PUBLICATION

Privacy and Cybersecurity Standards for NEVI Funded EV Charging Station Projects

Authors: Linghan H. Ji-Otto, Stefan R. Kostas, Aldo M. Leiva
March 23, 2023

This is the third article in a series of alerts that addresses what businesses, organizations and governmental entities should be considering as they navigate privacy and cybersecurity challenges encountered in the transition to electric vehicles and the supporting infrastructure. Please find our previous alerts here and here.

Privacy and Cybersecurity Standards for NEVI Funded EV Charging Station Projects

The National Electric Vehicle Infrastructure (NEVI) Formula Program, a program established and funded by President Biden's Bipartisan Infrastructure Law, has approved more than $1.5 billion in funding for the fiscal years 2022 and 2023 to build electric vehicle (EV) chargers across the U.S. This funding encourages a fast pace of infrastructure implementation and attracts an influx of new players to the electric vehicle charging space. As the adoption of EVs continue to increase and infrastructure is developed, both federal and state regulators are emphasizing the importance of prioritizing consumer privacy and security.

EV charging stations collect sensitive information such as payment data, and are connected to the power grid, meaning that a single attack could have severe consequences for both consumer privacy and the grid itself. Proactively addressing privacy and security issues during the construction of charging stations aligns with the federal government's push for widespread EV adoption and helps to prevent potential breaches in the charging infrastructure. This article offers a high-level discussion of the privacy and security requirements outlined in the Federal Highway Administration's (FHWA) rules and NEVI plans from three states, as well as a list of industry standards for charging stations.

Federal Highway Administration Rules

The Bipartisan Infrastructure Law requested that the FHWA develop mandatory standards concerning the development and operation of publicly available EV charging infrastructure in U.S. markets. As a result, in 2022, the FHWA proposed mandatory standards to provide a framework for the EV charging sector and the interconnected national grid. On February 28, 2023, the FHWA considered all comments received and published its final standards for projects funded under the NEVI Formula Program and projects for the construction of publicly accessible EV chargers under certain statutory authorities (Final Rule). The Final Rule takes effect on March 30, 2023. Note that the Final Rule is designed to set the *minimum* standards and does not prevent states and other designated recipients from establishing more stringent EV charging infrastructure requirements toward building a convenient, affordable, reliable, and equitable national charging network. To summarize, the Final Rule provides the following minimum requirements on privacy and cybersecurity issues for states and direct recipients of NEVI funds:

- **Payment processing**: Charging stations must offer secure payment methods that are accessible to people with disabilities and do not require a membership to use. Chargers and charging networks

must comply with Payment Card Industry Data Security Standards (PCI DSS).

- **Customer privacy**: Charging station operators should collect, process, and retain only personal information necessary to provide charging services to consumers. They must also take reasonable measures to safeguard consumer data.

- **Technical requirements**: Chargers, hardware, and software must conform to ISO 15118 standards for charger to electric vehicle communication. Chargers must communicate with a charging network via a secure method and be able to receive and implement secure remote software updates.

- **Data submission**: States and direct recipients must make certain data regarding charging stations and charging sessions on an aggregated and anonymized basis to the public. Some types of data should be submitted quarterly, some annually, and some only once.

- **Cybersecurity**: The Final Rule requires states to implement appropriate physical strategies for the location of the charging station and cybersecurity strategies that protect consumer data and protect against the risk of harm to, or disruption of, charging infrastructure and the grid. FHWA considered public comments on specific cybersecurity standards and decided to leave cybersecurity provisions in this Final Rule as areas of consideration by states to allow for evolution of state NEVI cybersecurity plans outside the regulatory process.

State NEVI Plans

The FHWA has approved the NEVI plans for EV charging infrastructure deployment in all 50 states, Puerto Rico, and D.C. (all approved plans can be found at this link). As a result, all states now have access to all fiscal year 2022 and 2023 NEVI formula funding to aid in building EV chargers covering approximately 75,000 miles of highway across the country. Most (if not all) of those approved plans address consumer privacy and cybersecurity issues, which underscores the significance of these issues in the EV charging landscape. Please see a high-level discussion below on the NEVI plans of California, Tennessee, and Florida[1].

California

The California Electric Vehicle Infrastructure Deployment Plan was approved by the FHWA on September 14, 2022. The plan recognizes the importance of securing EV chargers, because "EV chargers provide direct connections to the vehicle's onboard system and the EV charging service provider's network, and indirectly to the driver's smart phone if the charge is paid for with an app, banking information if a debit or credit card is utilized, telecommunications provider, and the electric grid." The plan cites California's Senate Bill 327 (SB-327), which is a law that requires a manufacturer of a connected device to equip the device with reasonable security features that are appropriate to the nature and function of the device. Although not specifically stated, the plan is signaling that EV chargers can be considered connected devices subject to SB-327. Applying the requirements of SB-327 to charging stations, charging station operators must implement reasonable security features to their EV charging stations to protect any information they collect from unauthorized access, destruction, use, modification, or disclosure.

Tennessee

In Tennessee, the Departments of Transportation, and Environment and Conservation collaborated and developed the Tennessee Electric Vehicle Infrastructure (TEVI) Deployment Plan. This plan provides an outline for Tennessee's goals of creating an EV charging infrastructure and joining the interconnected network across the country. One key consideration of the plan is the state's commitment to protecting against cybersecurity risks. Specifically, this plan discusses the attack vectors that arise with the necessary

components of EV charging, such as drivers' smartphones, banking information, and the connection between non-state-owned assets and state-owned intelligent transportation system infrastructure. As part of this commitment, "the State will require any subrecipients, prior to issuance of the award or other funding, to provide a cybersecurity plan that 'demonstrates compliance with applicable state and federal cybersecurity requirements.'" The state will then review the plan to ensure the subrecipient has demonstrated compliance with applicable state and federal cybersecurity requirements. Additionally, the plan must provide how the subrecipient will continually maintain and update its cybersecurity protocols throughout the life of the project.

Florida

On September 14, 2022, the FHWA approved the Florida Department of Transportation's (FDOT) Electric Vehicle Infrastructure Deployment Plan, which recognized that Florida "charging stations must provide reasonable assurance against cyberattacks, data breaches, and loss of privacy." The plan also identifies the operational impacts that such cyber incidents may cause, such as power quality issues and phase instability which could result in a cascade of effects throughout the electric power grid.

To address these concerns, the FDOT will develop and implement a cybersecurity plan that will govern such stakeholders as grid operators, vehicle manufacturers, original equipment manufacturers, vendors, and charging network operators. Cybersecurity plan requirements will include full-scope risk assessments to identify the comprehensive threat surfaces presented by the new EV infrastructure, as well as segmentation requirements, compliance with PCI DSS requirements, and documentation of security operations and certification of System and Organization Controls. The cybersecurity plan will also include guidance to inform risk assessments (including schedules for performing the same), as well as processes for selecting and implementing cybersecurity controls. The FDOT will also provide for governance and oversight of this cybersecurity plan and its implementation.

Industry Standards

The industry standards listed below are referenced in the FHWA Final Rules, state NEVI plans or other guidance as best practices for addressing privacy and cybersecurity concerns when constructing EV charging stations.

Open Charge Point Protocol

Open Charge Point Protocol (OCPP) is an application protocol that allows for communication between an EV charging station and the charging station management system. This protocol enables the charging unit and the central management system to communicate across different EV chargers (referred to as Electric Vehicle Supply Equipment, or EVSE). The OCPP's security framework addresses three common security issues: (i) secrecy of communications; (ii) authentication of the server, and (iii) authentication of the client.

ISO 15118

ISO 15118 is an international standard for the communications protocol between an EV and the charging station. Through this protocol's plug and charge feature, EV drivers can obtain instant authorization at linked charging stations by plugging the vehicle into the charge point. Charging stations must ensure encryption of messages with the EV and authentication processes to maintain compliance with ISO 15118. These standards have been endorsed by FHWA's Final Rules.

ISO 27001

The ISO/IEC 27001 is a comprehensive set of guidelines created by the International Standard Organization (ISO). These standards provide guidance for global businesses to maintain and regulate their information security systems and properly store business data. Specifically, these standards seek to achieve information security through confidentiality, integrity, and availability. Although these ISO standards were not specifically developed for electric vehicles or their charging infrastructure, it has been widely adopted in various industries. As a result, charging station operators may consider using it as a guide when building and configuring the hardware and software of their charging stations.

NIST Standards

The National Institute of Standards and Technology (NIST) provides non-binding guidelines for technologies and processes. NIST is currently developing a guidance document to provide methods for evaluating EVSEs with commercially available test instrumentation. NIST has previously released a tentative code regarding the operating requirements and transaction capabilities of EVSEs. This tentative code included the recommendation to administer repeated tests for accuracy and consistency. A published guidance document from NIST will have clearer standards for EVSEs and a safe, reliable, and interconnected national network.

Bottom Line

Establishing secure cybersecurity and privacy protocols is paramount to the protection of consumers as EV charging infrastructure is developed across the nation. Different levels of regulators have emphasized this point. To protect sensitive customer data, prevent security breaches, and ensure eligibility for federal and state funds, it is crucial to maintain compliance with federal and state-level regulations and industry standards. Companies constructing EV charging stations should seek guidance from legal counsel on specific requirements and implement the best practices outlined in this article. By doing so, companies can establish safe and secure charging stations that protect their customers' privacy, while contributing to a cleaner and more sustainable transportation system.

[1] We selected California for discussion because it received over $56 million funding in FY 2022, which is fairly large compared to other states. Tennessee and Florida are selected because Baker Donelson has offices in those states.