U.S. General Services Administration

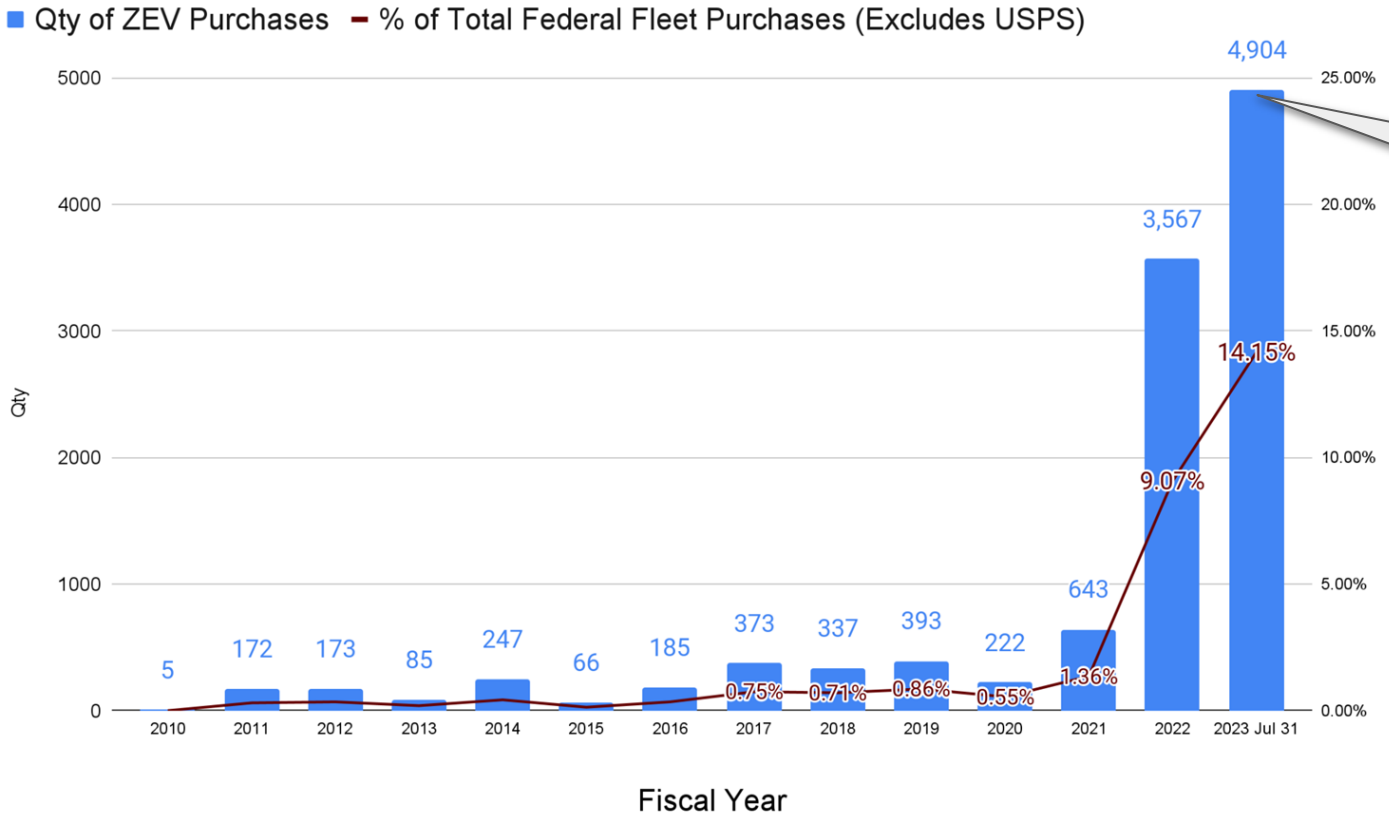
GSA Virtual EVSE Showcase

August 29 & 30, 2023

Cybersecurity for EVSE

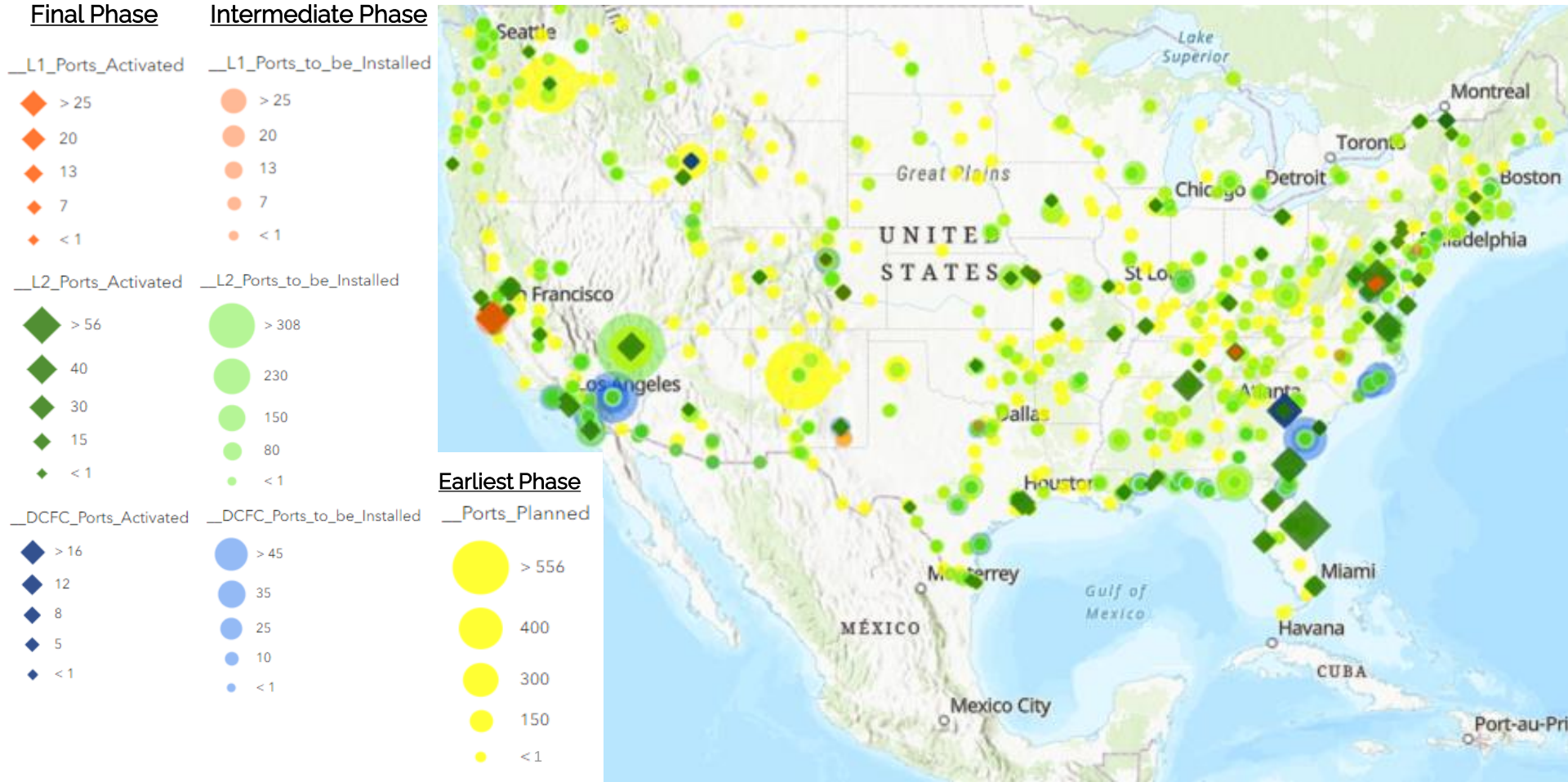
Stephanie Gresalfi (GSA Fleet)
Brian Turnau (GSA CISO)
Emmitt Durkaj (GSA CISO)
Tony Markel (NREL)

Federal Zero-Emission Vehicle Orders



5,372 as of August 27

Results: FY23 Q3 EVSE Deployment Report



Benefits of Cybersecurity

Prevents against Potential Threats

Secures Against Vulnerabilities

Allows Users to Confidently Use Technology

Measures to Protect

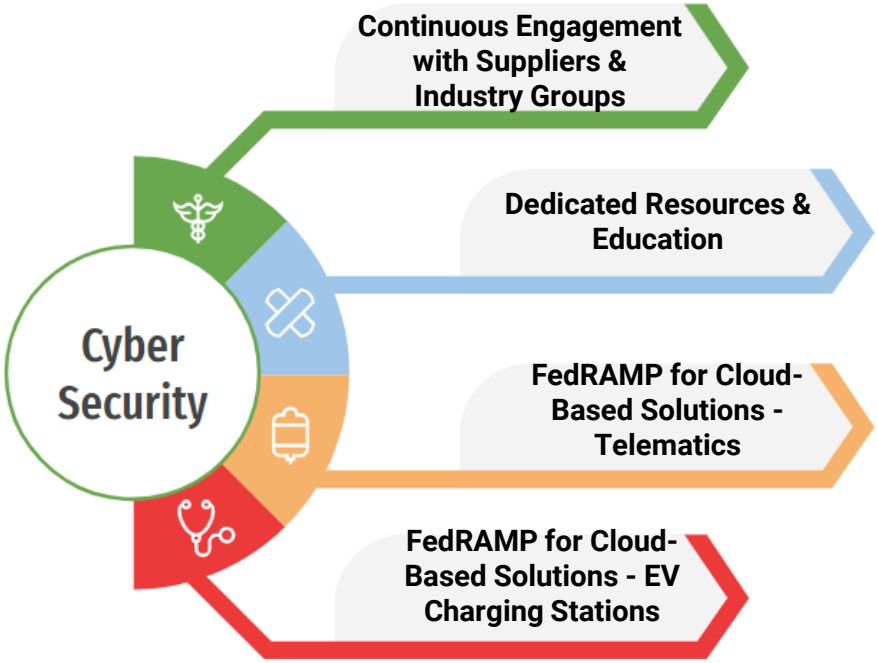
Risk Assessments

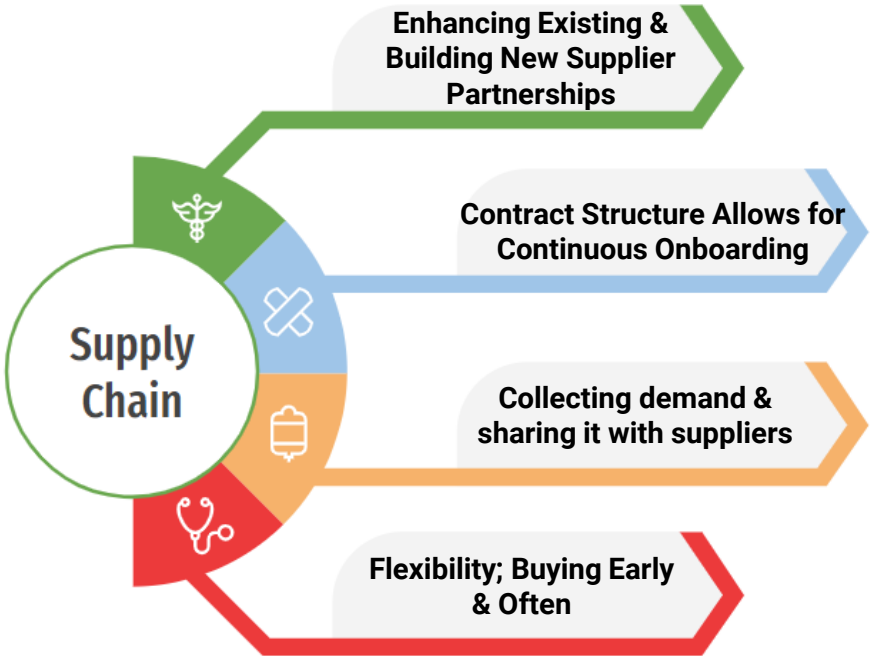
Security Measures

Regulations and Standards

NIST's new draft guidance for DC Fast

GSA's Approach to Cybersecurity





Continuous Monitoring Via GSA's Vendor Risk Assessment Program & C-SCRM Plan

Included IT Security Requirements in Winter 2022 EVSE Solicitation

7.4 Security, Privacy, and Supply Chain Security Requirements

Commercial Electric Vehicle (EV) Service platform providers are required to meet the appropriate Security and Privacy requirements identified in section 7.4.1 and Supply Chain Requirements in section 7.4.2 within six months of BPA award. No task orders can be issued under the BPA until the BPA Holder meets these requirements.

Offerors reselling commercial EV service platform solutions are presumed to provide EV platform provider solutions 'as-is' without additional value-added reseller systems (e.g., provisioning, billing, metering, etc.). See the ensuing sections for Security, Privacy, and Supply Chain Security Requirements.

All costs associated with meeting the Security, Privacy, and Supply Chain Security Requirements are the sole responsibility of the BPA Holder.

7.4.1 IT Security and Privacy Requirements

BPA Holders must obtain approval from GSA for the EVSE Deployment Option A or B for each distinct platform its products operate on using "NIST 171 v FedRamp Qualifying Template" (Appendix C). Products covered under Option A and B include but are not limited to network-connected charging stations or those that have the ability to connect to a network, products that store system or transactional data and network data plans.

The BPA Holder and the Government will mutually agree on a deployment option. Depending on the deployment option agreed upon, different security evaluation requirements will apply as outlined below. The final determination will be made by the Government.

A FEDRAMP OVERVIEW:

Introduction

Hardware vs Cloud?

Other considerations?

Criteria for Path Determination

Telematics

Verify that no information specific to a vehicle location can be readily tied back to a named individual through the IT solution.

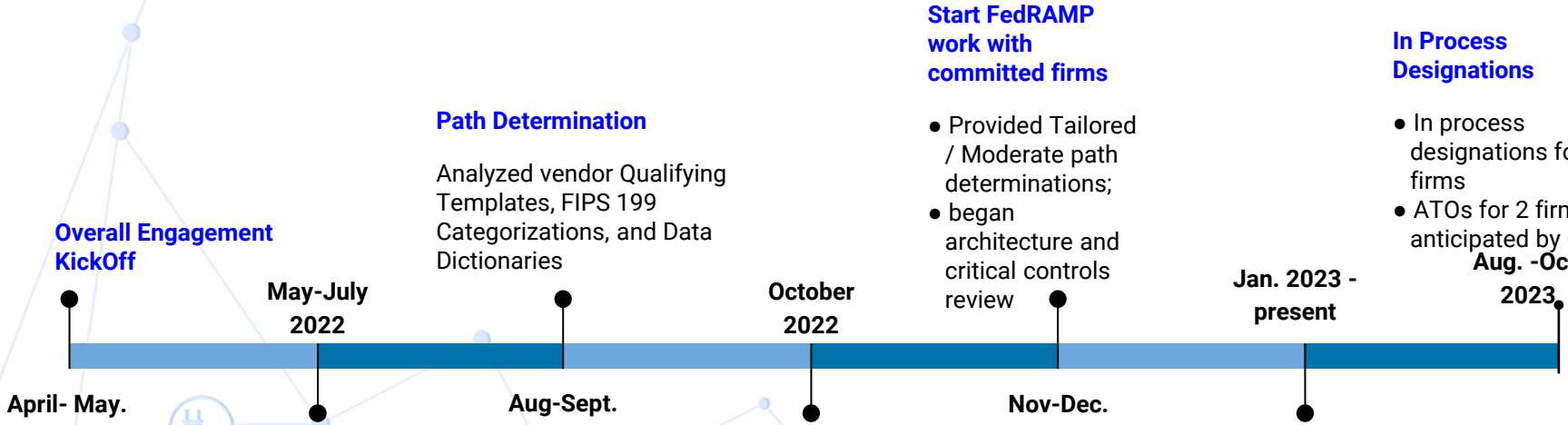
PII

Information solely tied to an individual

PCI

Information relating to payments such as bank routing or account numbers or credit card information to include the Primary Account Number (PAN), cardholder name, expiration date, and service code

Timeline



April- May. 2022

Overall Engagement KickOff

May-July 2022

Individual Vendor KickOffs

Aug-Sept. 2022

Path Determination

Analyzed vendor Qualifying Templates, FIPS 199 Categorizations, and Data Dictionaries

October 2022

Path Decision

All IT solution vendors would follow a FedRAMP path.

Nov-Dec. 2022

Start FedRAMP work with committed firms

- Provided Tailored / Moderate path determinations;
- began architecture and critical controls review

Jan. 2023 - present

Ongoing Path Determination & FedRAMP work

- Path determinations for recently added and unproductive vendors.
- Architecture and control review of productive vendors.
- Working with EVSE program to collect vendor schedules and formalize FedRAMP engagement.

Aug. -Oct. 2023

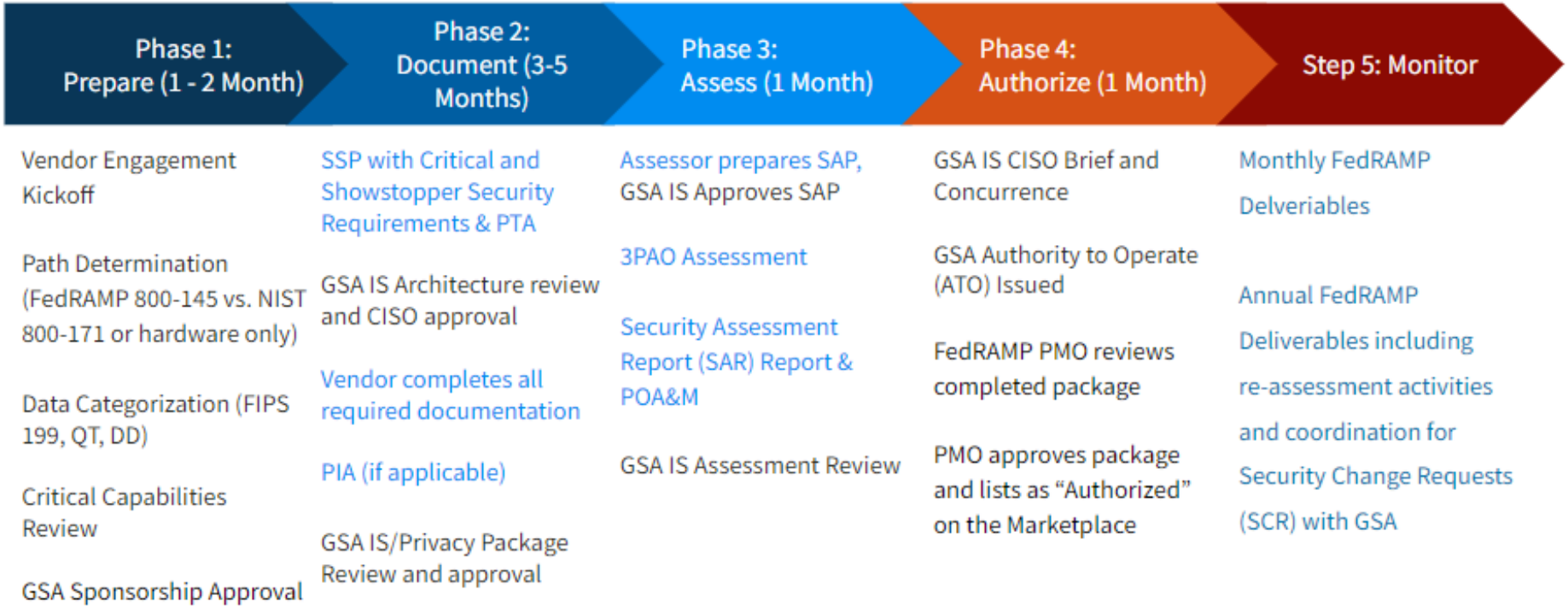
In Process Designations

- In process designations for 3 firms
- ATOs for 2 firms anticipated by Oct.

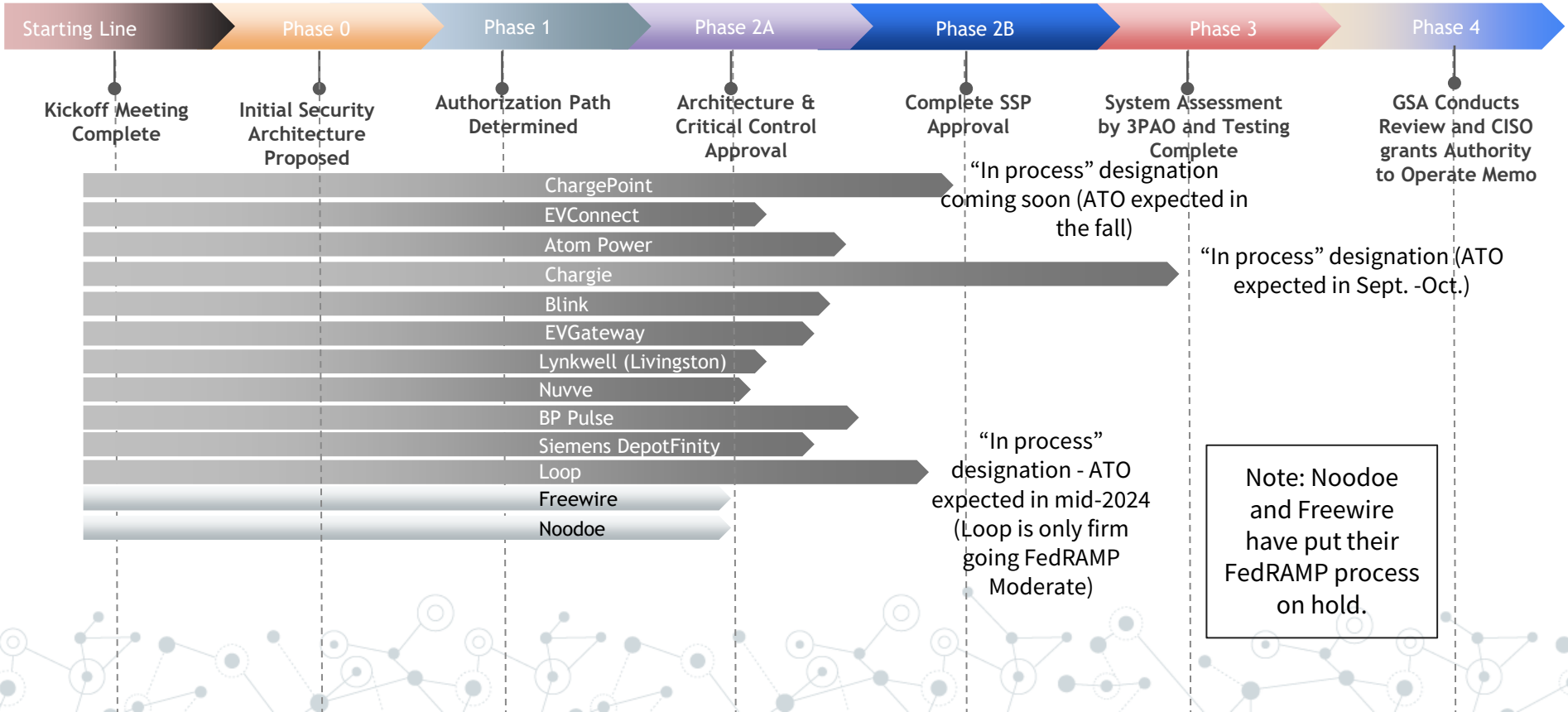
- GSA FedRAMP authorization is a well structured and interactive engagement that follows FedRAMP PMO guidelines
  - Expected timeline from FedRAMP Kick-Off :
    - Moderate: 12 - 18 months
    - Tailored: 6 - 9 months

FedRAMP - General Process & Overview

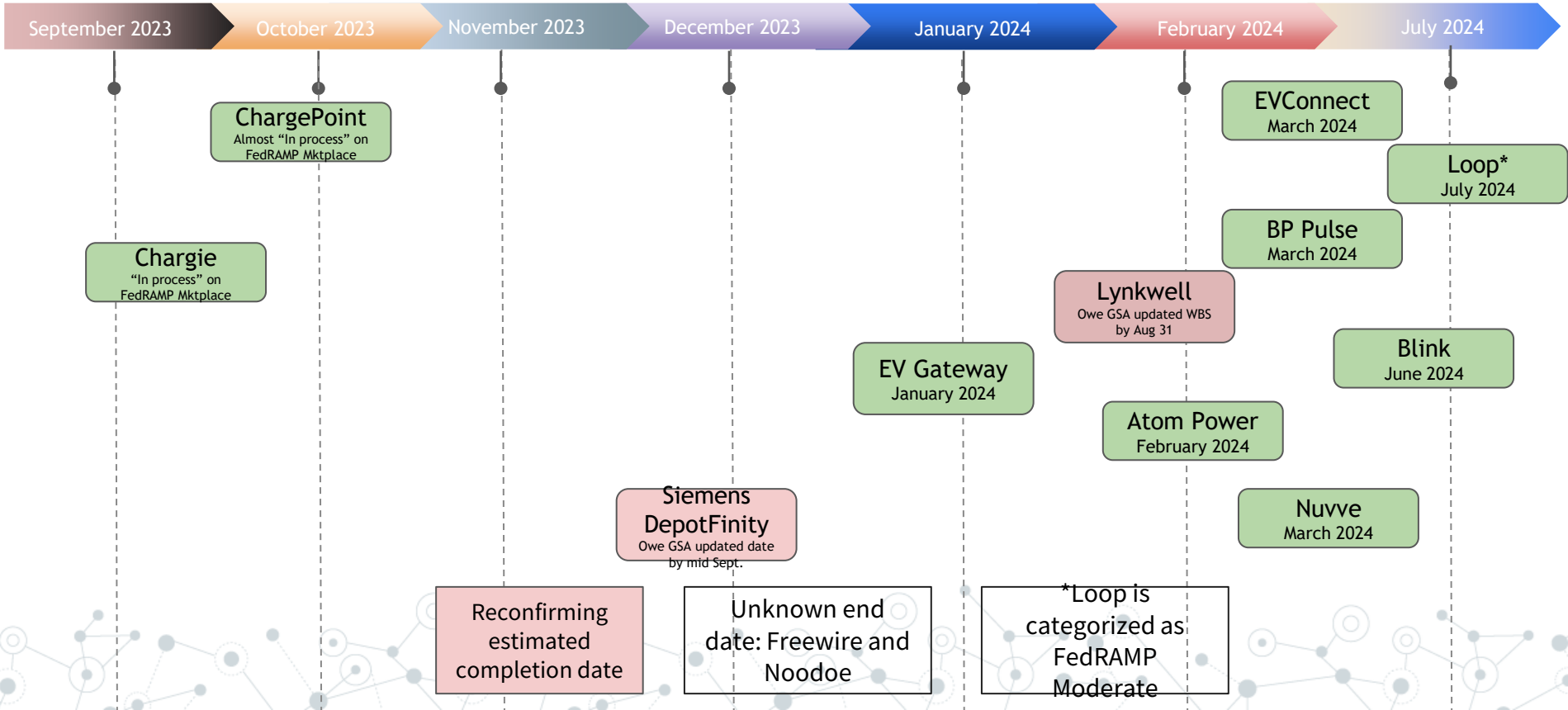
Legend:
Grey Text: GSA Responsibility
Blue Text: Vendor/Assessor Responsibility



EVSE IT Security FedRAMP Progress as of 8/21/23



FedRAMP Estimated Completion Dates Based on Firm Submitted Timelines (subject to change)



Interested in Learning about ATOs

- ➔ GSA will share all ATOs via email with all GSA Fleet customers and stakeholders
- ➔ Leave your email in the chat to be added to our EVSE Gov Delivery Box for future updates
- ➔ Attend Federal EV Agency Roundtable Meetings
- ➔ Attend Relevant GSA Trainings gsa.gov/gsa-fleet-training
- ➔ FedFleet 2024 - January 22-25, 2024
- ➔ DOE Energy Exchange March 26-28 2024 Pittsburgh, PA

Common questions?

How to Authenticate a Charging Station?

Common Questions

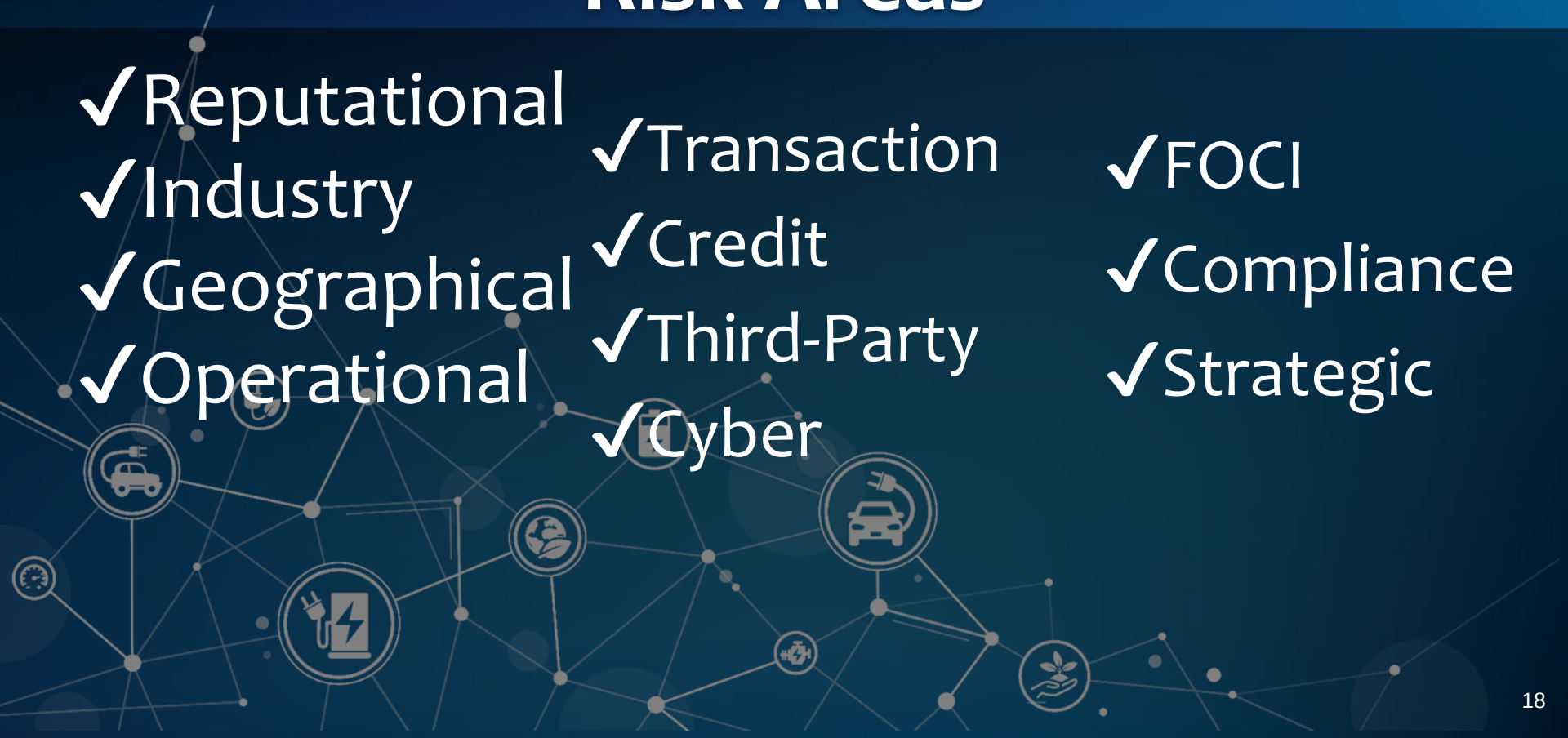
How to Authenticate a Charging Station?

How do we continue to mitigate risks?

The continuous monitoring process is a repeatable process that continuously identifies, evaluates, informs, monitors, mitigates, and remediates cyber supply chain and third-party risk exposure for GSA.

Risk Areas

- ✓Reputational
- ✓Industry
- ✓Geographical
- ✓Operational
- ✓Transaction
- ✓Credit
- ✓Third-Party
- ✓Cyber
- ✓FOCI
- ✓Compliance
- ✓Strategic



Vendor Risk Assessment Tool

- BitSight
- Exiger
- Govini
- Bloomberg


GSA

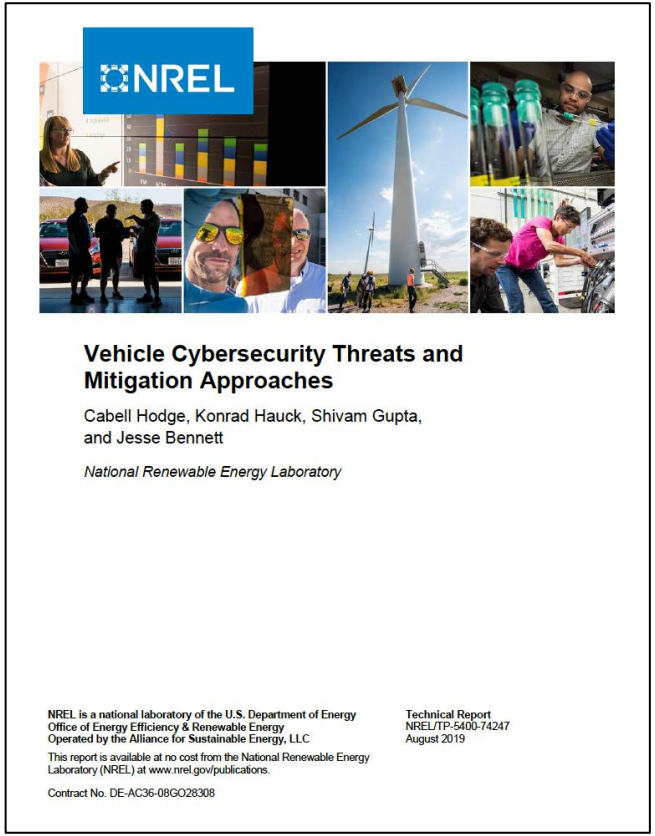
EVSE Cybersecurity and Resilience

Tony Markel, tony.markel@nrel.gov
Senior Researcher, Partnership Development

8/30/2023
GSA EVSE Cyber Panel

EVSE Cybersecurity

- In 2019 the FEMP Fleet Team at NREL published a report on Vehicle Cybersecurity Threats and Mitigation Approaches
  - Outlines Threat Vectors
    - Modern Vehicles
    - Connected and Automated Vehicles (CAV)
    - Telematics
    - EVSE
  - Risk Mitigation Techniques
  - Procurement Language

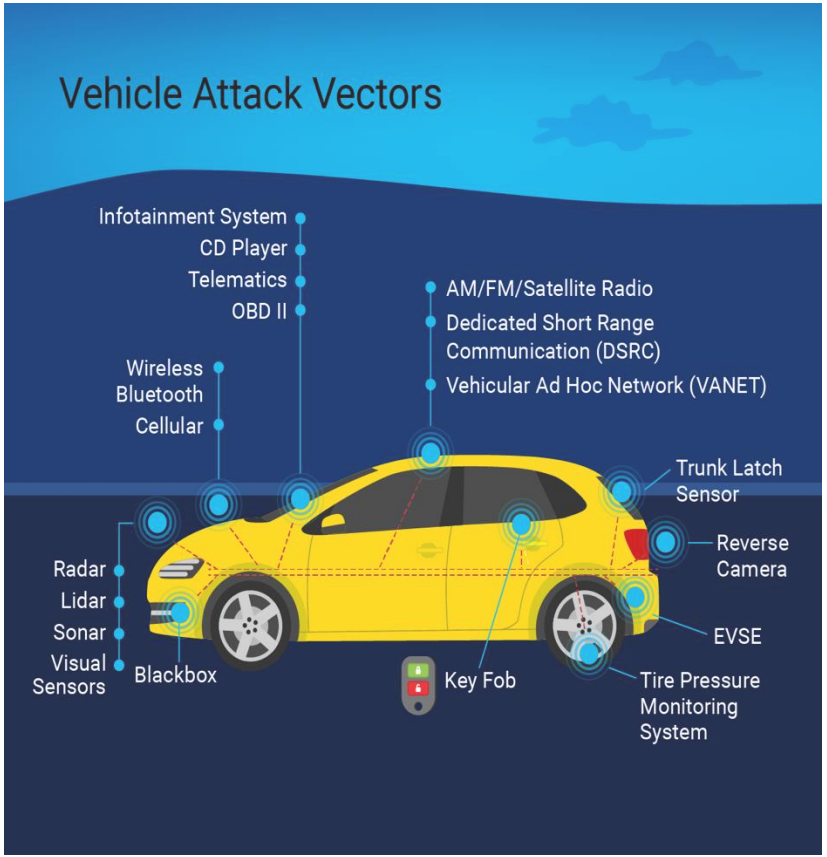


https://www.energy.gov/eere/femp/federal-fleet-cybersecurity

EVSE Cybersecurity

EVSE Cybersecurity Risks

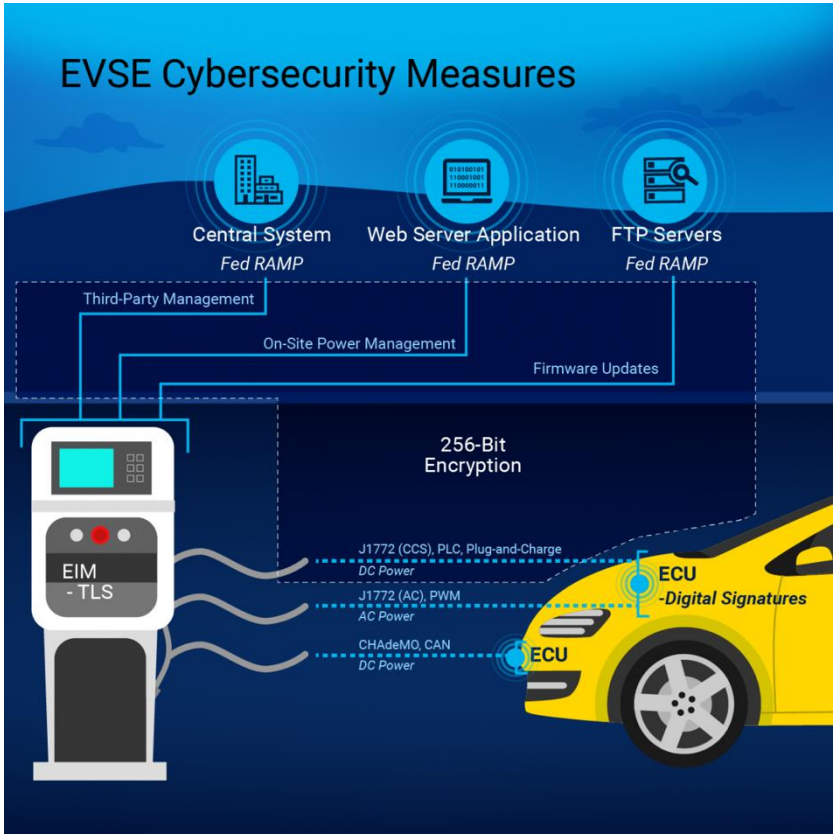
- Physical Access
  - An attacker with direct access to EVSE ports could directly upload malicious code resulting in malfunctioning EVSE or the release of PII.
  - Malfunctioning EVSE could impact power equipment.
- Remote Access
  - Access to information flow between EVSE and remote management service for wireless firmware updates, EVSE management, or transaction processing.
  - An attacker could acquire valuable user data or manipulate firmware updates to create EVSE malfunctions.



EVSE Cybersecurity

Cybersecurity Risk Mitigation

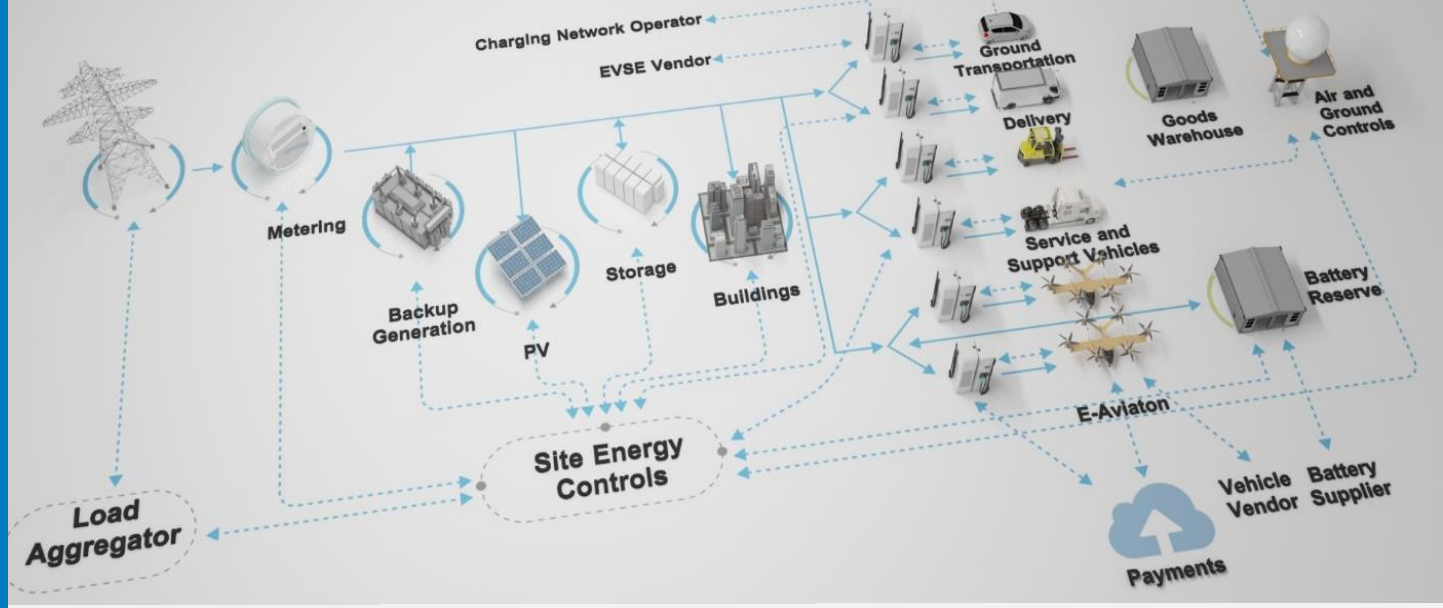
- Physical Access
  - EVSE should be constructed without external control board physical access.
  - All communication and management of the EVSE should include high-level encryption.
- Remote Access
  - Firmware updates should be encrypted.
  - Federal cloud servers must meet FedRAMP standards.
  - All remote access to EVSE through a web server should use secure communication.



Resources for Further Study

- Government Fleet and Public Sector Electric Vehicle Supply Equipment (EVSE) Cybersecurity Best Practices and Procurement Language Report (Volpe, 2019) - https://rosap.ntl.bts.gov/view/dot/43606/dot_43606_DS1.pdf
- Vehicle Cybersecurity Threats and Mitigation Approaches (NREL, 2019) https://www.nrel.gov/docs/fy19osti/74247.pdf
- DOE labs conducting research
  - Recommended EVSE cybersecurity practices (SNL, 2021) – (https://doi.org/10.13140/RG.2.2.11141.37602)
  - Survey of EVSE vulnerabilities (SNL, 2022) – (https://www.mdpi.com/1996-1073/15/11/3931)
- Joint Office of Energy and Transportation (DOT/DOE)
  - National Electric Vehicle Infrastructure Formula Program (DOT, 2022) (https://www.govinfo.gov/content/pkg/FR-2022-06-22/pdf/2022-12704.pdf)
- Industry activities
  - SAE PKI Task Force - https://www.sae.org/news/press-room/2022/04/sae-international-performs-first-test-of-ev-charging-pki-design
  - SAE/ISO Vehicle Cybersecurity Engineering - https://www.sae.org/standards/content/iso/sae21434/
  - Auto-ISAC Community Calls - https://automotiveisac.com/community-calls
  - Open Charge Alliance - Improved security for OCPP 1.6-J edition 3 FINAL, 2022-02-17 - https://www.openchargealliance.org/about-us/info-en-whitepapers/

Components and Interfaces



Components

EVSE

Vehicle

Charge Network Operations Center

Stakeholders

Charge Network Owner/Operator

EVSE Manufacturer

User/Driver

Vehicle Manufacturer

Fleet Operator

Interfaces

User to EVSE

User to Charge Network Operations

Vehicle to EVSE

EVSE to Charge Network Operations

Fleet Operator to EVSE/Charge Network Operations

Interoperable PKI for secure ISO 15118-2 communications confirmed!

~20 different key structure scenarios were tested over a 3-day period with 2 vehicles and 2 chargers in ESIF EVRI.

EVSE Security And Resilience Strategies

1. Understand what you have
2. Insert and wrap security solutions into the environment
3. Learn and architect a better system
4. Develop tools and insights to monitor and respond