State Guidance for EV Charging Infrastructure Cybersecurity

Massachusetts Electric Vehicle Infrastructure Coordinating Council

Jay Johnson
Renewable and Distributed Systems Integration
Sandia National Laboratories, Albuquerque, NM, USA

July 27, 2023
Cybersecurity Risks to EV Chargers

There has been good media coverage recently about EV Supply Equipment (EVSE) cybersecurity risks and attacks.

For those technically-inclined, there are also many research papers that cover the EV charger cybersecurity vulnerabilities, impacts, and defenses.

https://www.wired.com/story/electric-vehicle-charging-station-hacks/
Cybersecurity Clauses for EV Charging Infrastructure Procurements

- States submitted plans to National Electric Vehicle Infrastructure (NEVI) Formula Program: [https://driveelectric.gov/state-plans/](https://driveelectric.gov/state-plans/)
  - Limited detail on cybersecurity requirements for EVSE.

- PNNL and INL are working with DOT/DOE Joint Office to craft sample cybersecurity procurement language for the states.
  - Procurement Language expected at end of July. Preview located at: [https://driveelectric.gov/webinars/cybersecurity-procurement](https://driveelectric.gov/webinars/cybersecurity-procurement)

What’s this mean exactly?

Cybersecurity Clauses for EV Charging Infrastructure Procurements

**Cybersecurity Program**

- Audits and assessments
- Continuity of Operations
- Incident prevention and handling
- Robust Cybersecurity Program
- Subcontractor protections
- Risk acceptance and mitigation

**Identity, Credential, and Access Management**

- 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)]

**Configuration, Vulnerability and Update Management**

- 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)]

**Secure Payment**

- Payment Card Processing [23 CFR § 680.106 (f) (1)] [23 CFR § 680.106 (l)]

**Secure Communications**

- Secure charging communications [23 CFR § 680.114 (a) (b) (c) (d)]
- Data Privacy [23 CFR § 680.106 (l)]
- Cloud
- Cryptographic agility, Public Key Infrastructure [23 CFR § 680.106 (h) (2)] [23 CFR § 680.114 (a) (2)]

**Physical Security**

- Tamper prevention, detection, and response [23 CFR § 680.106 (h) (1)]
- Secure operation during communication outages. [23 CFR § 680.106 (h) (2)]

Managing Cybersecurity Contract Language

- **Preparing for the Contract**
  - Establish a cybersecurity team that operates for the life of the contract.
  - Establish and adhere to cybersecurity evaluation criteria (rubric) for all RFPs.

- **Over the Life of the Contract**
  - Cybersecurity and its importance should be regular themes in conversations.
  - Review and provide feedback on the Cybersecurity Program and Plan annually.

- **Managing Cyber Risk**
  - Cybersecurity risks evolve.
  - A 5-year contract requires 5 years of cybersecurity and contract management.
  - Focus on risk to the organization/site rather than compliance.
  - Ensure all cyber-related contract reporting is reviewed by your Cybersecurity staff, not just Contracts staff.

- **Contract End**
  - EV charging infrastructure cybersecurity protections should remain operative and effective.