Sandia National Laboratories

Exceptional service in the national interest

# 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

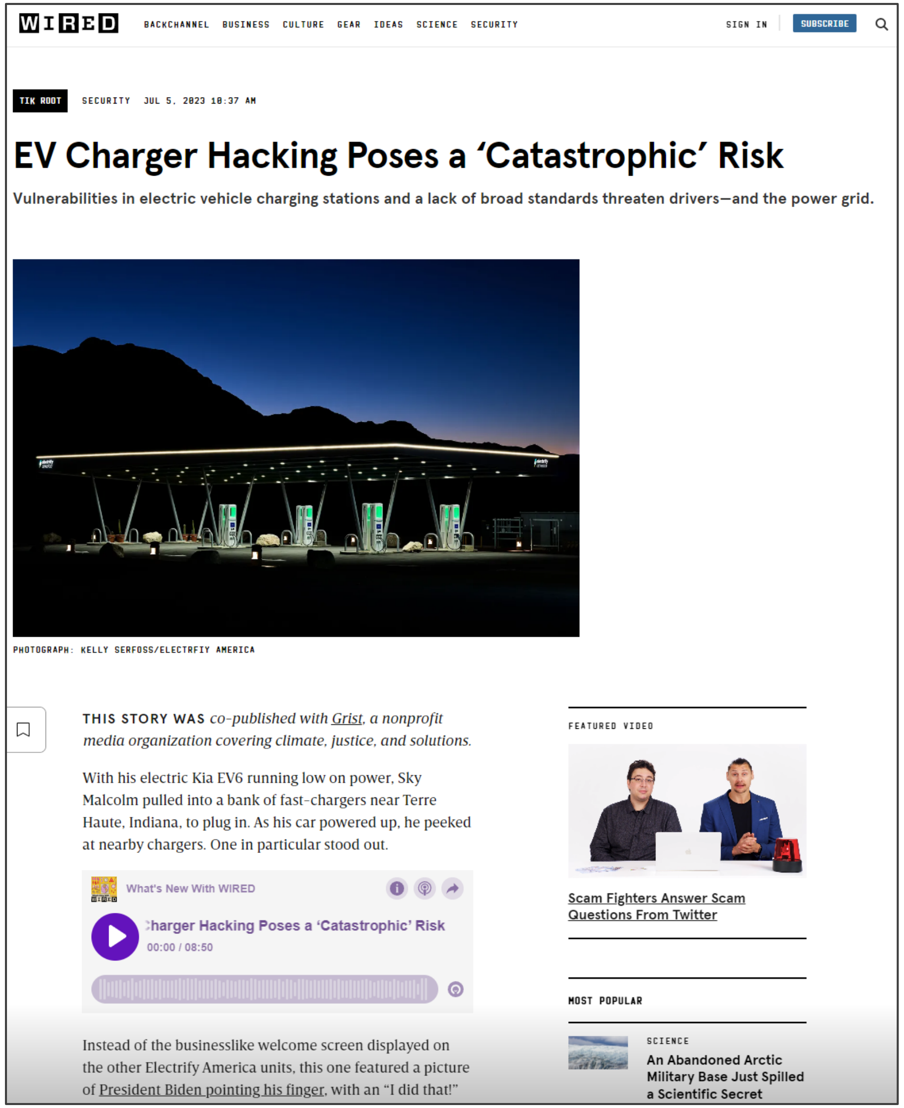
July 27, 2023

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

# 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.



TIK ROOT SECURITY JUL 5, 2023 10:37 AM

## EV Charger Hacking Poses a ‘Catastrophic’ Risk

Vulnerabilities in electric vehicle charging stations and a lack of broad standards threaten drivers—and the power grid.

PHOTOGRAPH: KELLY SERFOSS/ELECTRFIY AMERICA

THIS STORY WAS *co-published with Grist, a nonprofit media organization covering climate, justice, and solutions.*

With his electric Kia EV6 running low on power, Sky Malcolm pulled into a bank of fast-chargers near Terre Haute, Indiana, to plug in. As his car powered up, he peeked at nearby chargers. One in particular stood out.

Instead of the businesslike welcome screen displayed on the other Electrify America units, this one featured a picture of President Biden pointing his finger, with an “I did that!”

FEATURED VIDEO

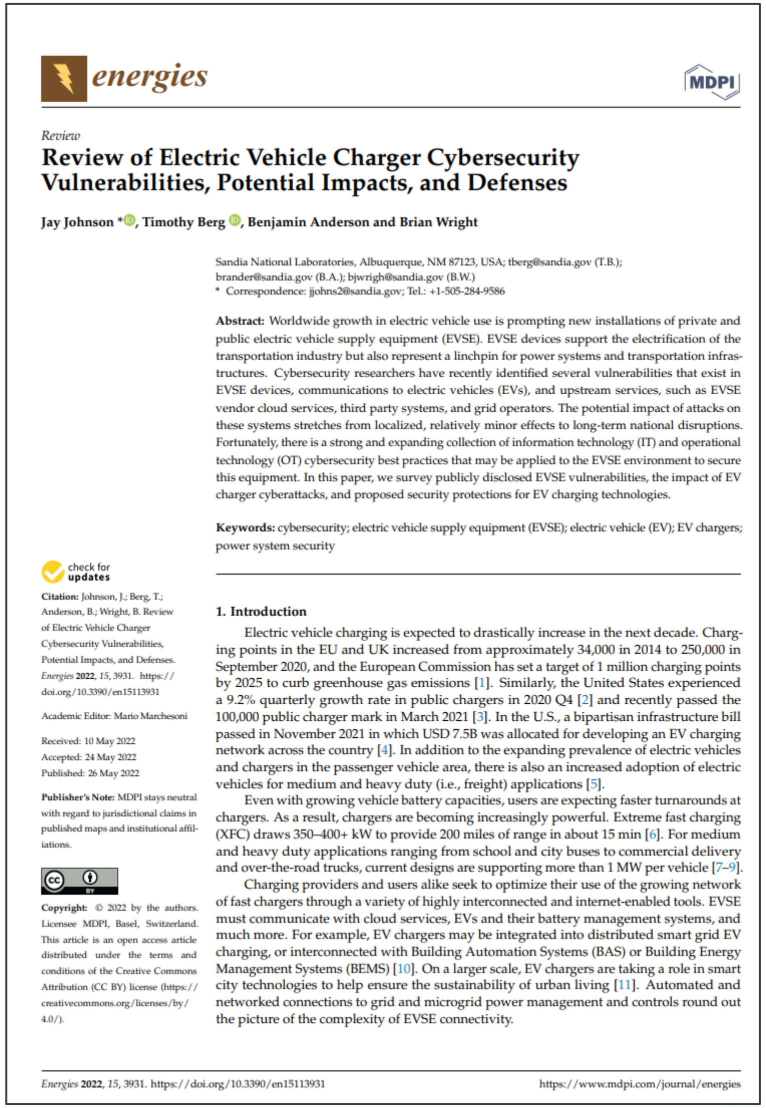
Scam Fighters Answer Scam Questions From Twitter

MOST POPULAR

SCIENCE

An Abandoned Arctic Military Base Just Spilled a Scientific Secret

https://www.wired.com/story/electric-vehicle-charging-station-hacks/



*Review*

### Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses

**Jay Johnson** *, **Timothy Berg**, **Benjamin Anderson and Brian Wright**

Sandia National Laboratories, Albuquerque, NM 87123, USA; tberg@sandia.gov (T.B.); brander@sandia.gov (B.A.); bjwrigh@sandia.gov (B.W.)
* Correspondence: jjohns2@sandia.gov; Tel.: +1-505-284-9586

**Abstract:** Worldwide growth in electric vehicle use is prompting new installations of private and public electric vehicle supply equipment (EVSE). EVSE devices support the electrification of the transportation industry but also represent a linchpin for power systems and transportation infrastructures. Cybersecurity researchers have recently identified several vulnerabilities that exist in EVSE devices, communications to electric vehicles (EVs), and upstream services, such as EVSE vendor cloud services, third party systems, and grid operators. The potential impact of attacks on these systems stretches from localized, relatively minor effects to long-term national disruptions. Fortunately, there is a strong and expanding collection of information technology (IT) and operational technology (OT) cybersecurity best practices that may be applied to the EVSE environment to secure this equipment. In this paper, we survey publicly disclosed EVSE vulnerabilities, the impact of EV charger cyberattacks, and proposed security protections for EV charging technologies.

**Keywords:** cybersecurity; electric vehicle supply equipment (EVSE); electric vehicle (EV); EV chargers; power system security

check for updates

**Citation:** Johnson, J.; Berg, T.; Anderson, B.; Wright, B. Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses. *Energies* **2022**, *15*, 3931. https://doi.org/10.3390/en15113931

Academic Editor: Mario Marchesoni

Received: 10 May 2022
Accepted: 24 May 2022
Published: 26 May 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

#### 1. Introduction

Electric vehicle charging is expected to drastically increase in the next decade. Charging points in the EU and UK increased from approximately 34,000 in 2014 to 250,000 in September 2020, and the European Commission has set a target of 1 million charging points by 2025 to curb greenhouse gas emissions [1]. Similarly, the United States experienced a 9.2% quarterly growth rate in public chargers in 2020 Q4 [2] and recently passed the 100,000 public charger mark in March 2021 [3]. In the U.S., a bipartisan infrastructure bill passed in November 2021 in which USD 7.5B was allocated for developing an EV charging network across the country [4]. In addition to the expanding prevalence of electric vehicles and chargers in the passenger vehicle area, there is also an increased adoption of electric vehicles for medium and heavy duty (i.e., freight) applications [5].

Even with growing vehicle battery capacities, users are expecting faster turnarounds at chargers. As a result, chargers are becoming increasingly powerful. Extreme fast charging (XFC) draws 350–400+ kW to provide 200 miles of range in about 15 min [6]. For medium and heavy duty applications ranging from school and city buses to commercial delivery and over-the-road trucks, current designs are supporting more than 1 MW per vehicle [7–9].

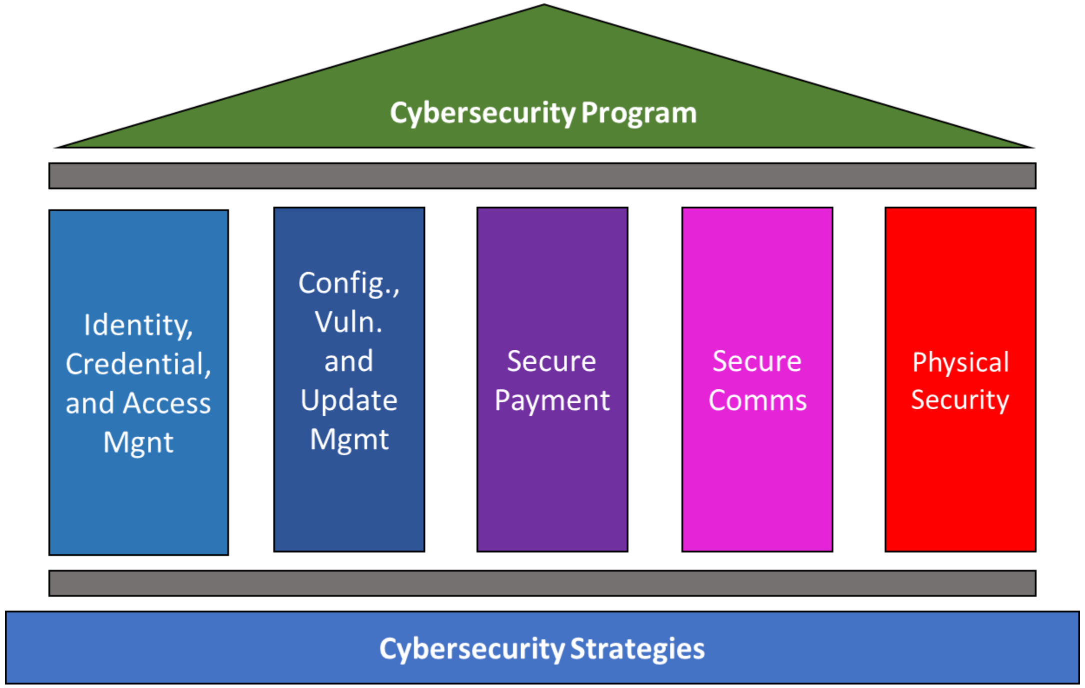
Charging providers and users alike seek to optimize their use of the growing network of fast chargers through a variety of highly interconnected and internet-enabled tools. EVSE must communicate with cloud services, EVs and their battery management systems, and much more. For example, EV chargers may be integrated into distributed smart grid EV charging, or interconnected with Building Automation Systems (BAS) or Building Energy Management Systems (BEMS) [10]. On a larger scale, EV chargers are taking a role in smart city technologies to help ensure the sustainability of urban living [11]. Automated and networked connections to grid and microgrid power management and controls round out the picture of the complexity of EVSE connectivity.

*Energies* **2022**, *15*, 3931. https://doi.org/10.3390/en15113931 https://www.mdpi.com/journal/energies

https://www.mdpi.com/1996-1073/15/11/3931

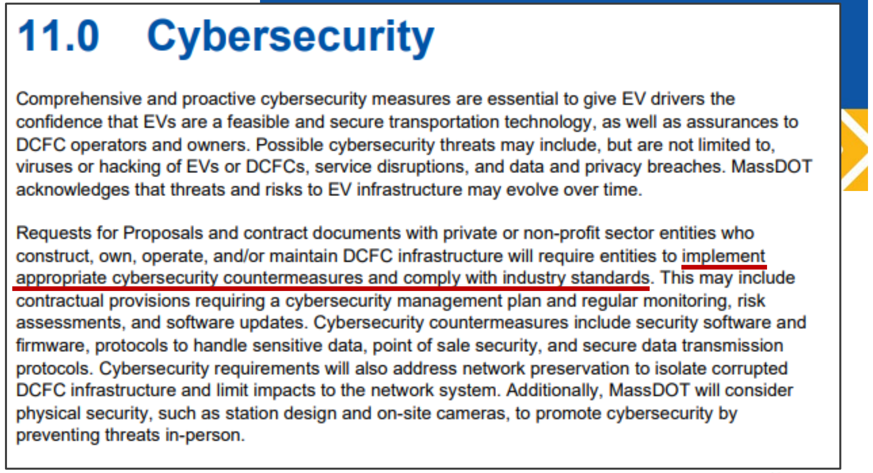
# Cybersecurity Clauses for EV Charging Infrastructure Procurements

- States submitted plans to National Electric Vehicle Infrastructure (NEVI) Formula Program: 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



National Electric Vehicle Infrastructure (NEVI) Program
Deployment Plan for Massachusetts
massDOT
Massachusetts Department of Transportation

What's this mean exactly?



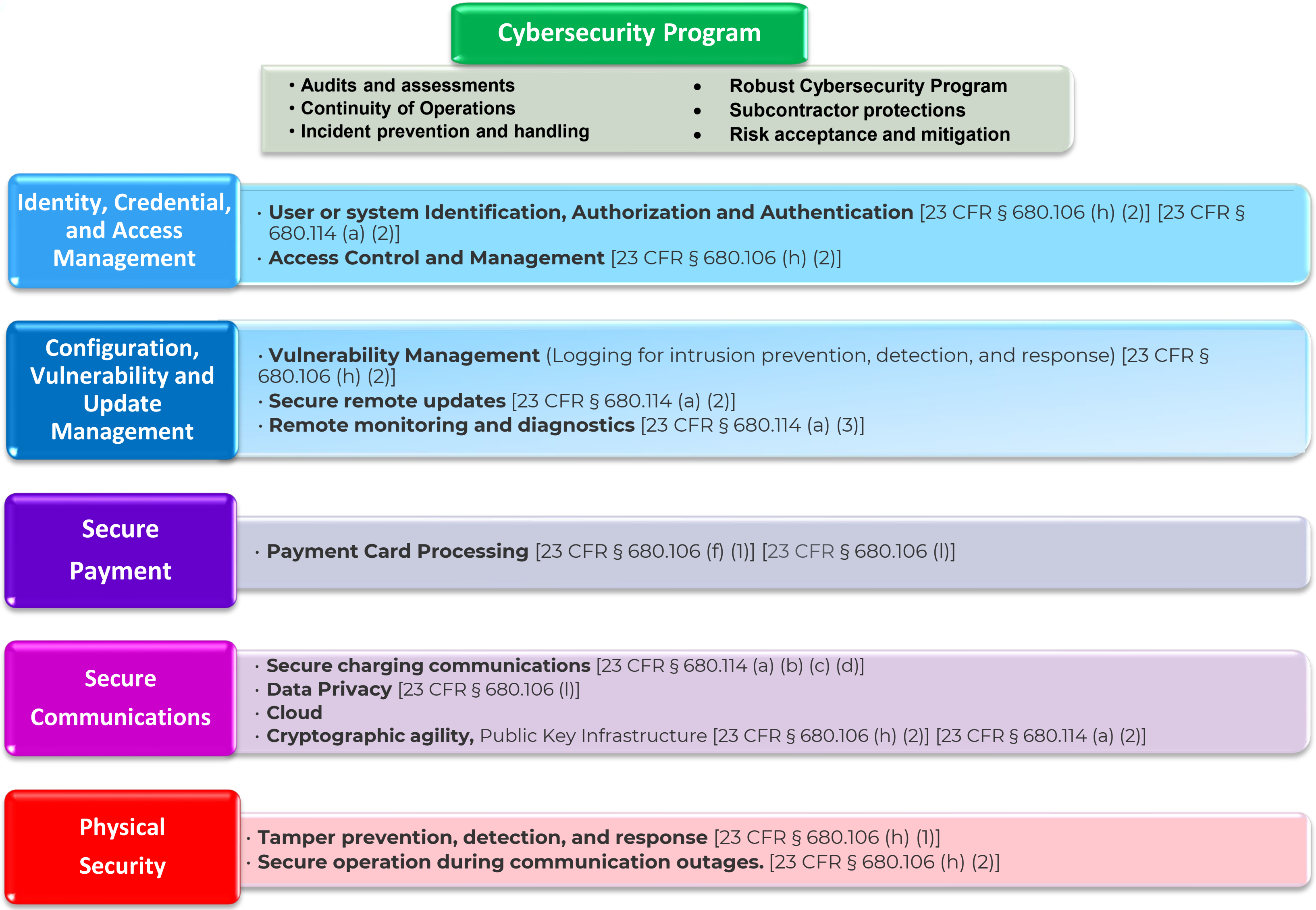
## 11.0 Cybersecurity

Comprehensive and proactive cybersecurity measures are essential to give EV drivers the confidence that EVs are a feasible and secure transportation technology, as well as assurances to DCFC operators and owners. Possible cybersecurity threats may include, but are not limited to, viruses or hacking of EVs or DCFCs, service disruptions, and data and privacy breaches. MassDOT acknowledges that threats and risks to EV infrastructure may evolve over time.

Requests for Proposals and contract documents with private or non-profit sector entities who construct, own, operate, and/or maintain DCFC infrastructure will require entities to implement appropriate cybersecurity countermeasures and comply with industry standards. This may include contractual provisions requiring a cybersecurity management plan and regular monitoring, risk assessments, and software updates. Cybersecurity countermeasures include security software and firmware, protocols to handle sensitive data, point of sale security, and secure data transmission protocols. Cybersecurity requirements will also address network preservation to isolate corrupted DCFC infrastructure and limit impacts to the network system. Additionally, MassDOT will consider physical security, such as station design and on-site cameras, to promote cybersecurity by preventing threats in-person.

Lori Ross O'Neil, "Sample Cybersecurity Procurement Clauses for EV Charging Infrastructure," Joint Office Webinar 4/18/23, https://driveelectric.gov/webinars/cybersecurity-procurement
L.R. O'Neil, T.E. Carroll, E.M. Abdelhadi, M.D. Watson, C.L. Hammer, M.B. Psarakis, "Sample Cybersecurity Clauses for EV Charging Infrastructure Procurements, Joint Office Report," PNNL-34454.

# 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

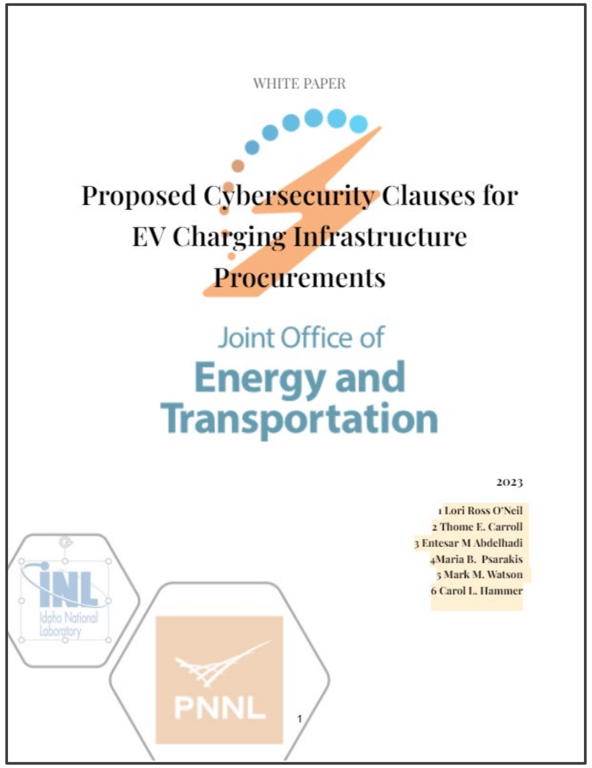
- **Payment Card Processing** [23 CFR § 680.106 (f) (1)] [23 CFR § 680.106 (l)]

## 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)]



WHITE PAPER

Proposed Cybersecurity Clauses for EV Charging Infrastructure Procurements

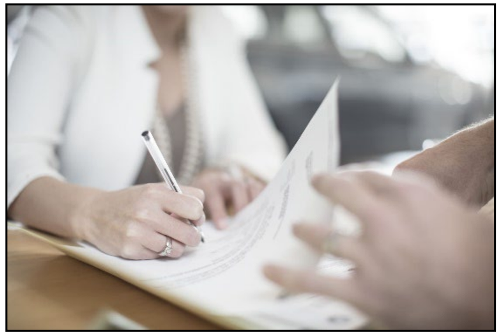
Joint Office of
Energy and Transportation

2023

1 Lori Ross O'Neil
2 Thome E. Carroll
3 Entesar M Abdelhadi
4Maria B. Psarakis
5 Mark M. Watson
6 Carol L. Hammer

Lori Ross O'Neil, "Sample Cybersecurity Procurement Clauses for EV Charging Infrastructure," Joint Office Webinar 4/18/23, https://driveelectric.gov/webinars/cybersecurity-procurement

# 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.

Lori Ross O'Neil, "Sample Cybersecurity Procurement Clauses for EV Charging Infrastructure," Joint Office Webinar 4/18/23, https://driveelectric.gov/webinars/cybersecurity-procurement