ITS AMERICA

Considerations for a Secure Electric Vehicle Charging Ecosystem

ITS AMERICA CYBERSECURITY WORKING GROUP

TECHNICAL EXCHANGE PANEL WHITE PAPER

ITSA.org 202-484-4847 info@itsa.org

A Mission for Safety

On June 29, ITS America's Cybersecurity Working Group, led by MITRE's Jess Baker, heard presentations from Susan Howard with Michael Baker International and ITS America Board Member Michelle Maggiore from Cisco on cybersecurity considerations for electric vehicle charging equipment. This special session convened leading experts and transportation stakeholders to bring clarity and awareness to the challenges and practice of "securing EV (Electric Vehicle) infrastructure" for ensuring a cybersafe, secure, and resilient transportation network.

The Problem to Solve

The working group discussed cybersecurity considerations related to electric vehicle charging, and, using the MITRE Problem Framing Canvas, brought specific attention to the immediate problem that cybersecurity for electric vehicle supply equipment (EVSE) is not being consistently implemented across the U.S. in accordance with any one framework for design, installation, or maintenance.

This lack of coordination impacts the ability to establish comprehensive cybersecurity requirements in statewide National Electric Vehicle Infrastructure (NEVI) Formula Program designs, which creates barriers and inequities in the ability to protect against, detect, and mitigate cyber-attacks to the power grid and substation equipment, electric vehicles, charging stations, and payment systems. This also leads to inadequate and insecure external operational data networks, further impacting stakeholder ability to secure PII (Personally Identifiable Information) data from an adversarial action and consequently increases operational budgets.

Ultimately, the main threat articulated was the security of the electric grid, national security safety concerns, and the economic impacts of grid breach.

Ultimately, the main threat articulated was the security of the electric grid, followed by national security safety concerns, and the economic impacts of grid breach, all of which represent a tempting target to potential harmful actors. This liability is further

expanded by the security risk and vulnerabilities present in some EVSE such as meters and other components.

Addressing the Dilemma

To address this dilemma, the speakers offered solutions that fell within two categories: increased collaboration among EV stakeholders, particularly between transportation and electric grid operators, combined with additional Federal policy guidance related to EV charging programs such as NEVI, and strengthened security procedures for EV infrastructure.

Increased Collaboration Between Electric Vehicle Stakeholders

The increasingly widespread deployment of EVSE represents a unique convergence between transportation and utility stakeholders. While these fields have overlapped to some extent with previous deployments, such as traffic management infrastructure and other digital infrastructure solutions, the scale and design of the planned electric vehicle charging infrastructure deployment presents a scenario in which coordination between transportation and utility stakeholders is necessary. The rules and standards governing the design and installation of electric vehicle charging infrastructure are primarily being written by experts from the transportation industry, such as in guidance from NEVI, and implemented by transportation agencies.

As an example, current NEVI cybersecurity requirements (NIST SP 800-175, 800-92, 800-94, 800-40, 800-61, 800-161, 800-53) relate primarily to IT (Information Technology) guidelines. These IT-focused standards are not effective barriers against cyberattacks on EVSE, while EVSE-cybersecurity specific standards such as NISTIR 8294 or OT-specific standards such as NIST SP 800-82 were left out of the requirements. More broadly, NIST requires 3rd party cybersecurity testing and certification, which provides no standard testing framework amongst NEVI funding recipients. Future Federal guidance and requirements related to EVSE design and installation must ensure that clear standards are set in place to prioritize mitigation of grid cybersecurity risks as a nondiscretionary, accountable requirement, as well as demonstrate how the policy development around those recommendations has

utilized input from grid security experts. Ideally, the method of Federal oversight of EVSE charging that the working group supports would be led by USDOT (U.S. Department of Transportation), and would include TSA (Transportation Security Administration), DHS (Department of Homeland Security), DOE (Department of Energy), and FERC acting cooperatively in coordination with state DOT (Department of Transportation) deployers. This collaborative approach will ensure that the various security considerations necessary for a robust electric vehicle charging network will be reflected in future Federal funding opportunities and regulations.

Strengthened Security Procedures for EV Infrastructure

In addition to working group recommendations pertaining to Federal regulations and guidance pertaining to EVSE, the speakers provided a number of specific best practices to better secure charging infrastructure from cyber threats. Here is a sample of some of the recommendations provided in this conversation:

- Encrypt all transmissions among EV infrastructure.
- Use a Public Key Infrastructure Certificate Authority to enable authentication between all EVSE equipment.
- Increase network segmentation and aspire toward a Zero Trust Network Architecture to the furthest extent possible.
- Follow NIST.IR.8294 and NIST SP 800-82r2/3 basic principles.
- Use Existing NERC-CIP Guidelines for the Electric Sector.
- Implement plans for continuous monitoring and incident response planning.
- Achieve network segmentation by isolating EVSE from other ITS systems and functions, including cameras and any localized Wi-Fi provisioning.
- Given that public sector operations staff will need to remotely access EVSE for maintenance, troubleshooting, and utilization metrics, ensure that the default passwords are not being used as current credentials for EVSE access.
- Utilize multifactor authentication to provide an extra step for accessing

the EV charging infrastructure network - use two or more independent credentials and a security token.
- In order to improve supply chain security, both software and hardware utilized with infrastructure management and monitoring should comply with IATF 16949 standards.
- Achieve network visibility by utilizing software that continuously monitors the network and enables the timely discovery of cybersecurity events.
- Develop a comprehensive cybersecurity program that not only provides safeguards to attacks, but also supports the ability to take the appropriate course of action and activities to contain an incident when it occurs.

EVSE Areas for Improved Practices

On July 20, cybersecurity committee leaders regrouped the technical panel and transportation experts to prepare a structured visualization and, using the MITRE Lotus Blossom innovation tool, organized aspects of EVSE cybersecurity into specific classifications that members then used to submit their feedback and ideas.

Figure 1 represents an initial set of focus area candidates for industry collaboration.

Securing Electric Vehicle Charging Infrastructure					
NEVI Cyber Regulation & Government Oversight	**National Cybersecurity Standards and Practices**	**Local Grid Protection from cyber-attacks at Entry Points**	**Local IT Ecosystem Security for Safe Integration**	**IOO & Complete Supply Stakeholder Ecosystem**	**Culture and Awareness for Digital Security**
▪ Operationalize national research as the baseline to regulation ▪ Need mechanism to invoke law on cyber incursions ▪ No Federal law & guidelines for securing EVSE (Electric Vehicle Supply Equipment) ▪ Could be patterned after power industry's NERC-CIP ▪ Missing liability regulations for outcome of cyber attack ▪ Responsible authority ambiguity ▪ Increase mechanisms to prevent physical manipulation of EVSE to create physical threats to users by changing the capacity to regulate electrical charges ▪ Increase mechanisms to improve user privacy, which can be impacted by unauthorized access to location, PII, and PSI data of individuals.	▪ All EV equipment should be Open Charge Point certified ▪ All EVSE in cloud should be Fed Ramp compliant ▪ Need standard testing frameworks ▪ Consider Consequence-Driven CSR for high-power charging infrastructure ▪ Missing electric IEEE (Institute of Electrical and Electronics Engineers) & IEC (International Electrotechnical Commission) (International Electrotechnical Commission) power standards for substations ▪ Missing adopted NIST standards for EVSE ▪ Encryption method implementations ▪ Convergent decision making	▪ Threat Modeling of Vehicle Charging Infrastructure ▪ Protect consumer data and the payment process ▪ Protect against disruption or harm to charging infra. and the grid ▪ V2X interface with facility's power management ▪ Adopt and enforce a reference architecture	▪ CSMS (Charging Station Management System) secure system mgt & payment processing ▪ One Continuous cybersecurity monitoring operations ▪ One Centralized, segmented, and monitored networks ▪ Distributed Energy Resources (DER) ▪ Installation and maintenance Staff training ▪ Meter installation cybersecurity	▪ Enable collaborative decision making ▪ For gap in Federal Law, industry needs to validate components in EVSE DFARS-889	▪ One Convergence of transportation, power, telecommunications leave data vulnerable. ▪ Consequence-driven cybersecurity and resiliency adoption ▪ Enable culture of permitted failure reporting to enable economies of scale in project learnings

Figure 1. Areas for Improved ESVP Cybersecurity Practices