



Sample Cybersecurity Clauses for EV Charging Infrastructure Procurements

*Lori Ross O'Neil, Thomas E. Carroll, Entesar M. Abdelhadi, Mark D. Watson, Carol L. Hammer,
Maria B. Psarakis*

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights.** Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <<https://www.ntis.gov/about>>
Online ordering: <http://www.ntis.gov>

Revision History

Version	Date	Author	Rationale
0.1	5/26/23	PNNL	Initial draft version for review by Joint Office
0.2	5/31/23	JOET	Proposed revisions & comments
1.0	6/30/23	PNNL & JOET	Released version. PNNL clearance number PNNL-34454

Acknowledgments

The Pacific Northwest National Laboratory and Idaho National Laboratory project teams gratefully acknowledge the guidance and assistance provided by Mr. Brendan Harris of the U.S. Joint Office of Energy and Transportation. We also extend our thanks to various industry stakeholders who met with us and shared their thoughts and experience, including Arizona Department of Transportation, Minnesota Department of Transportation, Oregon Department of Transportation, IO Active, Berkshire Hathaway, and Seattle City Light. The accuracy of the information and the perspectives presented in this report are the responsibility of the authors.

List of Abbreviations & Acronyms

AGA	American Gas Association
CISA	Cybersecurity & Infrastructure Security Agency
CSA	Cloud Security Alliance
CSMS	Charging Station Management System
DHS	Department of Homeland Security
DOE	Department of Energy
DOT	Department of Transportation
EMV	Eurocard Mastercard Visa
ENCS	European Network for Cybersecurity
EV	electric vehicle
EVSE	electric vehicle supply equipment
EVCI	electric vehicle charging infrastructure
EVSP	electric vehicle service provider
FIPS	Federal Information Processing Standards
INL	Idaho National Laboratory
IoT	Internet of Things
IT	information technology
NEVI	National Electric Vehicle Infrastructure
NIST	National Institute of Standards & Technology
NPRM	Notice of Proposed Rulemaking
OT	operational technology
PCI DSS	Payment Card Industry Data Security Standard
PKI	public key infrastructure
PNNL	Pacific Northwest National Laboratory

Executive Summary

Electric vehicle charging infrastructure (EVCI) exhibits character traits of cloud computing, Internet of Things, and operational technology (OT). Critically, high-level communications and interconnectedness underlie it all. The benefits of connected technologies also come with cybersecurity risks, which must be managed and are managed most effectively early in the systems engineering process. States and other EVCI purchasers can reduce their exposure to cybersecurity risks by including sample cybersecurity procurement language clauses that clearly communicate cybersecurity requirements.

The proposed sample cybersecurity clauses for EVCI procurements are designed to assist in managing the risk of cyberattacks that may degrade the safety, security, and reliability of EVCI. The sample clauses are intended to be tailored and incorporated into procurement specifications for equipment and services related to the National EV Infrastructure Formula Program deployments. Widespread adoption of the sample cybersecurity procurement language will integrate cybersecurity throughout the life cycle of the infrastructure.

This document is a tool and an informative resource to be used in conjunction with other general procurement guidance for assisting state departments of transportation in defining cybersecurity-related procurement specifications. It is not intended to set policy or establish or replace any standards. The intention of this document is not to serve as a substitute or alternative to the National Electric Vehicle Infrastructure Formula Program, as stated in Title 23 Code of Federal Regulations (CFR) Part 680, but rather to provide support and enhancement.

Table of Contents

Acknowledgments	iv
List of Abbreviations & Acronyms	v
Executive Summary	vi
Audience	1
Feedback	1
Introduction	1
Application	2
Developing the Sample Procurement Language	3
Understanding the Sample Cybersecurity Procurement Language	4
Sample Cybersecurity Clauses for EVCI Procurements	5
CP: Cybersecurity Program	5
ICAM: Identity, Credential, and Access Management.....	8
CVUM: Configuration, Vulnerability, and Update Management	9
SP: Secure Payment.....	10
SC: Secure Communications	11
PS: Physical Security	12
Managing Cybersecurity Contract Language	13
Terminology	14
Resources.....	15
References.....	16
Appendix A – Webinar Poll Results	18
Appendix B – Sample Cybersecurity Program Deliverables	21

Audience

This resource is intended to guide state departments of transportation (DOTs) (the grantors), electric vehicle service providers (EVSPs) (the grantees), stakeholders, as well as other entities in the contracting of the acquisition, installation, and maintenance and operation of publicly accessible National Electric Vehicle Infrastructure (NEVI) Formula Program-funded electric vehicle (EV) charging infrastructure (EVCI) (https://www.fhwa.dot.gov/bipartisan-infrastructure-law/nevi_formula_program.cfm). The focus is cybersecurity and how to utilize procurement specifications to integrate and improve the cybersecurity of the equipment and services as they are acquired and deployed.

Feedback

On April 18, 2023, the Joint Office of Energy and Transportation hosted the webinar *Sample Cybersecurity Procurement Clauses for Electric Vehicle Charging Infrastructure*, where the sample clauses and justifications were presented to the public. More than 120 individuals attended the webinar. The audience was asked a set of poll questions designed to ascertain the audience members' affiliations and roles; gauge their interest and comfort level in cybersecurity, EV charging, and procurements; critique specific elements of the template language; and identify weaknesses that must be addressed. The poll questions and response summaries are recorded in Appendix A. A recording of the webinar can be found at <https://www.youtube.com/watch?v=ttckJ7EbYkU>. Additional information can be requested or feedback can be submitted at <https://driveelectric.gov/contact/>.

Introduction

EV charging is power transfer supplemented with digital communication, coordination, and decision-making among vehicles, infrastructure, and services. EV charging can be viewed as operating at the confluence of power, networking, computing, and data, as shown in Figure 1. Cybersecurity risks generated from these relationships have the potential to expand as the ecosystem grows to meet EV adoption. EVCI

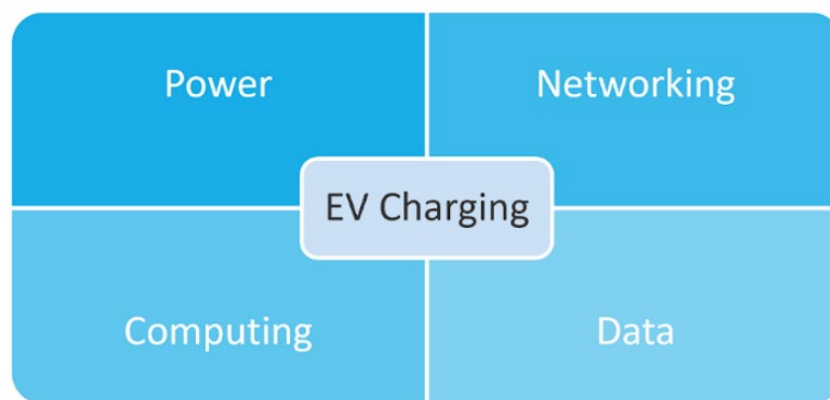
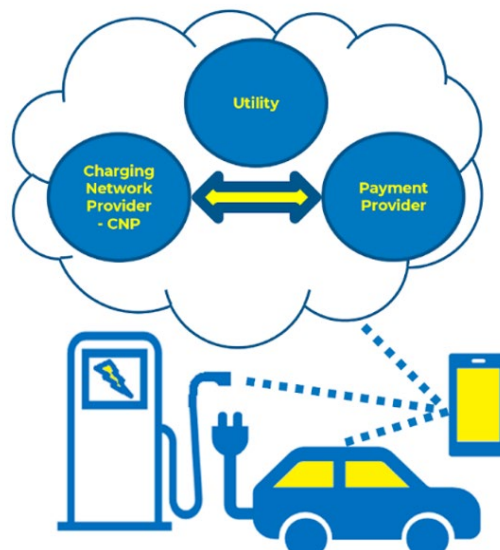


Figure 1 – EV Charging Interconnectedness

interconnectedness with cloud services, shown in Figure 2, demonstrates that EV charging operates at the confluence of power, networking, computing, and data.

The cybersecurity risk to EV charging will increase as the supporting ecosystem grows to meet EV adoption. Potential consequences of these risks include:

- disruption of the power grids, transportation networks, freight conveyance, and logistics networks
- disruption of the charging network (for example, via denial-of-service attack or ransomware) for repurposing for malicious intents (such as BotNets or cryptocurrency mining)
- potential disruption and damage to chargers and vehicles, including theft of customers' personal data, theft of power, or fraudulent payments.



Managing cybersecurity risks is necessary to assure EVCI safety and reliability. Presently, there is a patchwork of existing information technology (IT) and operational technology (OT) guidance—and interpretation of that guidance—to address EVCI. Efforts are underway by governance and standard bodies to tailor cybersecurity and cyber physical guidelines for EVCI; unfortunately, at the time of writing, these efforts are incomplete and unready to be interpreted by the public. However, EVCI grantors are making decisions now and need immediate guidance. To meet this need, this work provides sample cybersecurity procurement language. The sample language is intended to be tailored and incorporated in procurement specifications for EVCI equipment and services. Sample cybersecurity procurement language and sample language are employed synonymously throughout this document.

Application

The purpose of the sample cybersecurity procurement language is to aid state DOTs in managing a coherent and comprehensive life cycle contract process for securing EVCI. This is accomplished by providing a set of foundational cybersecurity clauses that specify what an EVSP must achieve in terms of cybersecurity without specifying how. Importantly, cybersecurity is considered throughout the contract lifetime, from pre-award to post-execution. Widespread use of the sample language creates understanding between the NEVI state plan formula grantors, EVSPs, stakeholders, and the state DOTs, which provides clarity and efficiency when communicating expectations and requirements during the contract life cycle.

The sample clauses are intended to provide a starting point for the procurement process. It is anticipated states will select clauses relevant to their EVCI and service acquisitions. The sample clauses are not intended to be incorporated verbatim into a

contract, replace standards, nor establish cybersecurity standards. Instead, they are meant to be adopted and tailored, with a focus on “what to do” rather than “how to do it.” NEVI state plan formula grantors and the states’ DOTs may go below or beyond the baseline procurement language listed in this document when preparing a request for proposal or request for information early in the EVCI system life cycle.

Developing the Sample Procurement Language

The sample cybersecurity procurement language presented in this document derives from several government and industry cybersecurity good practices, requirements, and procurement language resources. Government reports and guidance, along with existing procurement languages, were essential to the development of the cybersecurity clauses for EVCI. The notice of proposed rulemaking (NPRM) in volume 87 *Federal Register* (FR) 37262, National Electric Vehicle Infrastructure Program, and the final rule, 88 FR 12727, National Vehicle Infrastructure Standards and Requirements (referred to in this document as the NEVI Final Rule) provided the foundational cybersecurity pillars for identifying cybersecurity categories, and cybersecurity-related clauses, along with the following sources:

- American Gas Association (AGA): *Cybersecurity Procurement Language Tool*
- Department of Energy (DOE): *Cybersecurity Procurement Language for Energy Delivery Systems* (2014)
- U.S. DOT Volpe Report: *Government Fleet and Public Sector Electric Vehicle Supply Equipment (EVSE) Cybersecurity Best Practices and Procurement Language Report*
- European Network for Cybersecurity (ENCS): EV-301-2019, Version 2.0, *Security Requirements for Procuring EV Charging Stations*
- National Institute of Standards & Technology (NIST) 800-53, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

A complete list of these resources is available in the References section.

A risk-based approach was used to develop the overarching cybersecurity program (CP) supported by five cybersecurity pillars, as shown in Figure 3. This representation was developed to organize a hierarchy of concepts, understand relationships, and connect the high-level cybersecurity pillars from the NEVI Final Rule into actionable clauses. The five cybersecurity pillars are: Identity, Credential, and Access Management (ICAM); Configuration, Vulnerability, and Update Management (CVUM); Secure Payment (SP); Secure Communications (SC); and Physical Security (PS).

Each cybersecurity pillar leverages NEVI Final Rule categories and a set of ancillary sources to distill pages of cybersecurity controls down to a few fundamental clauses. The five cybersecurity pillars are denoted by a cybersecurity identifier (ID) and are

represented by sample language meant to provide state DOTs with procurement guidance for EVSPs. Each clause is intended to be a starting point to assist state DOTs with a mechanism to drive a robust and resilient EVCI through an EVSP’s cybersecurity program and plan.

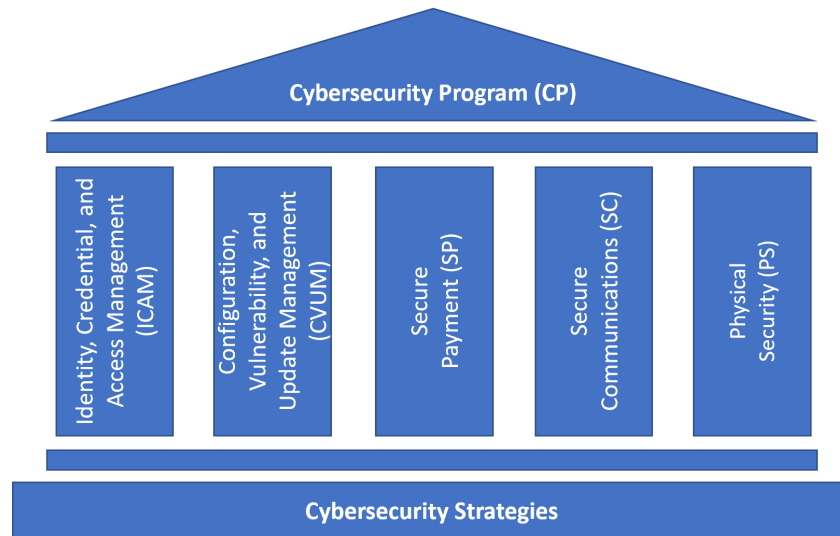


Figure 3 – Visual representation of the sample cybersecurity procurement language

Understanding the Sample Cybersecurity Procurement Language

A consistent format has been developed for each cybersecurity strategy or pillar, shown in the example below.

NEVI Final Rule Categories: Identifies sections of the NEVI Final Rule from which the clauses are drawn.

Sources: Identifies standards and related documents leveraged. These can be found in the References section of this document and shortened names are denoted in brackets [].

ID: Unique clause identifier Clause: Sample clause text	
Related Controls: Inputs beyond the NEVI Final Rule used in developing the clause are listed by their shortened title. Where applicable, specific sections of documents will be identified, such as: NIST 800-53 Rev5: AU-6, CA-2, CA-7. Full titles and sources can be found in the References section of this document.	Justification: Supporting information related to the clause’s intent and purpose.

Sample Cybersecurity Clauses for EVCI Procurements

CP: Cybersecurity Program

A robust and holistic cybersecurity program implements a risk-based cybersecurity strategy to protect the charging infrastructure. A comprehensive program manages cyber risks and effective responses to cyber threats and attacks. The overarching EVSP cybersecurity program is the structure and processes of cybersecurity operations and the reaction to evolving cybersecurity risk. The program scope is broader than the organization's business protections; it must also address EVCI cybersecurity risks. The EVSP must have a cybersecurity plan comprising the organization's security policies, procedures, and remediation plan. The cybersecurity plan should describe what the EVSP will do to meet the cybersecurity program requirements. The cybersecurity plan should address the unique EVCI challenges and consider the interconnectedness of these systems and their dependence on power, networking, and communications. The plan should include at a minimum user data privacy and protection, secure data transfer and protection at rest, secure communications protocols, payment systems, cloud protections, a way to ensure those that are entitled to access have it and those that do not are restricted, employee cyber training with respect to these protections, patching and updates, incident response reporting and recovery with a communications plan, audits and assessments, continuity of operations, risk acceptance and mitigation, disaster recovery, etc.



The cybersecurity procurement clauses build on a strong cyber program and governance strategy as a basis for their success. For example, the cybersecurity plan will identify incident detection, response, and recovery for the entire EVCI, which subsequent cybersecurity pillars' clauses will inherit and build upon. Without a strong risk-based cybersecurity program and plan as a foundation, cybersecurity clauses will not be able to protect the infrastructure needed.

NEVI Final Rule Categories: Audits and Assessments, Continuity of Operations, Incident Prevention and Handling, Robust Cybersecurity Program, Subcontractor Protections, Risk Acceptance and Mitigation, Life Cycle Cybersecurity.

Sources: [AGA], [DOE], [DOE EDS], [DOT], [ENCS], [NIST 800-53], [NIST 800-18], [FIPS 200]

ID: CP1 Clause: The EVSP Cybersecurity Program MUST address EVCI security and MUST document potential risks and protections throughout the lifetime.	
Related Controls: NIST 800-53 Rev5: PL-2, PL-7, PL-8, PM-7, PM-8, PM-9, PM-11, PM-17, PM-18, RA-1, RA-2	Justification: This Clause emphasizes the need for EVSPs to maintain a proactive risk-based approach to manage the Cybersecurity Program throughout the life cycle of the EVCI. It is important for EVSPs to implement risk management activities that focus on vulnerabilities and impact for each stage of the engineering, development, and system operations life cycle from design to disposal. EVSPs should have established evaluation criteria to assess the risks and impact when determining procurement or operations decisions involving EVCI hardware, software, data, personnel, subcontractors, and vendors.
ID: CP2 Clause: The EVSP MUST provide an annual self-assessment and/or third-party assessment to the State DOT that includes evidence of updates and adherence to the Cybersecurity Plan within [an acceptable time period e.g., 30 days] of annual assessment.	
Related Controls: NIST 800-53 Rev5: AU-6, CA-2, CA-7, PL-2, PM-18, RA-3, SA-11	Justification: This Clause emphasizes the need for the EVSP to maintain and update the Cybersecurity Program, and the current version of the Cybersecurity Plan shall be provided to the State DOT on an annual basis. The Cybersecurity Plan shall detail all of the items stipulated in the Cybersecurity Program Requirements and shall provide a mechanism for implementing the Cybersecurity Program either directly within the Cybersecurity Plan or by referencing additional, appropriate policy and procedure documents.
ID: CP3 Clause: The EVSP MUST revise the Cybersecurity Plan annually to accommodate new risks, requirements, and standards and provide an updated copy to the State DOT within [an acceptable time period e.g., 30 days] of annual update.	
Related Controls: NIST 800-53 Rev5: PM-1, PM-9, PM-28	Justification: This Clause emphasizes the need for the EVSP to evaluate and document any potential new cybersecurity risks or impacts from the proposed modification and implement appropriate security controls to mitigate negative impacts. Examples of changes include modifications to hardware or software, changes in system configurations or communications pathways, changes in security controls, and changes in physical or personnel security programs. On an annual basis, if the EVSP revises or makes updates to the Cybersecurity Plan, an updated copy MUST be provided to the State DOT for review and approval within [negotiated period – 30 days].

ID: CP4 Clause: Security incidents MUST be reported to [the designated security liaison] within [an acceptable time period e.g., 48 hours] of discovery.	
Related Controls: NIST 800-53 Rev5: AC-16, CA-7, IR-4 (8) (10), IR-5, IR-6 (2), IR-8 (1), RA-5 (11), RA-7, SI-5, SR-5, SR-6	Justification: This Clause emphasizes the need for the EVSP to rapidly respond (e.g., in a timely manner) to and report any identified cybersecurity incident (e.g., unintended data or privacy leaks, etc.) that delays, disrupts, or harms the EVCI or has the potential to impact EV charger networks. It is important that EVSPs immediately report available information of any incident that has severely impacted the EVCI and provide updates as more information becomes available. The Designated Security Liaison role is based on the NIST concept of cybersecurity point of contact. This entity will receive security incident reports.
ID: CP5 Clause: EVSP subcontractors MUST adhere to the same cybersecurity protections, as established for the EVSP.	
Related Controls: NIST 800-53 Rev5: SR-2, SR-3, SR-5	Justification: This Clause emphasizes the need for EVSP subcontractors to be held to the same rigor of cybersecurity. Therefore, it is the responsibility of the EVSP to ensure that the subcontractors' training and awareness of all cybersecurity policies, procedures, protections, cybersecurity roles and responsibilities, including how accountability will be established and maintained, are documented.
ID: CP6 Clause: The EVSP MUST indemnify, defend, and hold harmless, without limitations, the State, its departments, divisions, agencies, offices, commissions, officers, employees, and affiliates from all claims relating to cybersecurity breaches to the contracted EVCI.	
Related Controls: NIST 800-53 Rev5: SR-1	Justification: This clause emphasizes that the EVSP is responsible to protect the State and all listed parties from any liabilities relating to cybersecurity breaches to the contracted EVCI. The EVSP is obligated to act and defend the State and listed parties against any claim and proceeding of cybersecurity breaches to the contracted EVCI brought to them and is responsible for payments of any losses incurred by the State and all the listed parties relating to any claim suit or proceeding.

ICAM: Identity, Credential, and Access Management



ICAM is a key component to ensuring that access control to all systems is secure. The goal of this cybersecurity pillar is to provide the right person with the right privileges to access the right information at the right time to complete necessary tasks. Privileges should be restricted whenever possible, and individuals without proper access will not be permitted to perform privileged activities.

NEVI Final Rule Categories: User or System Identification, Authorization and Authentication [23 CFR § 680.106 (h) (2)] [23 CFR § 680.114 (a) (2)], Access Control and Management [23 CFR § 680.106 (h) (2)]

Sources: [NIST 800-53], [ENCS], [NIST 800-40]

ID: IC1 Clause: The EVSP MUST have centralized capabilities that authenticate, authorize, log, and monitor access.	
Related Controls: NIST 800-53 Rev5: AC-2; AU-6; IA-2, IA-3	Justification: Centralized capabilities provide a single point of control and management, making it possible to enforce consistent security policies and compliance across an organization's systems and applications. Centralized authentication and authorization help prevent and detect unauthorized access and maintain data confidentiality. Lastly, centralized logging and monitoring enable effective incident detection, response, and mitigation procedures.
ID: IC2 Clause: The EVSP MUST configure accounts to limit user permissions to the minimum level necessary to perform authorized tasks (e.g., EVSP, EV driver, charging station management system, and EV).	
Related Controls: NIST 800-53 Rev5: AC-2	Justification: Access control, which involves restricting access to systems, information, functions, tools, locations, components, or resources, plays a crucial role in limiting individual users and processes through the principle of least privilege. Insufficient access control methods can lead to unauthorized or unnoticed system breaches by adversaries. This principle limits access of each process, program, or user exclusively to authorized and necessary information and resources, effectively reducing potential attack entry points.
ID: IC3 Clause: The EVSP MUST employ multi-factor authentication.	
Related Controls: NIST 800-53 Rev5: IA-2, IA-5	Justification: This clause focuses on adding an extra layer of security beyond just a single password. Aligning with the requirement for multiple methods to authenticate (e.g., something you have, something you know, something you are, or somewhere you are), this clause affirms that EVSPs are required to enforce multiple factors of

	authentication, such as passwords, tokens, or a one-time access code.
--	---

CVUM: Configuration, Vulnerability, and Update Management

Systems are interconnected with various other systems and undergo changes or updates when necessary. However, changes and updates create opportunities for malicious devices or malware to connect to the network or leave security gaps in devices that can be exploited. Having knowledge of when a change was made to a device, software installation, or when a new system is connected to the network can help reduce security risks and achieve confidentiality, integrity, and authenticity. Understandably, no system is ever completely secure, and monitoring for vulnerabilities allows for best cybersecurity practices to be applied. Having a clear and concise vulnerability management plan equips organizations with the ability to identify and respond to threats in a timely manner.



NEVI Final Rule Categories: Vulnerability Management (Logging for intrusion prevention, detection, and response) [23 CFR § 680.106 (h) (2)], Secure Remote Updates [23 CFR § 680.114 (a) (2)], Remote Monitoring and Diagnostics [23 CFR § 680.114 (a) (3)]

Sources: [NIST 800-53], [NIST 800-40]

ID: CM1 Clause: The organization MUST ensure the authenticity and integrity of applied updates, report any violations, and MUST have a formal patch management plan that includes procedures for identifying, testing, approving, and deploying patches and updates in a timely manner.	
Related Controls: NIST 800-53 Rev5: SA-22; NIST 800-40v2	Justification: Emphasis on the criticality of ensuring the authenticity and integrity of updates helps protect against security breaches or threats. Establishing requirements to report violations highlights the significance of accountability and proactive response in maintaining a secure system. The EVSP should recognize that a formal patch management plan emphasizes the importance of structured procedures for handling timely updates, reducing risks, and ensuring a strong cybersecurity stance.
ID: CM2 Clause: The update management process must be automated for timely and consistent deployment of security patches across all systems.	
Related Controls: NIST 800-53 Rev5: SI-7	Justification: Regularly installing updates, patches, service packages, or other fixes to systems is essential for remedying discovered weaknesses and vulnerabilities, as the process of discovering these flaws is continuous. Such updates must be tested and validated before implementation, including for

	hardware, software, and firmware pertaining to all applicable products of the EVCI.
--	---

SP: Secure Payment



The intent of this cybersecurity pillar is to protect cardholder data and secure the integrity of credit card transactions. These complementary standards impose requirements and controls with which payment systems will need to comply. Elements for consideration include how to handle and not exclude future payment types that do not currently exist and what happens to payments in the event of a network outage.

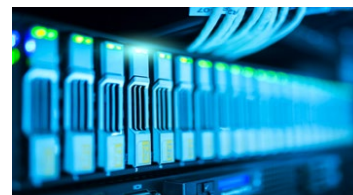
NEVI Final Rule Categories: Payment Card Processing [23 CFR § 680.106 (f) (1)] [23 CFR § 680.106 (l)]

Sources: [PCI DSS], [EMVCo]

ID: SP1 Clause: Payment systems MUST comply with current payment card industry security standards.	
Related Controls: PCI DSS v4.0	Justification: Demonstrating compliance with existing payment card industry standards reinforces the integrity of data security during payment transactions. These standards provide a baseline of requirements for payment protection.
ID: SP2 Clause: Payment terminals MUST be EMVCo L1 Certified.	
Related Controls: EMVCo	Justification: EMV specifications for all payment terminals is essential for payment protection to secure and protect physical, electrical and transport level interfaces enabling the communication of data between the payment device and the acceptance device.

SC: Secure Communications

SCs are a necessary element for protecting data confidentiality, authentication, and content integrity both in transit and at rest. SCs allow charging stations to digitally encrypt and authenticate (e.g., using public key infrastructure, the identification of users, devices, and services). Employing cryptographic-agile protocols allows charging stations to update encryption without having to redesign hardware or systems.

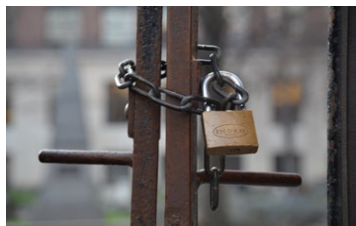


NEVI Final Rule Categories: Secure Charging Communications [23 CFR § 680.114 (a) (b) (c) (d)], Data Privacy [23 CFR § 680.106 (l)], Cloud, Cryptographic Agility, and Public Key Infrastructure [23 CFR § 680.106 (h) (2)] [23 CFR § 680.114 (a) (2)]

Sources: [NIST 800-53], [CSA], [FedRAMP]

ID: SC1 Clause: EVSP MUST employ standardized secure protocols utilizing modern encryption and design for cryptographic agility.	
Related Controls: NIST 800-53 Rev5: SC-8, SC-13, SC-28, SI-7 (6)	Justification: EV charging infrastructure relies on secure point-to-point communications. Secure protocols using modern encryption protect data in transit. As computers become more advanced, protocols and encryption methods are also improving. Cryptographic agility will provide the EVSP with the ability to update the systems more effectively providing the consumer with added security.
ID: SC2 Clause: EVSP MUST limit personal data collection to strictly necessary for purposes of EV charging and protect it throughout its life cycle.	
Related Controls: NIST 800-53 Rev5: AC-16	Justification: Information that is not collected cannot be leaked and information that is collected needs to be protected from the time of inception until destruction from both internal and external threats.
ID: SC3 Clause: All data MUST reside in the United States throughout its life cycle and is administered by those who have undergone background screening.	
Related Controls: CSA; FedRAMP; NIST 800-53 Rev5: PS-3, SA-9 (4), SA-9 (5)	Justification: While no standards or generally accepted guidance require this, we felt strongly enough to propose that cloud protection data live in the U.S. and those with access to it have a level of credibility validated via a background check.

PS: Physical Security



PS mechanisms protect software, hardware, networks, and data from physical actions and events that damage or disrupt functions or security objectives. PS fortifies the system by only allowing authorized personnel to physically access all systems and devices. It also protects against environmental threats, such as natural and man-made disasters, electrical interference, and electromagnetic radiation. Physical attacks

may change the operation of a device, and they may be in the form of illegal surveillance of payment devices, etc.

NEVI Final Rule Categories: Tamper Prevention, Detection, and Response [23 CFR § 680.106 (h) (1)], Secure Operation during Communication Outages [23 CFR § 680.106 (h) (2)]

Sources: [NISTIR], [NIST SP 800-53], [DOE]

ID: PS1 Clause: EVSP MUST utilize anti-tamper techniques to prevent, deter, and detect unauthorized physical access.	
Related Controls: NIST 800-53 Rev 5: AT-3 (2), PE-3, PE-5, CM-7 (8)	Justification: This clause addresses the physical security of EVCI. There are many ways for an organization to implement physical access control, using both devices and procedures. It is inspired from the principle of least functionality, in which systems are configured for security using appropriate access controls.
ID: PS2 Clause: Unexpected or unauthorized accesses MUST be immediately communicated.	
Related Controls: NIST 800-53 Rev5: AC-3 (12), AU-9, AU-13, IR-8, PS-7, SI-7	Justification: This clause is intended to address the enforcement of physical security and access control. Security is strengthened through monitoring and notifying the appropriate stakeholders in the event of unauthorized access.

Managing Cybersecurity Contract Language

Preparing for the Contract

The following are several important considerations for your organization as it prepares its EVCI cybersecurity contract language:

- Include cybersecurity experts in designing the language for the request for bids. In other words, bake cybersecurity in, do not snap it on later.
- Establish and adhere to cybersecurity evaluation criteria (rubric) for all bids. Doing so will ensure all EVSP bids are assessed equally.
- Include a cybersecurity expert in the EVSP review and selection process. The expert's role is to ensure that your organization's interests are protected to the best of the selected EVSP ability.
- Include cybersecurity requirements in all contracts and agreements to protect your organization from cybersecurity risk from third parties of the system installed. This step will not just protect your organization from the main EVSP but also from its partners as well. For example, a vendor who installs a solar array at your organization's site may utilize a third-party integrator and cloud provider. As the customer, your organization may not even be aware there are outsourced services. Organizations can manage third-party risks by requiring the EVSP to pass down cybersecurity requirements to subcontractors.

Over the Life of the Contract

- Include the topic of cybersecurity in conversations with EVSPs and stress its importance.
- Review and provide feedback on the EVSP cybersecurity program and plan annually.
- Include cybersecurity experts in the design and installation of the system.

Managing Cyber Risk

The following are several important considerations for managing your organization's cyber risk:

- A 5-year contract requires 5 years of cybersecurity and contract management.
- Require third-party, annual evaluation of the installed system's security.

Cybersecurity needs may evolve over time. Contracts may need to be updated to address new needs or requirements.

- Focus on risk to your organization/site rather than compliance throughout the life of the contract. The goal is to actively manage risk through proactive cybersecurity rather than a "check the box" approach that will be completed and not reviewed regularly.
- Don't let your selected EVSP charge you to have them do the right thing. Cybersecurity is not a luxury!

And finally, ensure all cyber-related reporting is reviewed by your organization's cybersecurity staff, not just contracts staff, to maximize value to the organization.

Terminology

charging station management system (CSMS): A backend system that manages a network of chargers.

charging station: The area in the immediate vicinity of a group of chargers, including the chargers, supporting equipment, parking areas adjacent to the chargers, and lanes for vehicle ingress and egress.

cybersecurity categories: The proposed cybersecurity categories were primarily identified from NEVI Final Rule §680.106 (f) (h), (L), 680.114 (a) (b) (c), and best practices were derived from industry publications, research, and interviews with the U.S. Department of Transportation (DOT).

cybersecurity strategies: The cybersecurity strategies are based on the NEVI Final Rule: 23 CFR Part §680 Federal Register / Vol. 88, No. 39 / Tuesday, February 28, 2023 / Rules and Regulations, existing cybersecurity guidelines, related publications, research, and interviews with state DOTs.

electric vehicle supply equipment (EVSE): The independently operated component that is responsible for delivering power to an EV.

electric vehicle charging infrastructure (EVCI)/charging network: A collection of chargers located on one or more property(ies) that are connected via digital communications to manage the facilitation of payment or electrical charging or any related data requests.

electric vehicle service provider (EVSP): Supplier/contractor/EVSP/grantee organization that enters into an agreement to supply the EV charging infrastructure.

public key infrastructure (PKI): A framework consisting of standards and services to enable secure, encrypted communication and authentication over potentially insecure networks, such as the Internet.

security event: Any observable occurrence in a network or system.

security incident: An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

smart charging: Energy management where power transfers are managed with respect to electric supply capacities.

software: For the purposes of this paper, this includes firmware, operating systems, applications, and application services (e.g., cloud-based software), as well as products containing software.

Resources

These resources were indirectly used to develop the sample cybersecurity clauses.

Cichonski, P., T. Millar, T. Grance, and K. Scarfone. 2012. *Computer Security Incident Handling Guide*. National Institute of Standards and Technology SP 800-61, Rev. 2. <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>.

CISA. n.d. “Cross-Sector Cybersecurity Performance Goals.” Cybersecurity & Infrastructure Security Agency. Accessed May 17, 2023, at <https://www.cisa.gov/cpg>.

DOT. 2023 “Architecture Reference for Cooperative and Intelligent Transportation.” United States Department of Transportation. Accessed May 17, 2023, at <https://www.arc-it.net/>.

Grassi, P. A., M. E. Garcia, J. L. Fenton. 2017. *Digital Identity Guidelines*. National Institute of Standards and Technology 800-63-3. <https://doi.org/10.6028/NIST.SP.800-63-3>.

Harnett, K., G. Watson, and G. Brown. 2019. *EVSE Cybersecurity*. U.S. Department of Transportation DOT-VNTSC-NAVY-20-01. <https://rosap.ntl.bts.gov/view/dot/43606>.

Joint Office of Energy and Transportation. n.d. “State Plans for Electric Vehicle Charging.” Accessed May 17, 2023, at <https://driveelectric.gov/state-plans/>.

Joint Task Force Transformation Initiative. 2011. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST SP 800-39. <https://csrc.nist.gov/publications/detail/sp/800-39/final>.

Joint Task Force. 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. National Institute of Standards and Technology SP 800-37, Rev. 2. <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>.

Kent, K. and M. Souppaya. 2006. *Guide to Computer Security Log Management*. National Institute of Standards and Technology SP 800-92. <https://csrc.nist.gov/publications/detail/sp/800-92/final>.

NIST. n.d. “NIST Technical Series Publication List: SP 1800.” National Institute of Standards and Technology. Accessed May 17, 2023, at <https://pages.nist.gov/NIST-Tech-Pubs/SP1800.html>.

Stouffer, K., M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, and S. Lightman. 2022. *Guide to Operational Technology (OT) Security*. National Institute of Standards and Technology SP 800-82. <https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft>.

References

These references were directly used to develop the sample cybersecurity clauses and are identified in the Sources section of each clause using square brackets [].

[AGA] Cybersecurity Strategy Task Force. n.d. AGA Cybersecurity Procurement Language Tool. American Gas Association. https://www.aga.org/wp-content/uploads/2022/11/aga_ot_procurement_language_calibration_tool_v1.5_april_2017.xlsx.

[CSA] CSA. n.d. “Welcome to the Cloud Security Alliance.” Accessed May 17, 2023, at <https://cloudsecurityalliance.org/>.

[DOE] Johnson, J., B. Anderson, B. Wright, J. Quiroz, T. Berg, R. Graves, J. Daley, K. Phan, M. Kunz, R. Pratt, T. Carroll, L. R. O’Neil, B. Dindlebeck, P. Maloney, J. O’Brien, D. Gotthold, R. Varriale, T. Bohn, and K. Hardy. 2022. Cybersecurity for Electric Vehicle Charging. Sandia National Labs SAND2022-9315. <https://www.osti.gov/servlets/purl/1877784>.

[DOE EDS] ECSWG. 2014. *Cybersecurity Procurement Language for Energy Delivery Systems*. Energy Sector Control Systems Working Group. <https://www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april-2014>.

[DOT] Harnett, K., G. Watson, and G. Brown. 2019. *Government Fleet and Public Sector Electric Vehicle Supply Equipment (EVSE) Cybersecurity Best Practices and Procurement Language Report*. U.S. Department of Transportation Volpe Center. <https://rosap.ntl.bts.gov/view/dot/43606>.

[EMVCo] EMVCo. n.d. “Enabling Seamless and Secure Payments Worldwide.” Europay, MasterCard, and Visa (EMVCo). Accessed May 17, 2023, at <https://www.emvco.com>.

[ENCS] ENCS. n.d. “Security requirements for procuring EV charging stations.” European Network for Cybersecurity EV-301-2019 Version 2.0. Accessed May 17, 2023, at <https://encs.eu/resource/ev-301-2019-security-requirements-for-procuring-ev-charging-stations/>.

[FedRAMP] FedRAMP. 2023. “Securing Cloud Services for the Federal Government.” Federal Risk and Authorization Management Program. Accessed May 17, 2023, at <https://www.fedramp.gov/>.

[FIPS 200] FIPS. 2006. *Minimum Security Requirements for Federal Information and Information Systems*. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>.

[NEVI Final Rule] 88 FR 12727. 2023. National Electric Vehicle Infrastructure Standards and Requirements. *Federal Register*.
<https://www.federalregister.gov/documents/2023/02/28/2023-03500/national-electric-vehicle-infrastructure-standards-and-requirements>.

[NISTIR] The Smart Grid Interoperability Panel-Smart Grid Cybersecurity Committee. 2014. *Guidelines for Smart Grid Cybersecurity*. National Institute of Standards and Technology NISTIR 7628 Rev. 1. <https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final>.

[NIST CSF] NIST. n.d. “Cybersecurity Framework.” National Institute of Standards and Technology. Accessed May 17, 2023, at <https://www.nist.gov/cyberframework>.

[NIST FIPS 140] NIST. 2019. *Security Requirements for Cryptographic Modules*. National Institute of Standards and Technology FIPS 140-3. Accessed May 17, 2023, at <https://csrc.nist.gov/publications/detail/fips/140/3/final>.

[NIST 800-18] Swanson, M., J. Hash, P. Bowen. 2006. *Guide for Developing Security Plans for Federal Information Systems*. National Institute of Standards and Technology SP 800-18, Rev. 1. <https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final>.

[NIST 800-40] Souppaya, M. and K. Scarfone. 2022. *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*. National Institute of Standards and Technology SP 800-40, Rev. 4.
<https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final>.

[NIST 800-53] Joint Task Force. 2020. *Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology SP 800-53, Rev. 5. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>.

[NIST 800-57] Barker, E., 2020. *Recommendation for Key Management: Part 1 – General*. National Institute of Standards and Technology SP 800-57 Part 1, Rev. 5.
<https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final>.

[NIST NCCOE] NIST NCOE. n.d. “Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure.” National Institute of Standards and Technology, National Cybersecurity Center of Excellence. Accessed May 17, 2023, at <https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-electric-vehicle-extreme-fast-charging-infrastructure>.

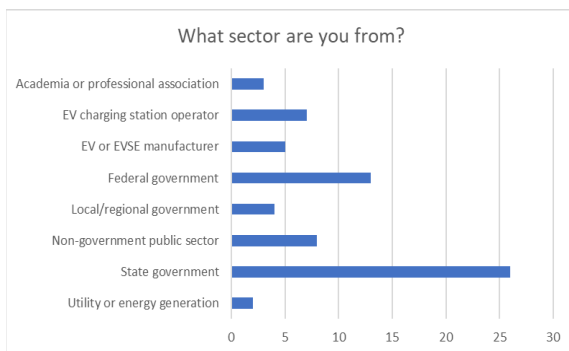
[NPRM] 87 FR 37262. 2022. National Electric Vehicle Infrastructure Formula Program. Notice of Proposed Rulemaking: 23 CFR Part 680. Federal Highway Administration, U.S. Department of Transportation. *Federal Register*.
<https://www.govinfo.gov/content/pkg/FR-2022-06-22/pdf/2022-12704.pdf>.

[PCI DSS] Goodspeed, L. 2022. “PCI DSS v4.0 Resource Hub.” Payment Card Industry Security Standards Council. Accessed May 17, 2023, at <https://www.pcisecuritystandards.org/>.

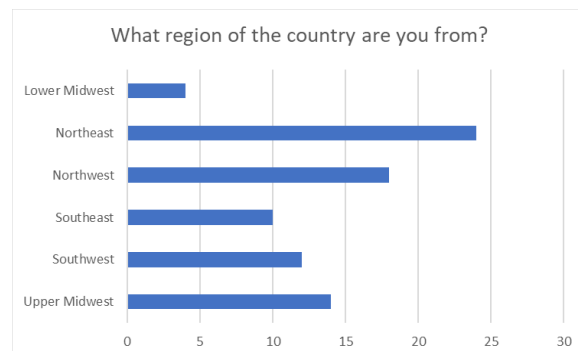
Appendix A – Webinar Poll Results

The following poll questions and feedback results were captured from the Sample Cybersecurity Procurement Clauses for Electric Vehicle Charging Infrastructure (EVCI) webinar hosted by the Joint Office of Energy and Transportation (Joint Office) on April 18, 2023.

What sector are you from?



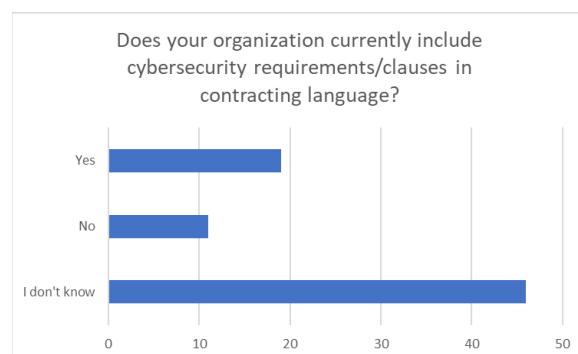
What region of the country are you from?



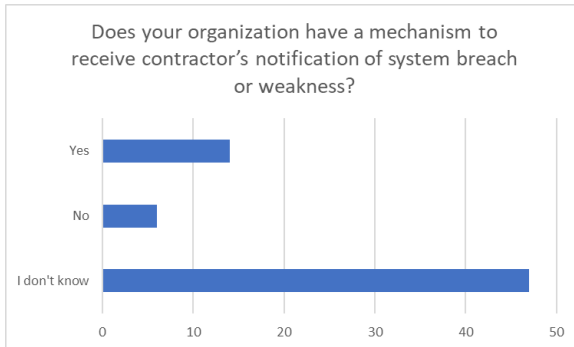
What is your role within your organization?



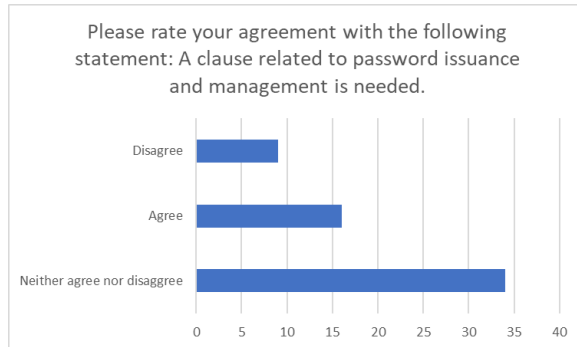
Does your organization currently include cybersecurity requirements/clauses in contracting language?



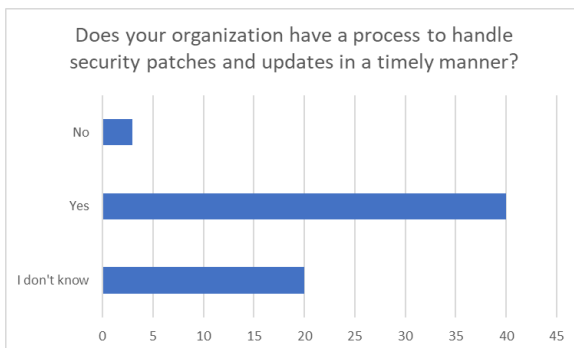
Does your organization have a mechanism to receive contractor's notification of system breach or weakness?



Please rate your agreement with the following statement: A clause related to password issuance and management is needed.

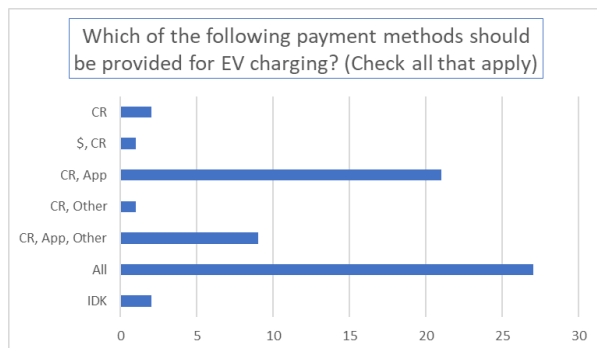


Does your organization have a process to handle security patches and updates in a timely manner?

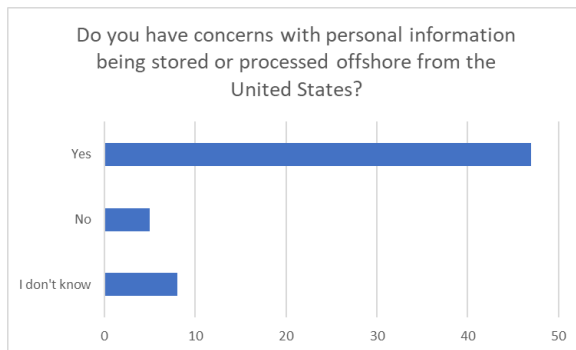


Which of the following payment methods should be provided for EV charging? (Check all that apply)

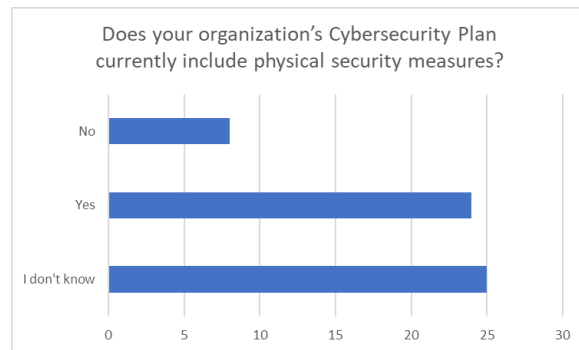
CR = Credit/debit cards App = App/subscription All = All of the above
\$ = Cash Other = Other IDK = I don't know



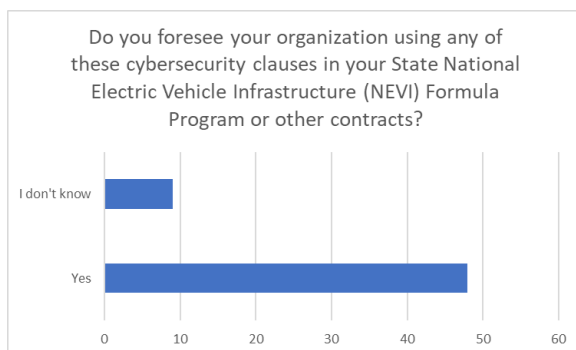
Do you have concerns with personal information being stored or processed offshore from the United States?



Does your organization's Cybersecurity Plan currently include physical security measures?



Do you foresee your organization using any of these cybersecurity clauses in your State National Electric Vehicle Infrastructure (NEVI) Formula Program or other contracts?



Appendix B – Sample Cybersecurity Program Deliverables

Table 1. Cybersecurity Deliverables

Clause	Description	Submittal Schedule	Recipient	Format
CP1	Cybersecurity Plan and Supporting Policy and Procedure Documents	After the contract is awarded and reviewed, the EVSP cybersecurity program MUST address EVCI security and MUST document potential risks and protections within <i>[negotiated period – 90 days]</i> and <u>annually</u> throughout contract lifetime.	State DOT	Electronic
CP2	Self/Third-Party Cybersecurity Assessment Reports	The EVSP MUST provide an <u>annual</u> self-assessment and/or third-party assessment that includes evidence of updates and adherence to the cybersecurity plan and provide a copy to the state DOT within <i>[e.g., 30 days]</i> of annual assessment.	State DOT	Electronic
CP3	Cybersecurity Plan Updates	Revise the cybersecurity plan <u>annually</u> to accommodate new risks, requirements, and standards and provide an updated copy to the state DOT within <i>[e.g., 30 days of]</i> annual update.	State DOT	Electronic
CP4	Cyber Incident Reporting	Security incidents MUST be reported to <i>[the designated security liaison]</i> within <i>[e.g., 48 hours]</i> of discovery.	State DOT <i>[designated security liaison]</i>	Electronic