactly as they are described in reviewed literature without any modifications.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Proof of the implementation could be the reports of a standardized test procedure such as the NIST Cryptographic Algorithm Validation Program (CAVP). • NIST SP 800-22 provides a standardized test suite to look for biases found in non-cryptographic random number generator during a black-box test.			

EVSE System Specification Section: Cryptography			**Charger Type(s):** L2, DCFC, XFC
Source: ElaadNL-Chapter 2 Section 2.2 Cryptographic Algorithms and Protocols [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSCR-03	Key Management	Local Controllers, Authentication Terminals	1. The Device SHALL support remote updates of all credentials and cryptographic keys. 2. The Device SHALL support limiting the duration

Assurances • Analysis of the design documentation provided by the Vendor. • Functional tests can be used to establish the functionality is present on the Device.	of a session to a time length that is configurable by the purchaser. 3. The Device SHOULD support establishing a fresh key for each communication session. 4. The Device SHOULD support using different keys for different services and applications relative to the level of privilege required to use a service or application, and the level to which the respective service or application requires access to elevated privileges, critical system resources, and control of system components. Each device needs to have a unique key.

EVSE System Specification Section: Cryptography			**Charger Type(s):** L2, DCFC, XFC
Source: ElaadNL-Chapter 2 Section 2.2 Cryptographic Algorithms and Protocols [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSCR-04	Cryptographic Versioning	Local Controllers, Authentication Terminals	1. The Device SHALL implement version identifiers for the communication protocol used. 2. The Device SHALL be able to configure the minimum required version of the cryptographic protocol that is used and reject connections and requests to use older protocol versions.
Assurances • Analysis of the design documentation provided by the Vendor. • Functional tests can be used to establish the functionality is present on the Device.			

5.2.3 Communication

EVSE System Specification Section: Communication			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSCO-01	Confidentiality	Local Controllers	1. The Device SHALL protect the confidentiality of communication on the Wide Area Network
Assurances			

• This requirement is verified in a functional security test. The test should in particular ensure that the allowed cryptographic algorithms are supported and that disallowed algorithms are rejected. Federal guidance for choosing a hash function can be found at: https://csrc.nist.gov/Projects/Hash-Functions/NIST-Policy-on-Hash-Functions	(WAN) interface by encrypting it using a protocol allowed by the cryptographic algorithms and key length requirements. 2. If passwords are used on the Device the Device SHALL NOT store passwords in readable plaintext. The Device SHALL generate and store a salt value for every password generated on the device. All stored credentials on the Device SHALL be the hashed value of the password combined with the salt value. 3. Hashing functions SHOULD be open-sourced and proven to be collision resistant one-way hash functions. 4. The Device SHALL NOT use known vulnerable hash functions.

EVSE System Specification Section: Communication			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSCO-02	Message Integrity	Local Controllers	1. If the Device detects that a message has been modified or if it cannot verify the integrity of the message, it SHALL reject or drop the message. 2. The Device SHALL allow parties it communicates with on the WAN or Maintenance interfaces to verify the integrity of application layer messages it sends by using a message authentication algorithm allowed by the cryptographic algorithms and key length requirements. 3. The Device SHALL verify the cryptographic integrity of messages received on the Local Network interface. 4. The Device SHALL allow parties it communicates with on the Local Network interface to verify the integrity of application layer messages it sends by using a message authentication algorithm allowed by the cryptographic algorithms and key length requirements.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Functional tests can be used to verify that the Device supports the required functionality. • Carrying out a penetration test can be used to determine if the Device verifies message integrity under all conditions.			

EVSE System Specification Section: Communication	**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [2]	

Ref #	Security Control Area	Devices	Requirements
SSCO-03	Firmware Integrity	Local controllers, EVSE, Authentication Terminals	1. The Device SHALL verify the source and integrity of firmware images before they are applied using a hashing function and hash provided by the Vendor. 2. The Device SHALL reject installation of firmware updates if it detects the firmware has been modified, or it cannot verify the firmware's integrity.
Assurances			
• The functional requirement can be verified by testing the implemented firmware-update functions.			

EVSE System Specification Section: Communication			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSCO-04	Replay Attack Detection	Local Controllers	1. The Device SHALL be able to detect replay attacks on all wireless interfaces. 2. If the Device detects that a message is replayed, it SHALL reject or drop the message.
Assurances			
• Analysis of the design documentation provided by the Vendor on the mechanisms used to protect against replay attacks. • Functional testing can be used to verify if the mechanisms are indeed implemented.			

EVSE System Specification Section: Communication			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSCO-05	Replay	Local Controllers	

	Prevention		The Device SHALL support verification of a message's source as that of a specific local component in the EVSE
Assurances			
• Analysis of the design documentation provided by the Vendor on the mechanisms used for message authentication. • Functional testing can be used to verify if the mechanisms are indeed implemented. • Penetration tests can be used to ascertain that attackers cannot bypass the authentication mechanisms.			

EVSE System Specification Section: Communication			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSCO-06a	Authentication	Local controllers, EVSE, Authentication Terminals	1. The Device SHALL support checking the authenticity of firmware images obtained through any of its available update mechanisms (both remote and local): before installing a firmware image 2. The Device SHALL verify that the firmware came from the Vendor by verifying its cryptographic signature against a trusted issuer. 3. In case the firmware storage medium is external to the processor that is executing it (e.g. external flash chip), the Device bootloader SHALL verify that the firmware signature is valid every time before running it, and not run it if it is invalid
Assurances			
• Analysis of the design documentation provided by the Vendor on the mechanisms used for non-repudiation. • Functional testing can be used to verify if the mechanisms are indeed implemented. • Penetration tests can be used to ascertain that attackers cannot bypass the non-repudiation mechanisms.			

EVSE System Specification Section: Communication			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSCO-06b	Authentication	Local controllers, EVSE,	The Device shall require a method of authentication for each system component at least as strong as the method used for

		Authentication Terminals	accessing the device remotely
Assurances			
Penetration tests can be used to ascertain the strength of the authentication components in the system.			

5.2.4 Hardening

EVSE System Specification Section: Hardening			**Charger Type(s):** L2, DCFC, XFC
Source: *Volpe-Telematics Cybersecurity Primer for Agencies CM-7 Least Functionality* [35]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSH-01	Least Functionality	System Wide	The Device SHALL only host services and applications critical to the normal functionality and maintenance of the Device and SHALL NOT host any unnecessary code libraries or applications that are no part of the Device's normal operation or required in the maintenance of the Device.
Assurances			

EVSE System Specification Section: Hardening			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.4 System Hardening* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSH-02	Device Hardening	Local Controllers, Authentication Terminals	1. The Device SHALL have all unneeded services and applications removed or disabled if removal is not possible. 2. The Device SHALL not use services or
Assurances			

• Vulnerability scanners can automatically check devices for known vulnerabilities. • Carrying out a penetration test can provide further assurance that this requirement is adequately implemented. • If high-impact functions are disabled in the Device code, the Purchaser can request a code review from the Vendor.	applications for security functions if there are unmitigated vulnerabilities known for them. 3. The Device SHALL use only communication protocols that are needed to meet the functional requirements, and for which no unmitigated vulnerabilities are known.

EVSE System Specification Section: Hardening			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.4 System Hardening* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSH-03	Interface Minimization	Local Controllers, Authentication Terminals	The Device SHALL have any unneeded interfaces and ports removed prior to deployment of the Device or disabled if removal is not possible. In particular, all hardware interfaces that are used for debugging (e.g. JTAG, UART) SHALL be removed or disabled if removing is not possible prior to deployment.
Assurances			
• Carrying out a penetration test can provide assurance that this design requirement is adequately implemented.			

EVSE System Specification Section: Hardening			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.4 System Hardening* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSH-04	Account Hardening	Local Controllers	1. The Device SHALL NOT support active default logins, guest accounts, or anonymous accounts/logins.
Assurances			

• Analysis of the design documentation provided by the Vendor. • Carrying out a penetration test can provide further assurance that this design requirement is adequately implemented.	2. The Device SHALL NOT allow remote access e.g. root accounts for non-update purposes on the Device. 3. The Device SHALL have Vendor-owned accounts removed where feasible. 4. The Device SHALL enforce a password policy that only allows passwords of sufficient complexity. See NIST SP800-63-3 Digital Identity Guidelines and SP800-63b Digital Identity Guidelines: Authentication and Lifecycle Management [38] for authentication guidelines

EVSE System Specification Section: Hardening			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.4 System Hardening* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSH-05	Security-enhancing features	Local Controllers, Authentication Terminals	The Device SHOULD deploy security-enhancing features of the underlying platform, implementation language, and tool chain when such features improve the security and resilience of the Device.
Assurances			
• Analysis of the design documentation provided by the Vendor on which security enhancing features are used. • Functional tests can be used to verify that features are indeed used.			

EVSE System Specification Section: Hardening			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.4 System Hardening* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSH-06	Protection against Physical Manipulations	EVSE	1. Physical manipulations of the EVSE SHALL be recognizable. 2. The EVSE door SHALL provide sufficient protection against physical manipulations.
Assurances			

• Carrying out a penetration test can provide further assurance that this design requirement is adequately implemented. • Analysis of the penetration test results.	3. The opening of the EVSE door SHALL be recognized by the Device/System using suitable means such as alarms, sensors. Any opening of the EVSE door SHALL generate an event in the Device's security log. 4. The removal of any part of EVSE SHALL be recognized by the Device/System using suitable means such as alarms, sensors. Any opening of the EVSE door SHALL generate an event in the Device's security log. 5. The removal of any part of EVSE SHALL generate an event in the security log. 6. The vendor SHOULD provide design evidence ensuring that this requirement is addressed. 7. The housing of the EVSE SHALL be constructed with a tamper resistant design, materials, and fasteners generate an event in the security log. 8. The vendor SHOULD provide design evidence ensuring that this requirement is addressed. 9. The housing of the EVSE SHALL be constructed with a tamper resistant design, materials, and fasteners

5.2.5 Resiliency

EVSE System Specification Section: Resiliency			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.5 Resilience* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSR-01	Message Integrity Verification	Local Controllers, Authentication Terminals	1. The Device SHALL verify the integrity of all messages it receives. 2. The Device SHALL reject or drop messages that are invalid or for which the message integrity cannot be verified.
Assurances			
• It is recommended to carry out fuzzing tests on all interfaces. • The Vendor should provide a detailed documentation of all security tests.			

EVSE System Specification Section: Resiliency			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.5 Resilience* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**

SSR-02	Fail-Secure Operation	Local Controllers, Authentication Terminals	1. The Device SHALL be fail-secure, i.e., it SHALL be designed to fail in a manner that limits any security compromise of its own operation and security compromise of other devices. 2. The Device SHALL NOT leak confidential information, such as keys or credentials, through any Device interface during a system failure or fault condition. 3. The Device SHALL protect the integrity of security critical data during failures. 4. The Device SHALL NOT allow access controls to be bypassed remotely during failures.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Carrying out a penetration test can provide further assurance of the design robustness.			

EVSE System Specification Section: Resiliency			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 2 Section 2.5 Resilience* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSR-03	Fail-Secure Operation	Local Controllers, Authentication Terminals	1. The Device SHALL attempt to perform a secure revision of the operating system to the last known good state after software failures as soon as possible for a maximum of 10 times.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Carrying out a penetration test can provide further assurance of fail-secure operation.			

5.2.6 Secure Operation

EVSE System Specification Section: Secure Operation			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 3 Section 3.1 Access Control* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSS-01	Access Control	Local Controllers	1. The Device SHALL restrict access to the WAN interface to certain hosts e.g., using a whitelist.
Assurances			

• This requirement is verified in a functional security test. The test should in particular ensure that each role has only the defined and necessary privileges. • Penetration testing can be used to make sure that the access controls cannot be circumvented by for instance privilege escalation.	2. The Device SHALL support and enforce varying levels of required privilege to perform various maintenance and debugging tasks. 3. On the Maintenance interface, the Device SHALL only grant access to configuration and firmware update functions if a user's role has the necessary privileges. 4. The Device SHALL allow new roles to be defined. 5. The Device SHALL require the use of unique security credentials and keys for each level of privilege and user account available on the Device.

EVSE System Specification Section: Secure Operation			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 3 Section 3.1 Access Control* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSS-02	User Authentication	Local Controllers	1. The Device SHALL authenticate the communication parties on the WAN interface using a challenge-response protocol based on either message authentication codes or public-key certificates. 2. The Device SHALL terminate the connection if the user authentication fails. 3. The Device SHALL authenticate the communication parties on the Local Maintenance interface. 4. The Device SHALL support blocking authentication requests, either temporarily or permanently, from an account after a configurable number of failed login attempts. The number of failed login attempts and the time for which access to the account is disabled SHALL be configurable.
Assurances			
• The implementation of user identification can be verified in a functional security test. • Carrying out a penetration test can provide further assurance that this design requirement is adequately implemented.			

EVSE System Specification Section: Secure Operation			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 3 Section 3.1.1 User Authentication for the Authentication Terminal* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSS-03	End User Authentication	Authentication Terminals	1. The Device SHALL support a cryptographic challenge-response authentication protocol to authenticate the end-user token
Assurances			

• Analysis of the design documentation provided by the Vendor on the authentication protocol. • Functional testing can be used to verify if the authentication protocol is indeed implemented. • Penetration tests can be used to ascertain that attackers cannot bypass the authentication protocol.	2. If the challenge-response protocol is used, the Device SHALL only accept an end-user token ID as valid once the end-user token has been successfully authenticated. 3. The Device SHALL support unique identification (UID). 4. The Device SHALL support disabling the UID identification mechanism remotely. 5. The Device SHALL NOT use a common master key for authentication of any kind. 6. The Device SHALL use a unique key for remote and local authentication. 7. The Device SHALL store its unique key in a Secure Access Module/TPM/HSM. 8. The Device SHALL rely on an internal Secure Access Module (SAM) to manage keys involved in the authentication protocol.

EVSE System Specification Section: Secure Operation			**Charger Type(s):** L2, DCFC, XFC
Source: *NMFTA XFC Cybersecurity Working Group*			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSS-04	Payment System	EVSE	The Device SHALL incorporate a secure payment system that follows payment card industry data security standards (PCI/DSS), which as a minimum includes payment controls such as access control, authentication, physical security (e.g. hardware anti-tampering), logging/auditing, malware detection
Assurances			

EVSE System Specification Section: Secure Operation			**Charger Type(s):** L2, DCFC, XFC
Source: *Volpe Telematics Cybersecurity Primer for Agencies(SC-12, SC-12(1), SC-12(2), SC-12(3) - CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT* [35]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSS-05	Cryptographic Key Management		1. The Utility Operator system SHALL deploy and utilize a PKI or key management system that includes a trusted Certificate Authority. 2. The Utility Operator system SHALL deploy and utilize a Hardware Security Module (HSM) solution for Key storage. See SAE J3101-Requirements for Hardware-Protected Security for Ground Vehicle Applications [39] for guidance.
Assurances			

	3. The Utility Operator Vendor SHALL utilize a certificate escrow to ensure availability in the event of key loss. 4. The PKI or other key management system used SHALL support the generation, issuing, and revocation of cryptographic material. 5. Cryptographic material SHALL be revoked on a configurable periodic basis. Accordingly, new cryptographic material SHALL be generated and issued to authorized relevant parties following the periodic revocation of material.

EVSE System Specification Section: Secure Operation			**Charger Type(s):** L2, DCFC, XFC
Source: *Volpe - Telematics Cybersecurity Primer for Agencies (SC-28 PROTECTION OF INFORMATION AT REST)* [35]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSS-06	Secure Local Storage of Sensitive Information (PII, VIN, Payment Info, etc.)		1. The EVSE Operator and/or Utility Operator system SHALL protect the confidentiality and integrity of Sensitive information stored as part of the Vehicle Identification process for billing/tracking as well as other Personally Identifiable Information.
Assurances			

EVSE System Specification Section: Secure Operation			**Charger Type(s):** L2, DCFC, XFC
Source: *Volpe - Telematics Cybersecurity Primer for Agencies Doc (IA-7 – CRYPTOGRAPHIC MODULE AUTHENTICATION)* [35]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSS-08	Cryptographic Hardware Module Authentication		If used the Vendor SHALL implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive orders, regulations, standards and guidance for such authentication e.g. FIPS 140-2, SL-3, or SL-4 [37]
Assurances			

EVSE System Specification Section: Secure Operation			**Charger Type(s):** L2, DCFC, XFC
Source: *Volpe - Telematics Cybersecurity Primer for Agencies Doc (SI-7(9) Software, Firmware and Information Integrity* [35]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSS-09	Secure power up /power down and secure boot for safe grid operation		1. Vendor SHALL provide evidence of system design that facilities the safe and secure start up and shut down of devices to prevent negative impacts to the power grid 2. The Device SHALL support the use of Secure Boot to increase the resiliency of the Device against compromise and physical manipulation.
Assurances			

EVSE System Specification Section: Secure Operation			**Charger Type(s):** L2, DCFC, XFC
Source: *Volpe Telematics Cybersecurity Primer for Agencies Doc (CA-8(1)* [35]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSS-10	Third-Party Penetration Testing and Security Testing		1. The Vendor shall conduct a third-party penetration and security testing of system and product devices before deployment and the documentation needs to be provided to the Purchaser 2. The Vendor SHALL establish a process for maintaining ongoing third-party penetration and security testing of system and product devices. 2. The Vendor SHALL ensure all applicable devices, technologies and applications are tested as part of the required penetration test. 3. The Vendor SHALL implement a Vulnerability Disclosure Program (VDP) to ensure any security issues identified are addressed in a timely manner to permit the safe public disclosure of the identified vulnerabilities.
Assurances			

5.2.7 Logging

EVSE System Specification Section: Logging			**Charger Type(s):** L2, DCFC, XFC
Source: *NMFTA XFC Cybersecurity Working Group*			
Ref #	**Security Control Area**	**Devices**	**Requirements**

SSL-01	Black Box Recorder		EVSE Device SHALL have a logging device which captures data from internal and external interfaces before and after a vendor-defined security event
Assurances			

EVSE System Specification Section: Logging			**Charger Type(s):** L2, DCFC, XFC
Source: *Volpe - Telematics Cybersecurity Primer for Agencies Doc (SI-4 INFORMATION SYSTEM MONITORING)* [35]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSL-02	Intrusion Detection and Logging of independent power quality and quantity		1. The EVSE Operator system SHALL monitor the information system to detect unauthorized manipulation of power supply stability configurations. 2. The EVSE Operator system SHALL identify and alert Utility Operator admins/operators of power quantity and/or quality levels that fall outside of predetermined thresholds.
Assurances			

EVSE System Specification Section: Logging			**Charger Type(s):** L2, DCFC, XFC
Source: *NMFTA Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cybersecurity Baseline Reference Document-Section 13.3* [3]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSL-03	IDS/IPS systems	EVSE	1. The device SHOULD incorporate an Intrusion Detection System (IDS) and/or an Intrusion Prevention System (IPS). For each event detected: a. the Device SHALL store either onboard or off board the affected interface(s), event type, packet data, system state, time stamp/user, role, or process which caused the event such as log-in attempts, replay attacks, configuration changes, firmware updates/patches, alarms triggered by physical manipulation. 2. The EVSE SHALL allow remote monitoring of information about device status. Time
Assurances			

	synchronization is required to allow log events from different devices on the same network to be correlated.

EVSE System Specification Section: Logging			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 3 Section 3.2 Logging* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSL-04	Logging Security Events (Local Controllers)	Local Controllers	1. The Device SHALL log security events in a locally stored log. 2. The Device SHALL take measures to prevent the ability of attackers to modify, delete or overwrite security logs. 3. The Device SHALL support automatically sending log events to a central logging server. 4. The Device SHOULD allow remote monitoring of information about the device status such as processor and memory usage. 5. The Device SHOULD store for each security event at least the interface, the event type, a time stamp, and the user, role, or process causing the event.
Assurances			
• The implementation of logging mechanisms can be verified in a functional security test. • Carrying out a penetration test can provide further assurance that attackers cannot bypass detection mechanisms or modify the security log.			

EVSE System Specification Section: Logging			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 3 Section 3.2 Logging* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSL-05	Logging Security Events (Authentication Terminals)	Authentication Terminals	1. The Device SHALL send the log security events to the Local Controller. 2. The Device SHOULD send to the Local Controller for each security event at least the interface, the event type, a time stamp, and the
Assurances			

• The implementation of logging mechanisms can be verified in a functional security test. • Carrying out a penetration test can provide further assurance that attackers cannot bypass detection mechanisms or modify the security log.	user, role, or process causing the event.

5.2.8 Lifecycle and Governance

EVSE System Specification Section: Lifecycle and Governance			**Charger Type(s):** L2, DCFC, XFC
Source: *Volpe-Telematics Cybersecurity Primer for Agencies Appendix A* [35]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSLG-01	Vulnerability Disclosure Program	System Wide	1. Vendors SHALL institute a vulnerability disclosure program for receiving, implementing, and addressing vulnerabilities discovered or reported in their products. 2. Vendors SHALL maintain a vulnerability response and vulnerability disclosure program in accordance with established standards such as International Organization of Standards (ISO)/International Electrotechnical Commission (IEC) 29147:2018 (Information technology -- Security techniques -- Vulnerability Disclosure) [40] and ISO/IEC 30111:2013 (Information technology -- Security techniques -- Vulnerability Handling Processes) [41].
Assurances			

EVSE System Specification Section: Lifecycle and Governance			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 4 Product Lifecycle and Governance* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSLG-02	Information Security Management System (ISMS)	System wide	1. The Vendor SHALL implement an Information Security Management System (ISMS), the scope of which includes at least all systems used to develop, test, manufacture and provision the Devices and any software and hardware tools
Assurances			

	needed for the maintenance of the Devices. 2. The Vendor SHOULD have regular audits of the ISMS performed by an accredited external auditor. 3. The Vendors SHALL provide a proof of the audit to the Purchaser on request. 4. The Vendor SHOULD obtain an ISO 27001 [42] certification for the ISMS. 5. The Vendor SHALL make a proof of the certificate available on request. 6. The Vendors SHOULD share their security policies with the Purchaser.

EVSE System Specification Section: Lifecycle and Governance			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 4 Product Lifecycle and Governance* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSLG-03	Configuration Management System	System wide	1. The Vendor SHALL employ a configuration management system for the administration of upgrades to hardware configurations and source code of devices. 2. The Vendor SHALL ensure that the configuration management system stores for each change an explanation, the party which performed the upgrade, the role of the party, the software and/or hardware components that were modified, and the time at which the upgrade was made. 3. The Vendor SHOULD allow the purchaser to audit the configuration management system.
Assurances			

EVSE System Specification Section: Lifecycle and Governance			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 4 Product Lifecycle and Governance* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSLG-04	Vulnerability Management Process	System wide	1. The Vendor SHALL have an established and documented vulnerability management process. 2. The Vendor SHALL continuously monitor information sources (e.g. Common Vulnerabilities and Exposures/Common Weakness Enumeration (CVE/CWE) database) on vulnerabilities to determine if the Device is affected by any existing known vulnerabilities. 3. The Vendor SHALL correct vulnerabilities found by the Vendor itself, the Purchaser or system integrator, or external security
Assurances			

	researchers in a timely manner. 4. The Vendor SHALL disclose to the Purchaser all known vulnerabilities on the Device as soon as possible. 5. The Vendor SHALL communicate vulnerabilities to the Purchaser in a secure manner. 6. The Vendor SHALL issue a recommendation to the Purchaser on how to mitigate a vulnerability as immediately as possible. 7. The Vendor SHALL evaluate the criticality of a vulnerability using established standards such as the Common Vulnerability Scoring System (CVSS). 8. The Vendor SHALL prioritize fixing vulnerabilities based on the potential impact to the Purchaser and to the End Users of the Device. 9. The Vendor SHALL publish their vulnerability disclosure policy

EVSE System Specification Section: Lifecycle and Governance			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 4 Product Lifecycle and Governance* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSLG-05	Security Updates and Patching	System wide	1. The Vendor SHALL provide security updates or patches for the Device to fix high impact vulnerabilities found during the Device's lifecycle. 2. The Vendor SHALL test all security updates and patches prior to deployment. 3. The Vendor SHOULD provide documentation that all security patches were tested and validated prior to deployment. 4. The Vendor SHOULD provide tools enabling batch updating of Devices. 5. The Vendor SHOULD release a patch or firmware update for a vulnerability no more than three months based on the severity of the vulnerability after it was reported to the Vendor.
Assurances			

EVSE System Specification Section: Lifecycle and Governance			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 4 Product Lifecycle and Governance* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**

SSLG-06	Security Training and Awareness		1. The Vendor SHALL be able to document that the necessary knowledge to securely develop and securely produce the EVSE exists and is in use within the Vendor. 2. The Vendor SHALL name a product security officer responsible for security-related matters who acts as contact person for the Purchaser. 3. The Vendor SHOULD provide documented professional experience in the area of IT security or a security.
Assurances			

EVSE System Specification Section: Lifecycle and Governance			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 4 Product Lifecycle and Governance* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSLG-07	Security Production and Credential Provisioning	System wide	1. The Vendor SHALL ensure secure provisioning of cryptographic keys, passwords and initial security credentials during manufacturing and servicing processes. 2. The Vendor SHALL ensure a secure production area to ensure the secure initial provisioning of credentials and cryptographic keys to the device. 3. The Vendor SHALL establish a secure hand-over process of the provisioned information to the central systems of the Purchaser.
Assurances			

EVSE System Specification Section: Lifecycle and Governance			**Charger Type(s):** L2, DCFC, XFC
Source: *NMFTA Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cybersecurity Baseline Reference Document-Section 13.5* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSLG-08	EVSE Incident Response Plan	EVSE	The Vendor SHALL have an incident response plan (such as outlined in NIST 800-61 Computer Security Incident Handling Guide)[43] which is specific to the EVSE that covers EVSE incident response policies and procedures addressing purpose, scope, roles, responsibilities, along with compliance and procedures to facilitate implementation of the incident response policy and associated incident controls.
Assurances			

EVSE System Specification Section: Lifecycle and Governance	**Charger Type(s):** L2, DCFC, XFC
Source: *Department of Defense Instruction 8510: Risk Management Framework for DoD Information*	

Technology			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSLG-09	Assessment and Authorization	EVSE	1. The vendor SHOULD provide Risk Management Framework (RMF) compliant system documentation to assist in any necessary Assessment and Authorization (A&A) activities required by the Authorizing Official for the applicable agency, command, Federal office, etc. 2. The vendor SHALL support testing and evaluation as needed for compliance with any applicable STIGs for technologies. 3. The vendor shall provide support for product updates, documentation/artifact updates and risk mitigation and remediation as identified by the Authorizing Official or his subordinate Security Control Assessor(s) (SCA).
Assurances			

EVSE System Specification Section: Lifecycle and Governance			**Charger Type(s):** L2, DCFC, XFC
Source*: Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework*			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSLG-10	FedRAMP Compliance	EVSE	The vendor, in offering backend EVSE IT infrastructure that includes cloud storage and technology, SHALL be a FedRAMP authorized service provider having been certified by a certified FedRAMP Third Part Assessment Organization (3PAO).
Assurances			

5.2.9 Assurance

EVSE System Specification Section: Assurance			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 5 Assurance* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSA-01	Design Evidence (part 1)	System wide	1. The Vendor SHALL document all interfaces of the Device, including the protocols and services used on each interface.
Assurances			

	2. The Vendor SHALL provide design evidence that sufficient reserves are available to update security functionality to meet requirement SSD-01. 3. The Vendor SHALL provide design evidence that only cryptographic algorithms, protocols, and parameters allowed by the cryptographic algorithms and key length requirements are used for security functions, including a description of which algorithms, protocols, and parameters are used for which functions. 4. The Vendor SHALL provide design evidence that cryptographic random number generation is implemented according to requirement SSCR-02, including a description of which random number generator is used. 5. The Vendor SHALL provide design evidence of the authentication protocol required in for SSCO-01. 6. The Vendor SHALL provide design evidence that firmware authenticity is protected as required in SSCO-02 including a step-by- step description of the firmware update process. 7. The Vendor SHALL provide design evidence that unused interfaces are disabled or removed to meet requirement SSH-03.

EVSE System Specification Section: Assurance			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 5 Assurance* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSA-02	Design Evidence (part2)	System wide	8. If interfaces or services are disabled and not removed, the Vendor SHALL provide information on how they have been disabled. 9. If security-enhancing features as described in requirements SSH-04 are used, the Vendor SHALL provide design evidence on how they are used. 10. The Vendor SHALL provide design evidence on how the Device has been made fail-secure to meet requirement SSR-02, including a list of all relevant failure types and their countermeasures. 11. The Vendor SHALL provide design evidence that user authentication is implemented as required in SSS-01 12. The Vendor SHALL provide design evidence
Assurances			

	that security logging is implemented as required in SSL-03. The Vendor SHALL provide design evidence at a level of detail that makes it easy to verify that the security requirements are implemented, and to test that they are implemented on the Device as described. 13. The Vendor SHALL allow verification of the design evidence by an independent third party selected by the Purchaser.

EVSE System Specification Section: Assurance			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 5 Assurance* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSA-03	Security Testing	System wide	1. The Vendor SHALL perform tests to verify that all the security requirements identified in this document have been implemented correctly. 2. The Vendor SHALL test the complete functional scope of the Device prior to deployment or sale of the Device, including the communication chain between the Device and all connected field devices and the central systems. 3. The Vendor SHALL periodically test both regularly used as well as rarely used functionalities of the Device. 4. The Vendor SHALL document the concepts and details of the security tests in a comprehensible way. 5. The Vendor SHALL use vulnerability scanners to test each firmware version for known vulnerabilities prior to release and administration of the firmware update to Devices. 6. The Vendor SHALL allow the Purchaser to contract an independent test lab to perform a security tests on the Device. 7. The Vendor SHALL conduct robustness tests, such as fuzzing or flooding, on all protocols used by the device both on the application layer and on lower operating system/networking layers. 8. The Vendor SHALL conduct periodic design reviews and code reviews and provide the results of these reviews to the Purchaser.
Assurances			

EVSE System Specification Section: Assurance	**Charger Type(s):** L2, DCFC, XFC

Source: *ElaadNL-Chapter 5 Assurance* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSA-04	Secure Coding Practices	System wide	1. The Vendor SHALL establish and enforce the use of secure coding practices in the development of the Device following established best practices such as the MISRA and CERT Secure Coding Standards. 2. The Vendor SHALL establish an internal code review process that in part reviews the security of source code and integrated third party code libraries. 3. The Vendor SHALL use automated code analysis tools to scan all source code for security vulnerabilities.
Assurances			

EVSE System Specification Section: Assurance			**Charger Type(s):** L2, DCFC, XFC
Source: *Volpe - Telematics Cybersecurity Primer for Agencies (RA-5 VULNERABILITY SCANNING)* [35]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSA-05	Vulnerability Scanning of Device and Backend		1. Vendor SHALL execute vulnerability scans of all networking equipment and remote backend and cloud servers used in connection with the Device. 2. Vendor SHALL follow an established process for reporting and disclosing identified vulnerabilities such as the Common Vulnerabilities and Exposures system (CVE).
Assurances			

5.2.10 EVSE Operator/Utility Operator Communications

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSOC-01	EVSE Operator Confidentiality	EVSE Operator's system	1. The EVSE Operator's system SHALL protect the confidentiality of all communications with encryption using a protocol allowed by the
Assurances			

	cryptographic algorithms and key length requirements over the EVSE Operator's interface. 2. The EVSE Operator's SHALL protect the confidentiality of communication by encrypting it using a protocol allowed by the cryptographic algorithms and key length requirements over the WAN interface.

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSOC-02	Utility Operator Confidentiality	Distribution System	The Utility Operator system SHALL protect the confidentiality of communications over the EVSE Operator interface with encryption using a protocol allowed by the cryptographic algorithms and key length requirements.
Assurances			

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSOC-03	EVSE Operator Message Integrity		1. If the EVSE Operator system detects that a message has been modified or if it cannot verify the integrity of the message over the EVSE Operator interface, it SHALL reject or drop the message. 2. The EVSE Operator system SHALL allow parties it communicates with; to verify the integrity of application layer messages it sends by using a message authentication algorithm allowed by the cryptographic algorithms and key length requirements over the EVSE Operator interface. 3. The EVSE Operator system SHALL verify the integrity of application layer messages received, using a message authentication algorithm allowed by the cryptographic algorithms and key length requirements over the WAN interface. 4. If the EVSE Operator system detects that a message has been modified or if it cannot verify the integrity of the message over the WAN interface, it SHALL reject or drop the message.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Functional tests can be used to verify that the EVSE Operator system supports the required functionality. • Carrying out a penetration test can be used to determine if the EVSE Operator system verifies message integrity under all conditions.			

	5. The EVSE Operator system SHALL allow parties it communicates with; to verify the integrity of application layer messages it sends by using a message authentication algorithm allowed by the cryptographic algorithms and key length requirements over the WAN interface.

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSOC-04	Utility Operator Message Integrity		1. If the Utility Operator's system detects that a message has been modified or if it cannot verify the integrity of the message over the EVSE Operator interface, it SHALL reject or drop the message. 2. The Utility Operator system SHALL allow parties it communicates with; to verify the integrity of application layer messages it sends by using a message authentication algorithm allowed by the cryptographic algorithms and key length requirements.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Functional tests can be used to verify that the Utility Operator system supports the required functionality. • Carrying out a penetration test can be used to determine if the Utility Operator system verifies message integrity under all conditions.			

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSOC-05	EVSE Operator Message Authentication		1. The EVSE Operator system SHALL be able to determine that the source of a sensor reading request or control command is a specific host in the EV Charging system.
Assurances			

• Analysis of the design documentation provided by the Vendor on the mechanisms used for message authentication. • Functional testing can be used to verify if the mechanisms are indeed implemented. • Penetration tests can be used to ascertain that attackers cannot bypass the authentication mechanisms.	2. The EVSE Operator system SHALL be able to determine that the source of message is the Utility Operator system.

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSOC-06	Utility Operator Message Authentication		The Utility Operator system SHALL be able to determine that the source of a message is the EVSE Operator system.
Assurances			
• Analysis of the design documentation provided by the Vendor on the mechanisms used for message authentication. • Functional testing can be used to verify if the mechanisms are indeed implemented. • Penetration tests can be used to ascertain that attackers cannot bypass the authentication mechanisms.			

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			**Charger Type(s):** L2, DCFC, XFC
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [2]			
Ref #	**Security Control Area**	**Devices**	**Requirements**
SSOC-07	EVSE Operator Message Integrity Verification		1. The EVSE Operator system SHALL verify the integrity of all messages it receives. 2. The EVSE Operator system SHALL reject or drop messages that are invalid or for which the integrity cannot be verified.
Assurances			
• It is recommended to carry out fuzzing tests on all interfaces. • The Vendor should provide a detailed documentation of all security tests.			

EVSE System Specification Section: EVSE OPERATOR/Utility	**Charger Type(s):** L2, DCFC, XFC

<table>
<tr><td colspan="3">Operator Communications</td><td></td></tr>
<tr><td colspan="4">Source: ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication [2]</td></tr>
<tr><td>Ref #</td><td>Security Control Area</td><td>Devices</td><td>Requirements</td></tr>
<tr><td>SSOC-08</td><td>Utility Operator Message Integrity Verification</td><td></td><td rowspan="3">1. The Utility Operator system SHALL verify the integrity of all messages it receives.
2. The Utility Operator system SHALL reject or drop messages that are invalid or for which the integrity cannot be verified.</td></tr>
<tr><td colspan="3">Assurances</td></tr>
<tr><td colspan="3">• It is recommended to carry out fuzzing tests on all interfaces.
• The Vendor should provide a detailed documentation of all security tests.</td></tr>
</table>

6 Applicable Guidance Documents for EVSE Cybersecurity

Document Name	Document Description
NIST Special Publication 800-53 Rev 4 – Security and Privacy Controls for Federal Information Systems and Organizations	This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors (both intentional and unintentional).
NIST Special Publication 800-61 Computer Security Incident Handling Guide	This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively.
ISO 15118-2:2014 – Road to Vehicles – Vehicle to Grid Communication Interface – Part 1: General Information and Use-Case Definition	This document provides a general overview and a common understanding of aspects influencing identification, association, charge or discharge control and optimization, payment, load levelling, cybersecurity and privacy. It offers an interoperable EV-EV supply equipment interface to all e-mobility actors beyond SECC
NMFTA Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cybersecurity Baseline Reference Document	This document is a comprehensive review of cybersecurity for electric medium and heavy duty vehicles, charging stations and the electric grid. This document provides a reference baseline for the various stakeholders in heavy duty electric vehicle charging.
NIST Special Publication (SP) 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.	This publication develops the next-generation Risk Management Framework (RMF) for information systems, organizations, and individuals, in response to Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, OMB Circular A-130, Managing Information as a Strategic Resource, OMB Memorandum M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, and OMB Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program.
European Network for Cyber Security, EV Charging Systems Security Requirements	This document describes security requirements for EVSE
Extreme Fast Charging (XFC) Cybersecurity Threats, Use Cases and Requirements For Medium and Heavy Duty Electric Vehicles	This document was produced by DOT Volpe for the NMFTA and presents threats and cybersecurity requirements for both Medium and Heavy Duty Electric Vehicle (MD/HDEV) Extreme Fast Charging (XFC) systems.
Unified Facilities Criteria (UFC) Cybersecurity of Facility-Related Control Systems	This UFC describes requirements for incorporating cybersecurity in the design of all facility-related control systems. It defines a process based on the Risk Management Framework suitable for control systems of any impact rating, and provides specific guidance suitable for control systems assigned LOW or MODERATE impact level.
NIST Special Publication 800-82 – Guide to Industrial Control Systems (ICS) Security	This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements
International Organization for Standardization, ISO/IEC 29147:2018-Information technology-Security techniques-Vulnerability disclosure	This document provides requirements and recommendations to vendors on the disclosure of vulnerabilities in products and services.
International Organization for Standardization, ISO/IEC 30111:2013-Information technology-	This document provides guidelines for how to process and resolve potential vulnerability information in a product or online service.

Security techniques-Vulnerability handling	
International Organization for Standardization, ISO/IEC 27001 Certification Information security management systems	A family of standards designed help an organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to them by third parties.
FIPS 186-4 Digital Signature Standard	This standard specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory.
FIPS 140-2 Security Requirements for Cryptographic Modules	This Federal Information Processing Standard (140-2) specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments.

Table 5: EVSE Cybersecurity Applicable Publications

7 Conclusion

The electrification of government vehicle fleets will continue as it leverages the operational cost savings and emissions improvements of electric vehicles. While the rate at which EVs and EVSE are being procured and deployed is steadily increasing, there is still a window of opportunity to get ahead of the curve in cybersecurity for these systems.

Too often the cybersecurity considerations of a new electronic product or system are overlooked resulting in resource-intensive, time consuming, and less than adequate post-deployment applications of cybersecurity controls. The EVSE cybersecurity requirements and considerations identified in this report are intended to be used as a starting point for those organizations (i.e. DoD, Federal Government, State and Local Governments/Municipalities, and Law Enforcement agencies) which procure, operate, or interface with EV and EVSEs. As with any cybersecurity tool, these requirements are not final formal standards but rather an initial step toward the development of a robust and thoroughly vetted standard.

8 References

1. DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report: https://rosap.ntl.bts.gov/view/dot/34991

2. European Network for Cyber Security, EV Charging Systems Security Requirements: https://www.elaad.nl/uploads/downloads/downloads_download/Security_Requirements_Charge_Points_v1.01_august2017.pdf

3. National Motor Freight Traffic Association, NMFTA Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cybersecurity Baseline Reference Document: http://www.nmfta.org/

4. Extreme Fast Charging (XFC) Cybersecurity Threats, Use Cases and Requirements For Medium and Heavy Duty Electric Vehicles: https://github.com/nmfta-repo/nmfta-hvcs-xfc

5. National Plug-In Electric Vehicle Infrastructure Analysis: https://www.nrel.gov/docs/fy17osti/69031.pdf

6. ChargePoint Home security research: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/12/13084354/ChargePoint-Home-security-research_final.pdf

7. Schneider Electric EVLink Parking ICS Advisory (ICSA-19-031-01): https://www.us-cert.gov/ics/advisories/ICSA-19-031-01

8. Mathias Delheimer Chaos Communication Congress Presentation (English Translation): https://www.youtube.com/watch?v=szYeqOIQ9Bw

9. Circontrol CirCarLife ICS Advisory (ICSA-18-305-03): https://www.us-cert.gov/ics/advisories/ICSA-18-305-03

10. Public Plug-In Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?: https://arxiv.org/pdf/1907.08283.pdf

11. Losing The Car Keys: Wireless PHY-Layer Insecurity in EV Charging: https://www.youtube.com/watch?v=4VaXqtZkQmE https://www.usenix.org/conference/usenixsecurity19/presentation/baker

12. BloombergNEF Global Passenger Sales Outlook: https://about.bnef.com/electric-vehicle-outlook/

13. EVAdoption EV Sales Forecast: https://evadoption.com/ev-sales/ev-sales-forecasts/

14. Gannon, Rob, *With some all-electric buses, Metro Transit rides into the future*, The Seattle Times, (02 October 2017). Retrieved 03 May 2018 from https://www.seattletimes.com/opinion/with-some-all-electric-buses-metro-transit-rides-into-the-future/

15. Technavio, *Global Electric Bus Market 2016-2020*, published by Technavio, (April 2016). Retrieved 03 May 2018 from https://www.

16. Bloomberg Electric Vehicle Outlook 2019: https://about.bnef.com/electric-vehicle-outlook/

17. the NIST 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach:* https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final

18. NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations:* https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

19. Cloud Security Alliance (CSA): https://cloudsecurityalliance.org/

20. EVSE Awarded Under GSA BPA: https://www.gsa.gov/cdnstatic/All_Configurations_Awarded.pdf

21. Safeguarding Covered Defense Information and Cyber Incident Handling: https://www.law.cornell.edu/cfr/text/48/252.204-7012

22. Federal Risk and Authorization Management Program (FedRAMP): https://fedramp.gov/

23. Fixing America's Surface Transportation Act (FAST Act): https://www.fhwa.dot.gov/fastact/

24. SANS A Black Box Approach to Embedded Systems Vulnerability Assessment: https://www.sans.org/reading-room/whitepapers/riskmanagement/black-box-approach-embedded-systems-vulnerability-assessment-37452

25. OWASP IoT Testing Guides: https://www.owasp.org/index.php/IoT_Testing_Guides

26. NIST SP 800-115 *Technical Guide to Information Security Testing and Assessment*: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

27. NIST National Vulnerability Database: https://nvd.nist.gov/800-53/Rev4/control/CA-8

28. National Renewable Energy Laboratory's Vehicle Cybersecurity Threats and Mitigation Approaches report: https://www.nrel.gov/docs/fy19osti/74247.pdf

29. Idaho National Laboratory Cyber Assessment Report of Level 2 AC Powered Electric Vehicle Supply Equipment: https://avt.inl.gov/sites/default/files/pdf/reports/Level2EVSECyberReport.pdf

30. DOE's Federal Energy Management Program Fleet Cybersecurity Toolkit: https://www.energy.gov/eere/femp/federal-fleet-cybersecurity

31. International Organization for standardization, ISO 15118-2:2014 Road vehicles-Vehicle to Grid

Communications Interface-Part 2: Network and Application Protocol Requirements: https://www.iso.org/standard/55366.html

32. UPTANE Securing Software Updates for Automobiles: https://uptane.github.io/

33. Open Charge Alliance: https://www.openchargealliance.org/

34. Internet Engineering Task Force: https://www.ietf.org/

35. Telematics Cybersecurity Primer for Agencies: https://neutralvehicle.com/Cyber-PrimerforFM_Final%20Draft%20V8%20[Public].pdf

36. FIPS 186-4 Digital Signature Standard: https://csrc.nist.gov/publications/detail/fips/186/4/final

37. FIPS 140-2 Security Requirements for Cryptographic Modules: https://csrc.nist.gov/publications/detail/fips/140/2/final

38. NIST 800-63-3/B Digital Identity Guides: https://csrc.nist.gov/publications/detail/sp/800-63/3/final

39. SAE J3101 Requirements for Hardware-Protected Security for Ground Vehicle Applications: https://www.sae.org/standards/content/j3101/

40. International Organization for Standardization, ISO/IEC 29147:2018-Information technology-Security techniques-Vulnerability disclosure: https://www.iso.org/standard/72311.html

41. International Organization for Standardization, ISO/IEC 30111:2013-Information technology-Security techniques-Vulnerability handling: https://www.iso.org/standard/53231.html

42. International Organization for Standardization, ISO/IEC 27001 Certification Information security management systems: https://www.iso.org/isoiec-27001-information-security.html

43. NIST 800-61 Computer Security Incident Handling Guide: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Appendix A: Threat Actors, STRIDE Threat Model, and Attack Impacts

Threat Actors

Threat Actor Profiles
This section briefly reviews attacker motivations in the context of the range of cyber attackers, whether a lone attacker, an insider threat, an organized group with malicious intent, or a hostile nation state. These factors can be psychological, technical, financial, and/or political. It also explores why an EVSE unit and its unique vulnerabilities may represent an attractive target.

There is an important difference between a "hacker" and "attacker." In this document, a hacker is a person who uses cybersecurity tools to exploit system vulnerabilities and/or create new methods to exploit vulnerabilities. An attacker is a hacker who uses these cybersecurity tools in an intentionally malicious fashion.

Although the profiles below describe certain classes of attackers, consideration also needs to be given to the intent and capability of the attacker. One inherent danger of cyber-attacks is the use of "canned" or cookbook attack instructions combined with the occasional reluctance of equipment owners to patch known vulnerabilities. This combination greatly enhances the capability of less sophisticated attackers (e.g., a "script kiddie" who is simply unaware of ramifications of their actions).

Individual or Lone Attacker
The expertise of individual attackers (e.g., hobbyist hackers, rogue mechanics) can vary widely, from that of "script kiddies" who use tools developed by others to that of experts with advanced knowledge of embedded systems. Individual attackers can also have varying levels of access to the target system's data. Basic and advanced access information might be obtained from online communities. Sometimes proprietary information can be gleaned from physical access to the device.

Insider Threats
Insider threat attackers (e.g., disgruntled employees) usually benefit from having both specialized knowledge about the target and broad authorized access to the system. They may also have direct access to proprietary data. An insider is more likely to know where the system's vulnerabilities lie and what mitigations need to be overcome. An insider may be motivated personally or may be susceptible to promises of financial gain for disclosing critical knowledge of the system. A disgruntled employee can theoretically be associated with any element in the EVSE system's supply chain, from the equipment designer to the vendor to the network operator/aggregator.

Hacking Collectives

In contrast to the individual attacker, hacking collectives synergistically pool the efforts of multiple hackers and attackers. Collectives can be motivated by their association with external groups (e.g., hacktivists, organized crime, nation states). The collective known as "Anonymous," for example, operates using a decentralized group model and has a global following. It is known for hacking many organizations including the Pentagon, Visa, MasterCard and PayPal.

Criminal Organizations and Enterprises

Criminal groups are motivated by potential financial gain. The EVSE community is certainly vulnerable to traditional criminal activities, such as payment fraud, which might be enabled by existing cybersecurity tools.

Nation States

Nation states typically have the greatest financial and technological resources and therefore employ the most sophisticated tools and techniques. They may seek intellectual property, military intelligence, proprietary technology, or other private data for competitive advantage or even propaganda value. They may also investigate methods to strategically cripple industries through large-scale cyber-attacks. These attackers typically employ complex attack methods such as supply chain attacks, sophisticated malware deployments, distributed and strategically orchestrated attacks on targets, and long-term (months or years) reconnaissance and information gathering campaigns.

STRIDE Threat Model

The Microsoft STRIDE model characterizes known threats according to the types of exploit that are used. The STRIDE acronym is made up of the first letter of each of the threat categories in Table 6. STRIDE threats are evaluated for each component of the system and their interactions.

Types (STRIDE Method[1])
Spoofing Identity: *Spoofing* is a key risk for applications that have many users but provide a single execution context at the application and database level. In particular, users should not be able to become any other user or assume the attributes of another user.
Tampering with Data: Users can potentially change data delivered to them, return it, and thereby potentially manipulate client-side validation, GET and POST results, cookies, HTTP headers, and so forth. The application should not send data to the user, such as interest rates or periods, which are obtainable only from within the application itself. The application should also carefully check data received from the user and validate that it is sane and applicable before storing or using it.
Repudiation: Users may dispute transactions if there is insufficient auditing or recordkeeping of their activity. For example, if a user says, "But I didn't transfer any money to this external account!", and you cannot track his/her activities through the application, then it is extremely likely that the transaction will have to be written off as a loss. Therefore, consider whether the application requires non-repudiation controls, such as web access logs, audit trails at each tier, or the same user context from top to bottom. Preferably, the application should run with the user's privileges, not more, although this may not be possible with many off-the-shelf application frameworks.
Information Disclosure: Users are rightfully wary of submitting private details to a system. If it is possible for an attacker to publicly reveal user data at large, whether anonymously or as an authorized user, there will be an immediate loss of confidence and a substantial period of reputation loss. Therefore, applications must include strong controls to prevent user ID tampering and abuse, particularly if they use a single context to run the entire application. Also, consider if the user's web browser may leak information. Some web browsers may ignore the no caching directives in HTTP headers or handle them incorrectly. Similarly, every secure application has a responsibility to minimize the amount of information stored by the web browser in case it leaks or leaves information behind which can be used by an attacker to learn details about the application, the user, or to potentially become that user. Finally, when implementing persistent values, keep in mind that the use of hidden fields is insecure by nature. Such storage to secure sensitive information or to provide adequate personal privacy safeguards is unreliable.
Denial of Service: Application designers should be aware that their applications may be subject to a denial of service attack. Therefore, the use of expensive resources such as large files, complex calculations, heavy-duty searches, or long queries should be reserved for authenticated and authorized users and not available to anonymous users. For applications that do not have this luxury, every facet of the application should be engineered to perform as little work as possible, to use fast and few database queries, and to avoid exposing large files or unique links per user in order to inhibit simple denial of service attacks.

[1] The Open Web Application Security Project Threat Risk Modeling (https://www.owasp.org/index.php/Threat_Risk_Modeling)

Elevation of Privilege: If an application provides distinct user and administrative roles, then it is vital to ensure that the user cannot unilaterally elevate his/her privilege level. In particular, simply not displaying privileged role links is insufficient. Instead, all actions should be gated through an authorization matrix to ensure that only the authorized users can access privileged functionality.

Table 6: STRIDE Model

The tables below list the main component areas of the EVSE environment and contain threat categories, attack vectors, impacts.

Electric Vehicle Supply Equipment

EVSE System Component: *Charging Station*			
Threat Category	*Attack Vectors*	*Impact*	*EVSE Requirement Section*
Spoofing	Modules: Core Removable Storage Interfaces: Wide Area Network (WAN) Authentication Terminal Local Area Network (LAN)	• Unauthorized physical access • Firmware manipulation • Unauthorized access to services • Firmware in-transit manipulation • Access to system files • Enable unauthorized services • Configuration changes • Remote login via webservers Under/Over Charging	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Assurance EVSE-O/Utility Operator Communications

Tampering	Modules: Core Removable Storage Interfaces: WAN	• Firmware manipulation • Values measured manipulation • Unauthorized access to the device • Integrity errors (e.g. configurations) • Failures during execution of cryptographic functions • Physical manipulation • Unauthorized physical access • Improper data processing • Man in-the-Middle (MITM) • Packet manipulation • Forecasts manipulation • Arbitrary Code Execution • Under/Over Charging	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Assurance EVSE-O/Utility Operator Communications
Repudiation	Interfaces: WAN Authentication Terminal LAN	• Firmware manipulation • Values measured	Design Cryptography Communication Hardening Secure Operation EVSE-O/Utility Operator Communications
Information Disclosure	Modules: Core Removable Storage Interfaces: WAN Authentication Terminal LAN	• Disclosure of personal data • Eavesdropping • Economic espionage	Design Cryptography Communication Hardening Secure Operation Assurance EVSE-O/Utility Operator Communications
Denial of Service (DoS)	Modules: Core Removable Storage Interfaces: WAN Authentication Terminal LAN	• Resource exhaustion (DoS) • Improper data processing • MITM • Packet manipulation	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Assurance EVSE-O/Utility Operator Communications

Elevation of Privilege	Modules: Core Removable Storage Interfaces: WAN Authentication Terminal LAN	• Firmware manipulation • Values measured manipulation • Unauthorized access to the device • Integrity errors (e.g. configurations) • Failures during execution of cryptographic functions • Physical manipulation • Unauthorized physical access • Arbitrary Code Execution • Unauthorized access to services • Unauthorized access to components Under/Over Charging	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Assurance EVSE-O/Utility Operator Communications

Authentication Terminal

EVSE System Component: *Authentication Terminal*			
Threat Category	*Attack Vectors*	*Impact*	*EVSE Requirement Section*
Spoofing	Modules: Core Interfaces: User Authentication Interface	• Physical manipulation • Unauthorized physical access • Firmware manipulation via Charging Station • Unauthorized access to charging functions	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications

Tampering	Modules: Core Interfaces: User Authentication Interface	• Firmware manipulation • Radio Frequency Identification User Identification (RFID UID) manipulation • Unauthorized access to the device • Integrity errors (e.g. configurations) • Failures during execution of cryptographic functions • Physical manipulation • Unauthorized physical access • User impersonation • Man in the middle • Packet manipulation	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications

Repudiation	Interfaces: Authentication Terminal	• Firmware manipulation	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications
Information Disclosure	Modules: Core	• Disclosure of personal data	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications

Denial of Service	Modules: Core	• Resource exhaustion (DOS)	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications
Elevation of Privilege	Modules: Core	• Firmware manipulation • Values measured manipulation • Unauthorized access to the device • Integrity errors (e.g. configurations) • Failures during execution of cryptographic functions • Physical manipulation • Unauthorized physical access	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications

EVSE Vendors

EVSE System Component: *EVSE Vendors*			
Threat Category	*Attack Vectors*	*Impact*	*EVSE Requirement Section*
Spoofing	Interfaces: WAN EVSE Vendor Interface	• Unauthorized access to services • Firmware in-transit manipulation • Access to system files • Enable unauthorized services • Configuration changes • Remote login via webservers • Access to the EVSE Vendor system	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications
Tampering	Modules: WAN EVSE Vendor Interface	• Improper data processing • Man in the middle • Packet manipulation • Forecasts manipulation • Arbitrary Code Execution • Integrity errors (e.g. configurations)	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications
Repudiation	Interfaces: WAN	• Firmware manipulation • Values measured manipulation	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications

Information Disclosure	Interfaces: WAN EVSE Vendor Interface	• Disclosure of personal data • Eavesdropping • Economic espionage	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications
Denial of Service	Interfaces: WAN EVSE Vendor Interface	• Improper data processing • Man in the middle • Packet manipulation	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications
Elevation of Privilege	Interfaces: WAN EVSE Vendor Interface	• Arbitrary Code Execution • Integrity errors (e.g. configurations) • Unauthorized access to services • Unauthorized access to components	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications

GRID Operator

EVSE System Component: *Grid Operator*			
Threat Category	*Attack Vectors*	*Impact*	*EVSE Requirement Section*
Spoofing	Interfaces: EVSE Vendor Interface	• Unauthorized access to services • Access to system files • Enable unauthorized services • Configuration changes • Remote login via webservers • Access to the EVSE Vendor system	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications
Tampering	Modules: EVSE Vendor Interface	• Improper data processing • Man in the middle • Packet manipulation • Forecasts manipulation • Arbitrary Code Execution	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications

Information Disclosure	Interfaces: EVSE Vendor Interface	• Disclosure of personal data • Eavesdropping • Economic espionage	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications
Denial of Service	Interfaces: EVSE Vendor Interface	• Improper data processing • Man in the middle • Packet manipulation	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications
Elevation of Privilege	Interfaces: EVSE Vendor Interface	• Arbitrary Code Execution • Integrity errors (e.g. configurations) • Unauthorized access to services • Unauthorized access to components	Design Cryptography Communication Hardening Resiliency Secure Operation Logging Lifecycle and Governance Assurance EVSE-O/Utility Operator Communications

Attack Impacts

It is important to understand the potentially severe effects of cybersecurity issues to industry and to the national infrastructure. The resulting damage could run from thousands to hundreds of millions of dollars in losses and significantly compromise national security. The following examples are not meant to be exhaustive, merely indicative of impacts that a cybersecurity attack on EVSE (or a network of EVSE) could have.

Safety Impacts

Human life is always the highest priority when deploying any system. With appropriate access, an attacker could overcharge a vehicle or bypass safety features to overload the EVSE. This could lead to vehicle or EVSE unit fires, personal injury, and loss of life. These threats becomes more critical when the span of potential attack vectors is increased by connecting EVSE to a LAN or other IP-based network. The combination of network-connected technology with a direct connection to the power grid and substations represents an unacceptable opportunity to inflict damage to people and property.

Critical Infrastructure Impacts

The smart grid is considered critical infrastructure by DHS. The junction of power grids and transportation creates a nexus of mission critical systems and services whose disruption can have significant impacts on national security. Weaknesses in the design and implementation of commercial or federal EVSE units could have national security implications such as:

- Extended power outages, whether limited to a single naval installation or spreading across a broad geographic region.
- Damage and destabilization of power-generating assets, such as through abrupt load changes.
- Interruption of public and private transportation networks leading to gridlocks and stranding.

Financial/Economic Impacts

A cybersecurity attack on an EVSE and/or its supporting infrastructure could significantly impact the financial and economic programs surrounding government EVSE. The operational support, maintenance and sustainment of the government's EVSE inventory and the associated growth of ESVE infrastructure depends on the funds providing through the EVSE billing process. Should an EVSE network or its backend systems be compromised, NAVFAC might be unable to bill the appropriate command/program for the time and energy utilized. If EVSE units are made available for employee use for personal EVs, the public payment system could have additional impacts, such as identity theft of employees.

Although ESVE units must ultimately connect to the power grid, this connectivity does engender some risks. The ability to disrupt power and transportation capabilities could be an effective weapon in international conflicts. As such, it should be assumed that adversaries are already working towards this goal, as evidenced by recent cyber-attacks[2] against Ukrainian utilities.

[2] How Ukrain Became a test bed for cyberweaponry - https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/

Appendix B: Glossary

Attackers – an entity, nation state or individual with malicious intent aiming to damage, alter, manipulate or otherwise disrupt the intended function and operation of a system.

Authentication Terminal Interface– The data connection that provides communication between the authentication terminal and the Controller.

Authentication Terminal – The device and/or portion of an extreme fast charging system utilized by the user to authenticate to in order to utilize the charging system.

Availability – In the context of this report and an extreme fast charging system, availability refers to the amount of "up time" and state of readiness for a user to utilize the charging system.

Code Signing – digitally signing of executable code to ensure, at the point of execution, that the code has not been altered or modified since being signed.

Confidentiality – In the context of extreme fast charging systems, confidentiality refers to the system's features and abilities to protect and maintain the confidentiality of data.

Controller – the controller, or XFC controller, is the interface between the internal charging system components and those necessary outside communications connections such as the utilities and vendor systems.

Device - in the context of an XFC, a device identifies a component included in the EV charging system. A device can contain Modules and can have Interfaces to communicate with other devices.

Entity – in the context of an XFC, an entity identifies the physical part of the Device where important functionalities are to be found.

Extreme Fast Charging – XFC systems are meant to provide heavy duty electric vehicles quick and efficient charging capabilities with power outputs of 300KW – 1MW

Information Security Management System – a system of technology, devices, personnel and policy implemented by an organization to protect the confidentiality, integrity and availability of their data and IT assets.

Integrity – in the context of extreme fast charging systems, integrity refers to the system's ability, through design and security controls, to maintain the completeness and accuracy of information that is stored and transmitted through the system.

LAN Interface – Local Area Network interface providing data communication between the controller and extreme fast charging system.

Lifecycle – lifecycle refers to the sequence of stages that a product or asset goes through during the span of its development and/or ownership. This can include but is not limited to its procurement, deployment, usage, decommission and disposal.

Module – within an XFC, a module is defined as a physical part of a device where specific functionalities are to be found.

Over the Air Updates – OTA updates refers to the distribution of updates to software or firmware packages via mobile devices and networks.

Personally Identifiable Information (PII) – Information about an individual maintained by a company, agency or other entity that can be used to determine a person's identity such as name, social security number or date and place of birth as well as information that is linkable to an individual such as medical or financial information.

Protocols – protocols are networking standards and rules that define the way communication takes place between multiple devices.

Secure Access Module – a secure, integrated circuit on a smart card used to enhance the security and cryptography functions of devices.

Security Functions – features or capabilities of a devices or application designed to provide security enhancements for the environment in which they are installed.

Security-Enhanced Features – Security enhanced features are software or devices features or functions that have been enhanced to include security related functionality.

Services – in networking, services are applications that run at the network application layer or higher in the OSI model. These services provide storage, manipulation, presentation and commination capabilities for data.

Vulnerability – weakness or security shortcoming that provides an attack vector that a malicious user could exploit in an attack on the system.

WAN Interface – The Wide Area Network remotely connects the XFC vendor and utility/power management companies to the XFC controller.

U.S. Department of Transportation
John A. Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142-1093

617-494-2000
www.volpe.dot.gov