



# Electric Vehicle Supply Equipment Security Solutions

*National Renewable Energy Laboratory*  
*Sandia National Laboratories*

November 06, 2024



## Electric Vehicle Supply Equipment (EVSE) Life Cycle Key Stakeholders

- Charge point operators
- Site/distribution system/utility/grid operators
- Vendor/manufacturers
- EVSE system owners
- Energy managers.

## EVSE Security Business Process

- Development, manufacturing, and provisioning
- Procurement, testing, and validation
- Third-party dependencies and incident response
- Maintenance and cyber-risk management.

## EVSE Security Technical Management

- Asset configurations
- Network and communication security
- Cryptographic measures
- Standardized best practices.



# Distributed Energy Resources - Cybersecurity Framework 2.0

- Self assessments covering –
  - Cybersecurity Governance
  - Cyber-Physical Technical Management
  - Physical Security
- Generates prioritized recommendations
- Provides dashboards for executive leadership
- Conducts comparative analysis

## Distributed Energy Resource Cybersecurity Framework

DER-CF 2.1 is here! Log in to see what's new! ✕



Home About ▾ Related Tools ▾ Impact ▾ Publications Support ▾

Logout

### Distributed Energy Resource Cybersecurity Framework

The Distributed Energy Resource Cybersecurity Framework (DER-CF) is a no-cost, interactive web tool that holistically evaluates a facility's distributed energy resource (DER) cybersecurity posture—or health—and makes customized recommendations.

CONTINUE



### Securing Distributed Energy Systems with NREL's DER-CF

Compared to centralized generation, DERs result in complex, data-driven communications. With DER-CF, facilities can protect their renewable energy assets and help ensure a more secure grid.

Text version

Hosted by NREL at [www.dercf.nrel.gov](http://www.dercf.nrel.gov)

# Questions for Industry | DER-CF/EVSE Advancements

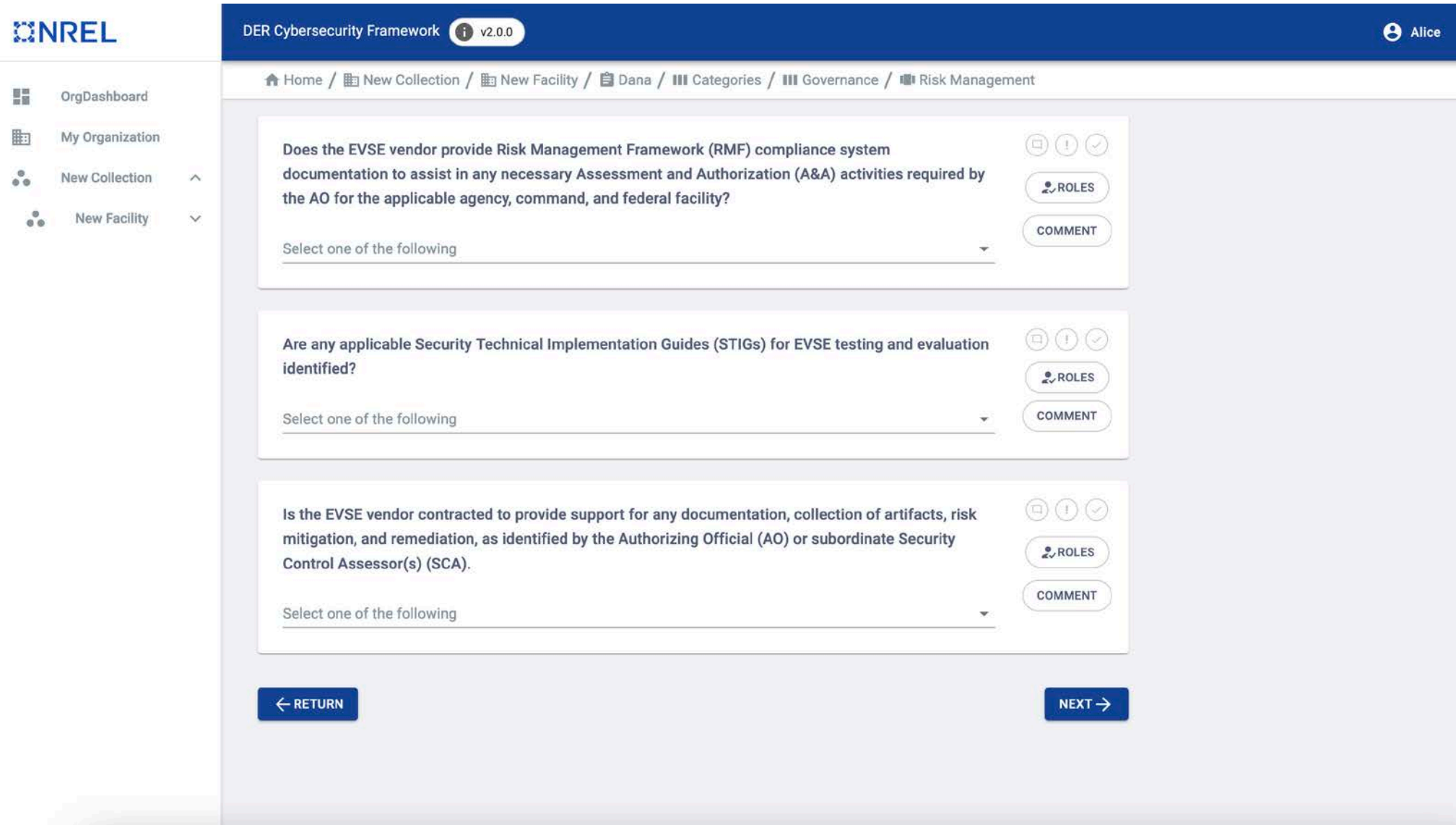
The screenshot displays the NREL DER Cybersecurity Framework v2.0.0 interface. The top navigation bar includes the NREL logo, the title "DER Cybersecurity Framework v2.0.0", and a user profile for "Alice". A breadcrumb trail shows the path: Home / New Collection / New Facility / Data / Categories / Governance / Third-Party Risk Management. The main content area features four survey questions, each with a dropdown menu and "ROLES" and "COMMENT" buttons.

**Question 1:** Is there a process for exchanging information on vulnerabilities with the vendor and implementing/addressing those vulnerabilities once discovered and reported in their products?

**Question 2:** Is there a process for the EVSE vendor to ensure secure provisioning of cryptographic keys, passwords, and initial credentials during manufacturing and servicing processes?

**Question 3:** Is there a process to verify if the EVSE vendor has established and enforced the use of secure coding practices in the development of the EVSE components following established best practices such as MISRA and CERT secure coding standards?

**Question 4:** Has the EVSE vendor established an internal code review process that in part reviews the security of the source code and integrated third party code libraries? Has this process been shared with the EVSE owner?



**DER Cybersecurity Framework** v2.0.0 Alice

Home / New Collection / New Facility / Dana / Categories / Governance / Risk Management

**OrgDashboard**  
**My Organization**  
**New Collection** ^  
**New Facility** v

**Does the EVSE vendor provide Risk Management Framework (RMF) compliance system documentation to assist in any necessary Assessment and Authorization (A&A) activities required by the AO for the applicable agency, command, and federal facility?**

Select one of the following

ROLES COMMENT

**Are any applicable Security Technical Implementation Guides (STIGs) for EVSE testing and evaluation identified?**

Select one of the following

ROLES COMMENT

**Is the EVSE vendor contracted to provide support for any documentation, collection of artifacts, risk mitigation, and remediation, as identified by the Authorizing Official (AO) or subordinate Security Control Assessor(s) (SCA).**

Select one of the following

ROLES COMMENT

**← RETURN** **NEXT →**



## Implementing the latest security methods and best practices

### Background

- Prior national lab work collected insights on subset of industry tools and capabilities.
- Opportunity to map tools and capabilities to EVSE security functions and needs.

### Current Focus and Progress

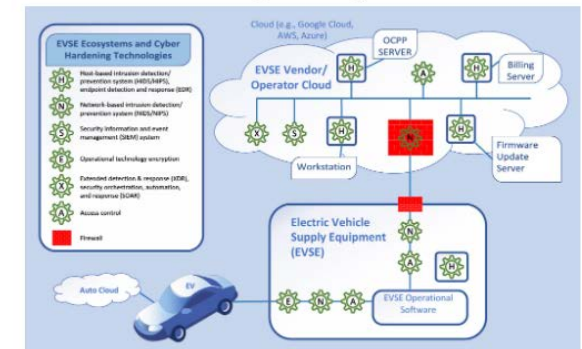
- Constructed a dynamic database (OpenEI platform) for engaging with industry.
- Ingested initial data from surveys.

### Future Directions

- Report on industry use and updates to the security solutions database.
- Assess where there may be gaps in needed security functions.
- Roll these insights into the development of assessment tools with EVSE stakeholder specific risk identification.



Electric Vehicle Charger Security Product Database



EVSE Security Solutions

Some of the cybersecurity hardening technologies available for EV charging systems include the following:

- HIDS/HIPS (H) - Host Based Intrusion Detection/Prevention System: System monitoring, logging traffic and activity that may be a threat./Host Intrusion Prevention System will be configured to halt suspected malicious activity on the system.
- EDR (H) - Endpoint Detection and Response: System monitoring, identification and response to threats at endpoints.
- NIDS/NIPS (N) - Network Based Intrusion Detection/Prevention System: NIDS listens to the network traffic and controls, logs and alerts.
- SIEM (S) - Security Information & Event Management System: This system organizes and prioritizes the data being logged in the systems response system.
- Encryption (E) - Operational Technology Encryption
- XDR/SOAR - Extended Detection & Response/Security Orchestration, Automation & Response: Create a Security Operations Center (SOC) that employs security information and event management (SIEM) and/or security orchestration, automation and response (SOAR) technologies.
- A/C (A) - Access Control

Hosted on OpenEI: <https://openei.org/wiki/EVSE>



- **HIDS/HIPS—Host-Based Intrusion Detection/Prevention System.**
  - System monitoring, logging traffic, and activity that may be a threat; HIPS will be configured to halt suspected malicious activity on the system.
- **EDR—End Point Detection and Response.**
  - System monitoring, identification, and response to threats at end points.
- **NIDS/NIPS—Network-Based Intrusion Detection/Prevention System.**
  - NIDS listens to the network traffic and controls, logs, and alerts.
- **SIEM—Security Information and Event Management System.**
  - This system organizes and prioritizes the data being logged in the systems' response systems.
- **Encryption—Operational Technology Encryption.**
- **XDR/SOAR—Extended Detection and Response/Security Orchestration, Automation, and Response.**
  - Create a security operations center (SOC) that employs SIEM and/or SOAR technologies.
- **AC—Access Control.**

## Conclusions

- Constructed a platform for open sharing of security tools for EVSE environment within OpenEI:  
<https://openei.org/wiki/EVSE>.
- Deployed EVSE control catalog within DER-CF.

## Next Steps

- Use the EVSE Security Solutions open data platform to engage with solution providers.
- Engage industry stakeholders to perform validation assessments using DER-CF/EVSE module.

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Vehicle Technologies Office. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.