NEVI PROJECT CYBERSECURITY PLAN TEMPLATE

The Arkansas Department of Transportation (hereinafter referred to as ARDOT) requires all Sponsors under the Arkansas National Electric Vehicle Infrastructure (NEVI) Program to complete, and submit to ARDOT, an annual cybersecurity plan for electric vehicle (EV) charging infrastructure sites in Arkansas.

ARDOT prioritizes and understands the importance of cybersecurity for all NEVI projects funded under the Federal NEVI Program (23 CFR 680). In the event a Sponsor or project site does not currently comply with the cybersecurity provisions outlined in the plan below, Sponsors must present a remediation plan to achieve compliance and demonstrate progress towards achieving compliance. This plan must be approved by ARDOT.

Please note: All sections of the plan marked with a (*) indicate security requirements that the Sponsor and associated project teaming partners must currently meet in order to achieve compliance and receive approval for the submitted plan.

Sponsors must use this template provided by ARDOT to complete the annual cybersecurity plan requirement under the NEVI Program. In the event that the Sponsor is utilizing the same teaming partners at all project sites, a plan is required to be submitted for each project. If the Sponsor is utilizing unique teaming partners, across multiple sites, each project site must submit a site-specific plan.

Submission: Upon submitting the NEVI Project Notice of Acceptance Request (Form LPA-039), Sponsors must attach a cybersecurity plan prior to the Operation and Maintenance Phase and no later than January 1, annually, during the Agreement Term. Completed plans must be submitted to LPA@ardot.gov.

Sponsor and Project Information *(required)*	
Sponsor Name:	
Job # - Job Name:	
Plan Coverage Period (*period may not exceed 12 mos.*)	__ / __ / ____ through __ / __ / ____
Sponsor Site Location:	
Contact Name:	
Phone Number:	
Email Address:	
Mailing Address:	
Additional Project Team Members:	
EVSE Equipment:	
EVSE Network:	
Payment Card Processor:	
Utility:	

Sponsor Certification

This certification must be completed and signed by an authorized representative or agent for the Sponsor who can attest to the annual cybersecurity plan's quality, accuracy, and completeness and verify that the questions have been answered to the best of the Sponsor's knowledge.	
_____ *(signature)*	_____ *(date)*

Cybersecurity Plan Submission Type:	
	First-time submission
	Plan Update / Renewal (Date of Last Plan Submission: __ / __ / ____)

1. Cybersecurity Program Structure

1.1. Please describe the culture of security at your company. Outline any actions taken over the previous year around cybersecurity, and what you plan to accomplish in the next 12 months to improve cybersecurity:

Note: Include background information on overall philosophy, standard framework for security followed (i.e. NIST IR 8743), and guiding principles around cybersecurity at your company.

1.2. Provide electric vehicle supply equipment (EVSE) company security culture information:

Note: Include the name of the EVSE company and information provided from the supplier specific to security culture at the company.

1.3. Provide networking company security culture information:

Note: Include the name of the networking company and information provided from the supplier specific to security culture at the company.

1.4. Provide payment processing company security culture information:

Note: Include the name of the payment processing company and information provided from the supplier specific to security culture at the company.

1.5. Please describe the overall approach and plan for cybersecurity in the project(s). Please include pre-determined proactive safety measures, security titles within the organization, and any pre-defined security strategies:

Note: Include specific safety measures and security controls (i.e. firewalls, antivirus, intrusion detection systems, encryption, monitoring, etc.).

1.6. As the entity responsible for identifying and mitigating risks, define potential EV charging infrastructure security risks and planned protections throughout the lifetime of the NEVI project(s). Provide a mitigation strategy to respond to the risk(s) when determining operations decisions involving EV charging infrastructure hardware, software, data, personnel, subcontractors, and vendors:

Note: Include any 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 (i.e. unauthorized access, data privacy, payment system attacks, network, software and firmware vulnerabilities, inadequate encryption, physical access, uptime, operation through network outage, etc.).

Risk	Responsible Party and Point of Contact (POC)	Mitigation Strategy

Please include additional risks, responsible party and POC, and mitigation strategies as an attachment to this template, as needed.

1.7. Define the process, including notification to ARDOT within 48 hours of detected incident, for incident response (e.g., in a timely manner) and reporting of any identified cybersecurity incident (e.g., unintended data or privacy leak or bad actor security intrusion) that delays, disrupts, or harms the EV charging infrastructure, the public customer of the system, the electric utility connected to the system or has the potential to impact EV charger networks. ARDOT expects notification by both a phone call **and** email to ARDOT's Primary Rapid Response Point of Contact (listed in 1.8) within 48 hours from incident identification:

Note: Include information about initial notification, assessment and triage, activation of response team, analysis and investigation, communication, mitigation strategies, documentation, post incident review, continuous monitoring, and training and awareness.

1.7.1 If no current process for rapid response and reporting exists, please describe a plan, with timing, for developing one within the coming year:

1.8. Primary Rapid Response Point(s) of Contact

SPONSOR	**ARDOT (Department Use Only)**
NAME:	**NAME:**
TITLE:	**TITLE:**
PHONE:	**PHONE:**
EMAIL:	**EMAIL:**

1.9. Describe how any subcontractors or other third parties will adhere to the cybersecurity protections outlined for each project:

Note: Include any training that you have or will provide around cybersecurity policies, procedures, protections, roles, and responsibilities. Include whether this clause is in your contract with subcontractors.

1.9.1. If subcontractors do not currently comply, outline how you will work to support compliance prior to the public opening of the charger:

1.10. Define the process to notify ARDOT of any cybersecurity-related lawsuit or potential legal action associated with the NEVI Program-funded EV charging infrastructure:

Note: Include process and timeline for notifying ARDOT of legal action associated with the charging infrastructure.

1.10.1. If no current approach exists, please describe how you will design an approach to comply:

Define any new risks, requirements, and/or standards for the project(s) since the last update (*if applicable*):

Note: Detail anything new since the submission last year (if applicable).

2. Identity, Credential, and Access Management (ICAM)*

2.1. Describe the structure for centralized capabilities that authenticate, authorize, log, and monitor access*:

Note: Include information about the authentication system (user and device), authorization framework (role-based access control), centralized logging (log collection, formatting, retention), and monitoring access (real-time, anomaly detection, incidence response integration).

2.2. Describe the process for configuring accounts to limit permissions to the minimum level necessary to perform authorized tasks and how it's being implemented*

Note: Include information on role-based access control, user segmentation, regular access reviews, separation of duties, use of groups, privilege escalation controls, auditing and logging, password policies, security trainings, and continuous monitoring).

2.3. Confirm the use of multifactor authentication (MFA)

Multifactor authentication is utilized for all authentication related to:

MFA control(s) used: _____

If MFA is not utilized for authentication related to the project, outline **how** and **when** MFA be adopted and implemented in the coming year:

3. Configuration, Vulnerability, and Update Management (CVUM)

3.1. Describe how the authenticity and integrity of system updates will be facilitated, and how violations will be reported. Outline the formal patch management plan that includes procedures for identifying, testing, approving, and deploying patches and updates in a timely manner:

Note: Include information on who is updating which equipment, and which processes are being used or defined in your plan, i.e. secure update channels, automated update checks, reporting violations, anomaly detection, phased deployment strategy (to minimize disruption), and automated deployment tools. Include information on timely deployment of system updates, minimal impact on end users, continuity of EVSE operation, security of the system, and communication with users.

3.1.1. If no current process for updates exists, outline how a process will be developed and implemented in the coming year:

3.1.2. Describe the automated update management process and how timely and consistent deployment of security patches across all systems will be implemented:

Note: Include information on automated update scanning, vulnerability assessment, testing environments, scheduled deployments, compliance monitoring, reporting dashboards and continuous monitoring.

3.1.3. If there is not an automated update process in-place, describe how a strategy for automated updates will be developed and implemented:

4. Secure Payment (SP)

4.1. Provide information on the project team members / vendors that are responsible for payment card processing:

Note: Include information on data discovery, network segmentation, data encryption, access control measures, vulnerability scanning, penetration testing, regular audits, and compliance reporting. Also include how information and collected and how customer data is protected.

4.2. Confirm the entities that provide payment processing services follow the PCI-DSS and have an Attestation of Compliance*:

☐ **Check here to confirm vendor has a PCI-DSS Attestation of Compliance**

Date of compliance: ___ / ___ / _____ (*updated annually*)

PCI-DSS Version: (*i.e. 3.0*) _____

If multiple Attestations of Compliance are applicable under this project, please include as attachments to this Plan submission.

4.3. Confirm all payment terminals have EMVCo Level 1 certification*:

☐ **Check here to confirm all payment terminals are EMVCo Level 1 certified**

5. Secure Communications (SC)

5.1. Describe employment of standardized secure protocols utilizing modern encryption and design for cryptographic agility for data at arrest and in transit:

Note: Include information on DNS security extensions, OpenID connect, key management best practices, security audits, and penetration testing, etc.

5.1.1. If modern encryption is not currently utilized, outline a process for implementation of modern encryption in the coming year:

5.2. Outline process for limiting personal data collection to data that is strictly necessary for purposes of EV charging and protecting it throughout its life cycle:

Note: Include information on data minimization, anonymization, transparent privacy policies, data security measures, data lifecycle management, data retention period, data audits, user access controls, data transmission, and compliance checks.

5.2.1. If a process to limit personal data collected is not currently in place, describe how you will develop a process for limited personal data collection in the coming year and include how long personally identifiable information will be kept:

5.3. The Project Team is **required** to ensure all data, generated or collected during EVSE operation, will be stored in the U.S.*:

☐ **Check here to confirm and certify all data will be (year 1) or is (years 2+) stored in the U.S.***

Note: Include information on data localization policies, data classification, data transfer mechanisms, access controls, data encryption, etc.

6. Physical Security (PS)

6.1. Confirm the utilization of anti-tamper techniques to prevent, deter, and detect unauthorized physical access:

☐ Yes, anti-tamper techniques are utilized on or around all electric vehicle charging infrastructure equipment at [all of] the project site(s).

What anti-tamper techniques are utilized?

☐ No, anti-tamper techniques are **not** utilized on all electric vehicle charging infrastructure equipment at [all of] the project site(s)

How will you work to implement and install anti-tamper techniques in the coming year?

6.2. Outline organizational processes for monitoring and notifying the appropriate parties (not including ARDOT and end-users) in the event of unauthorized access:

Note: Include information on automated alerts, incident response team, notification procedure, escalation protocols, incident triage, communication plan, post-incident analysis, training, and regular stakeholder updates.

6.2.1. If no organizational processes for notifying appropriate parties in the event of unauthorized access is in-place, please define a process for developing a monitoring and notification plan within the coming year:

6.3. Provide any additional notable information related to cybersecurity below (if applicable):