Distributed Energy Resource Cybersecurity Framework and Cyber Range Integration

Shane McFly, Jordan Peterson, and Tami Reynolds

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-82545
May 2022

Distributed Energy Resource Cybersecurity Framework and Cyber Range Integration

Shane McFly, Jordan Peterson, and Tami Reynolds

National Renewable Energy Laboratory

Suggested Citation
McFly, Shane, Jordan Peterson, and Tami Reynolds. 2022. *Distributed Energy Resource Cybersecurity Framework and Cyber Range Integration*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-82545. https://www.nrel.gov/docs/fy22osti/82545.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-82545
May 2022

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

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 U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Federal Energy Management Program. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

NREL prints on paper that contains recycled content.

Acknowledgments

The authors gratefully acknowledge Hayes Jones, program manager at the U.S. Department of Energy Federal Energy Management Program, for her support in developing and enhancing the Distributed Energy Resource Cybersecurity Framework.

List of Acronyms

ARIES	Advanced Research on Integrated Energy Systems
C2M2	Cybersecurity Capability Maturity Model
DER	distributed energy resource
DER-CF	Distributed Energy Resource Cybersecurity Framework
DER-RM	Distributed Energy Resource Risk Manager
EO	executive order
FCF	Facility Cybersecurity Framework
FEMP	Federal Energy Management Program
NREL	National Renewable Energy Laboratory
TRN	Technical Resilience Navigator
XML	Extensible Markup Language

Table of Contents

1 Introduction

Distributed energy resource (DER) systems feature complex, data-driven communications networks that require careful system coordination and constant vigilance to ensure that grid assets are secure. Because DERs are an important component of the decarbonization strategy, agencies need to secure energy data that could implicate issues of national security if compromised.

To help federal energy managers assess, monitor, and manage cybersecurity while achieving decarbonization, the National Renewable Energy Laboratory's (NREL's) Distributed Energy Resource Cybersecurity Framework (DER-CF) offers a comprehensive, web-based assessment tool focusing on cyber governance or policies, technical management, and physical security. The DER-CF currently presents users with a series of pertinent cybersecurity questions that are used to generate a site-specific report and recommendations.

Discussion among NREL researchers, DER-CF users, and other partners has shown that the DER-CF's site-specific reports and recommendations can be overwhelming to planners as they process the data into action plans; the sheer amount of data collected by the DER-CF and similar cybersecurity risk management tools can result in a sense of information overload. Without a contextualized frame of reference, categorizing that information by sections of the system or prioritizing various controls can be a guessing game. A comprehensive visual presentation of that wealth of information would enable decision makers to direct their efforts and budgets to action items that would have the largest and most immediate impact on improving the compliance of the system at large.

This white paper outlines a plan to integrate the DER-CF with another key asset—NREL's cyber range—to visualize cybersecurity resilience and compliance and to enhance the usability and accessibility of the DER-CF for federal facility energy managers and planners. This integration will result in a visualization environment to interpret and interact with compliance data. Its development will include regular conversations with stakeholders to assess the effectiveness of these efforts, refine the visualization capability, and ensure its value to our partners.

The cyber range, along with other possible tools discussed in this paper, will be a useful contribution to the DER-CF; it generates emulated, multilayer grid environments that allow researchers to visualize and evaluate the interdependencies of power systems and network communications flows and to safely explore vulnerabilities and mitigation effectiveness. This unique capability is helping researchers better understand how to improve the security, resilience, and black-start recovery of today's critical energy infrastructure.

NREL is establishing a niche in cybersecurity research for renewable energy systems, including redefining how cyber-physical threats are identified. With the development of a revolutionary emulation platform for evaluating a wide variety of energy systems, researchers at NREL are making cybersecurity evaluations more visual, more tangible, more scalable, and more meaningful. Integrating the DER-CF and other tools with the cyber range will be transformative, allowing for the interactive visualization of current and future cybersecurity scenarios for each site.

2 Cybersecurity, Resilience, and Compliance Tools

This section describes the U.S. Department of Energy's (DOE's) Federal Energy Management Program (FEMP) and DOE cybersecurity compliance tools that might be suitable for integration with the cyber range. These tools provide capabilities for understanding or modeling the cybersecurity and resilience state of an existing system. They were considered for their feasibility of integration with the cyber range to add capabilities related to assessment, situational awareness, or system compliance. For this section, NREL met with the Pacific Northwest National Laboratory to decide which tools to consider for integration. The team decided that the Facility Cybersecurity Framework (FCF) would be most applicable and that FEMP's Technical Resilience Navigator (TRN) would also be a good candidate for integration with the cyber range.

2.1 Distributed Energy Resource Cybersecurity Framework

NREL has developed a tool for organizations with DERs to assess and improve their cybersecurity posture. With support from FEMP, the DER-CF provides a holistic assessment for evaluating the cybersecurity posture of DER systems—filling an important gap that expands on existing cybersecurity frameworks for more modern energy systems. The DER-CF was founded on and expands DOE's existing Cybersecurity Capability Maturity Model (C2M2), the National Institute of Standards and Technology Cybersecurity Framework, as well as other existing commonly used frameworks within the industry for DER technologies. The DER-CF is available as a written framework and as an interactive web tool.[1]

[1] See https://dercf.nrel.gov/.

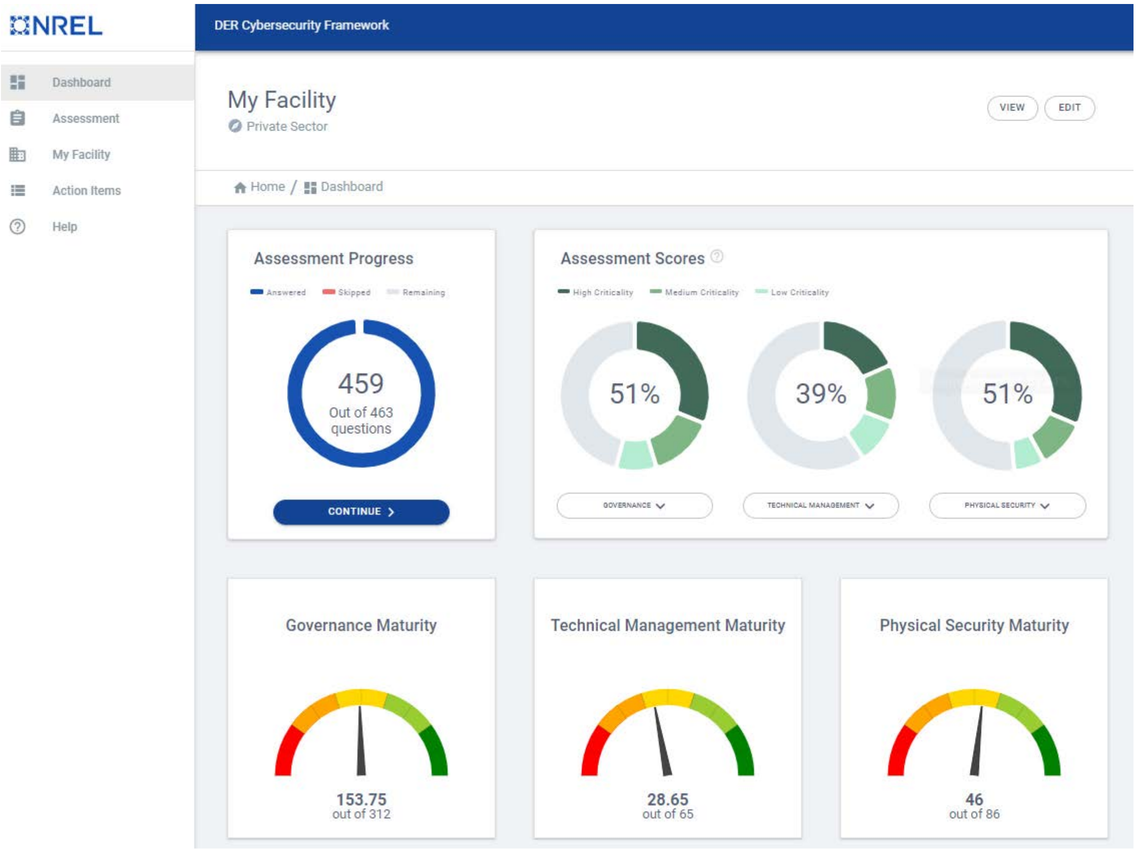


Figure 1. DER-CF asset definition page

First released in January 2020, the DER-CF provides a starting point for energy system facility managers to evaluate their cybersecurity posture through a guided assessment. It is a comprehensive tool that provides recommendations and prioritized action items based on the user's custom answers to a tailored questionnaire.

2.2 Distributed Energy Resource Risk Manager

The Distributed Energy Resource Risk Manager (DER-RM) was developed to help federal agencies strengthen their risk management processes and improve DER operational security.[2] The tool is unique in that it centers around an agile, content-driven approach, it serves as an internal-facing application to aid research and investigations based on user behavior, and it acts as a user experience-focused application to encourage repeated use. The tool also generates an Authorization to Operate package once the assessment is complete. The DER-RM allows the user to prepare for navigating through the steps of the risk management framework with structured questions about the facility and the DER system. This information is then used to enhance the user experience by customizing the stepwise process for each facility. The tool also provides recommendations for DER control implementation.

Designed to be a stand-alone application, the DER-RM is functional without external connections for the purpose of securely navigating through DER system-level questions. The

[2] See https://nrel-cyber.github.io/DER-RM/.

DER-RM is a framework that generates documentation for Authorization to Operate review and includes an easy-to-interpret and customized report that identifies common vulnerabilities and prioritizes mitigation strategies. The DER-RM addresses a critical consideration—the vulnerability of DERs to a range of operational risks—which does not exist in other well-known frameworks today.

2.3 Facility Cybersecurity Framework

The FCF tool equips organizations to better manage cyber risk, to continuously improve their cybersecurity posture, and to train operational technology and information technology staff on cybersecurity standards and best practices.[3] The easy-to-use, repeatable, holistic approach builds a culture that addresses the dynamic nature of cybersecurity risk. The FCF was designed based on the National Institute of Standards and Technology Cybersecurity Framework.

The FCF tool suite has been developed as part of several multiyear projects funded by FEMP. Operational technology cybersecurity tools help federal facilities understand their cybersecurity posture and comply with Executive Order (EO) 13636 and EO 13800. EO 13636, Improving Critical Infrastructure Cybersecurity, is designed to increase the level of core capabilities for our critical infrastructure to manage cyber risk. EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, focuses federal efforts on modernizing federal information technology infrastructure, working with state and local government and private sector partners to more fully secure critical infrastructure, and collaborating with foreign allies. In addition, all the tools within the FCF suite have been field-tested at multiple federal facilities. Although the FCF was primarily designed for operational technology networks in federal facilities, it can be used in nonfederal facilities as well.

2.4 Technical Resilience Navigator

FEMP's TRN helps organizations manage the risk to critical missions from disruptions in energy and water services. The TRN provides a systematic approach to identifying vulnerabilities and inefficiencies in a site's energy and water systems while prioritizing solutions that reduce risk. The TRN's unique focus on energy and water disruptions is intended to integrate with broader emergency preparedness as well as energy and water management, sustainability, and security efforts to strengthen the way those programs plan for energy and water resource availability. The completion of the TRN enables organizations to be proactive in identifying and addressing vulnerabilities to their critical energy and water systems, resulting in optimized systems that reduce outage impacts and support continuous mission operations that could result in cost and waste reduction.

2.5 Advanced Research on Integrated Energy Systems

Launched by DOE in 2020, the Advanced Research on Integrated Energy Systems (ARIES) is a research platform designed to mirror the complexity and scale of real energy systems[4] and support the transition to a modern energy system that is clean, secure, resilient, reliable, and affordable. Rather than evaluating new clean energy and energy-efficiency technologies in silos,

[3] See https://facilitycyber.labworks.org/.

[4] See https://www.nrel.gov/aries/.

ARIES expands the research view to take in the full picture—from consumers, to industry, to utilities. This perspective uncovers opportunities and risks in the spaces where energy technologies and sectors such as transportation, buildings, and the electric grid meet.

Although it is not a policy compliance tool like others in the paper, ARIES extends the power emulation environment of the cyber range, representing a substantial scale-up in experimental capability and allowing for power systems research at the 20-MW level. ARIES is built to be highly flexible, with the ability to plug and play different technologies into the core integrated system. This makes it possible to pivot and stay ahead of the rapidly evolving energy sector. ARIES was designed to support research of critical importance, including energy storage, power electronics, hybridization, infrastructure, and cybersecurity.

3 Cyber Range Emulation and Visualization

NREL's cyber range allows researchers and partners to study energy systems interactions with and dependence on digital communications devices and networks. NREL's unique energy system modeling and cosimulation capabilities are the differentiating factors in realizing proven cybersecurity protocols for increasingly renewable and distributed energy systems. To match the complexity of modern, multilayer grids, the cyber range is designed to evaluate multi-owner power systems and visualize interdependencies with digital communications devices and networks.

The cyber range provides the ability to virtualize, emulate, and visualize energy systems subjected to energy disruption scenarios, with the fidelity needed to represent future energy and telecommunications systems—from individual devices to regional grids.

The cyber range enables powerful, interactive research, administration, and management front ends; adds a powerful visualization and demonstration capability; and provides a library of emulation tools, including component models, configuration scripts, and prebuilt prototype research environments. This world-class capability is designed to answer research questions at scale using virtual and physical assets by leveraging simulation, emulation, and power-hardware-in-the-loop. Through the cyber range, NREL can emulate physical and communications-related aspects of DERs at scale to provide systems-level security evaluation for bulk power renewables and distributed energy systems.

3.1 Visual Representation Details

The cyber range uses a custom, NREL-designed application to provide 3D, real-time presentation of system data for an interactive, at-a-glance understanding of an experiment. It also uses data visualization dashboards and can be customized to use open-source or enterprise security information and event management systems for a deep view of an entire energy system. This allows the experiment user to visualize simulated attacks live for visual verification that their tests are running correctly. Alongside system emulation, visualizations can provide insight into broader elements, such as the state of compliance with respect to established security plans and processes.

3.2 Representation of Policy Compliance

The cyber range allows the user to view a system-wide illustration of compliance levels. The cyber range can create an emulated environment to demonstrate possible vulnerabilities associated with varying degrees of compliance. With minimal system information, the cyber range can illustrate generic compliance templates, reflecting low-, medium-, or high-compliance scenarios. With additional system information, a custom emulation can be generated.

NREL's cyber range provides a detailed view of a system's compliance state through advanced emulation and power-communications co-simulation, the ability to connect to physical hardware in the lab, and the ability to visually demonstrate a system's performance with its 3D, multilayer visualization tool.

4 Project Objective

The goal of this project is to build compliance visualization capabilities into the cyber range for use with the DER-CF and other risk management tools to enhance usability and accessibility for facility energy managers and planners in the federal sector and beyond.

During discussions with users and partners of the DER-CF and other FEMP tools, NREL researchers discovered that the format of the data collected by the assessment and compliance tools can create a barrier to further action plans. There is an opportunity to present the potentially overwhelming amount of data collected by these tools in a way that will prevent information overload. With the goal of creating a contextualized frame of reference, this integration seeks to categorize that information by sections of the system and create visual markers to highlight the effects of various strategies to prioritize implementing the tools' recommendations. Such a comprehensive visual overview of the data would provide insight to decision makers to help prioritize their efforts and maximize the allocation of resources to the recommendations that would have the greatest impact on the compliance state of the system as a whole.

Visualization will illustrate a site's current state of cybersecurity compliance based on technical and nontechnical information provided by the DER-CF. In turn, this visualization can help the user understand where they are in the compliance process and what remains to be done to attain full compliance. Further, this tool directs the user's attention to important areas that might still be incomplete, and this integration enables the modeling of user compliance in an emulated system hosted by the cyber range. A compliance server will deploy a templated system architecture, based on the user's responses, for the user to interact with. The project will be conducted in three phases over three years.

4.1 Phase 1

Phase 1 has two components. The first is developing a working visualization of system compliance using the DER-CF, and the second is planning the design of a server application that inputs data from the DER-CF into a working emulation model of the user's system.

The initial planning of the visualization entails designing the required user interface and data models. This phase will include minimal functionality because the core element is the user interface. Included in this phase is the ongoing collection of user feedback to influence the functionality and design of the visualization. The visualization application will need to intuitively reflect the user's compliance state based on the information provided to the integrated tools. Work performed in this phase will also include designs for connecting the front-end compliance visualization with the DER-CF tool. This step might require further development of the DER-CF to provide additional data to the visualization.

Designed components include (but are not limited to):

- Color markers for levels of compliance (red = noncompliant, yellow = partially compliant, green = compliant)
- Visual elements such as color highlighted boxes or pop-out text boxes to represent the different domains/areas of interest
- System architecture relating the DER-CF, compliance server, and visualization software

- Other visual constructs, such as risk graphs and compliance statistics.

The second component of this phase focuses on designing a compliance server. This server will act as the back-end computation and data processing for visualization. The core functionality of this server is to take information provided by the DER-RM to build a representative emulation of the user's described system. This emulation will be made into templates in various premade environments for the user to interact with. Key aspects of this emulated system will be influenced by the user's level of compliance. Some possible aspects include:

- Security of communications (HTTP/HTTPS)
- Access control
- System and event logging.

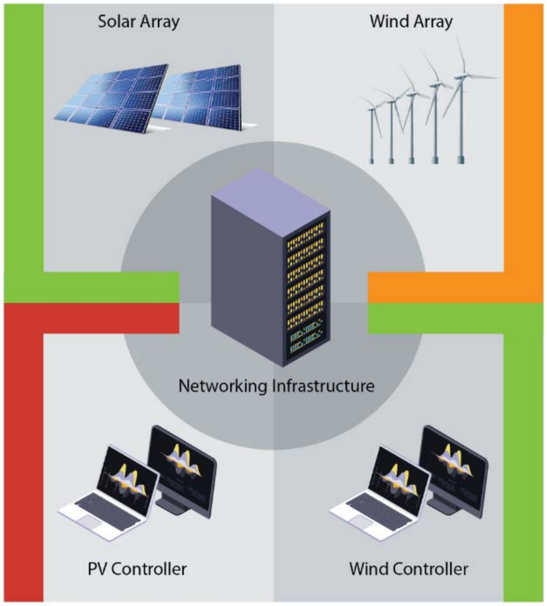


Figure 2. Example system compliance view. Green boxes indicate compliant system components, orange represents partial compliance, and red indicates noncompliance.

Image by Anthony Castellano, NREL

4.2 Phase 2

Phase 2 of the project is focused on building up the back end of the visualization and system emulation. In this phase, the data modeling and back-end architecture will be realized. The back end will connect to the DER-RM tool and process user data for the visualization to create a representative illustration of the user's compliance. Concurrently, this server will provide the system emulation with information on which template matches best. The designed components listed in Phase 1 will be built into a complete visualization system comprising DER-RM input, compliance server processing, emulation creation, and visualization software display. This phase will also include the exploration of any additional and/or optional information the user can provide to increase the fidelity of the visualization, statistics, and emulation.

4.3 Phase 3

With continued funding from FEMP, phase 3 will focus on expanding the integrated tools to use the ARIES initiative. The ARIES initiative aims to expand research on integrated energy systems to reflect the complexity and scale of real-world systems. The goal is to consider the full picture—including consumers, industry, and utilities—in the evaluation of clean energy. ARIES presents a unique opportunity for the DER-CF/cyber range integration to add realistic, complex modeling to help visualize the organization's assessment. The cyber range would also provide an interactive environment for understanding how system changes impact security compliance. To represent real-world clean energy applications, development cannot stop at the technical system. Adding these visualization capabilities to ARIES will help achieve the full-picture goal it is striving for by expanding the scope of the platform to assessment tools.

Including visualization for ease of use and understanding is a key feature provided by the DER-CF/cyber range integration. Leveraging ARIES in this integration allows for modeling complex energy systems at real-world scale. The ability of ARIES to provide flexibility through the plug and play of different technologies allows for richer and more realistic systems to include hardware-in-the-loop as well as the customization of software to better reflect the state of modeled systems.

ARIES integration with the DER-CF and the cyber range will support a variety of goals of existing projects that already use the platform. Providing an ARIES-enabled, interactive system replica will aid in planning equitable energy transitions, testing renewable scenarios for megacity modernization, checking errors of energy storage architecture plans, the provisioning of a secure environment to test proposed military microgrid solutions, and other future endeavors.

5 Technical Approach

5.1 Information Gathering

We have performed preliminary research through dry runs on three tools—DER-CF, FCF, and TRN—as mentioned in a previous section. We assessed a fictional environment and scenario to understand the output format of the results. In their current state, the tools lack machine-readable output that can be used to emulate representative environments. Most of the information documented by these tools is not system-specific, and additional information would be needed for an accurate representation of the machines and networks involved. The cyber range can be developed to be capable of compliance visualization regardless of the system information present. Combining system and policy information to provide a holistic view of compliance would immensely benefit the end user.

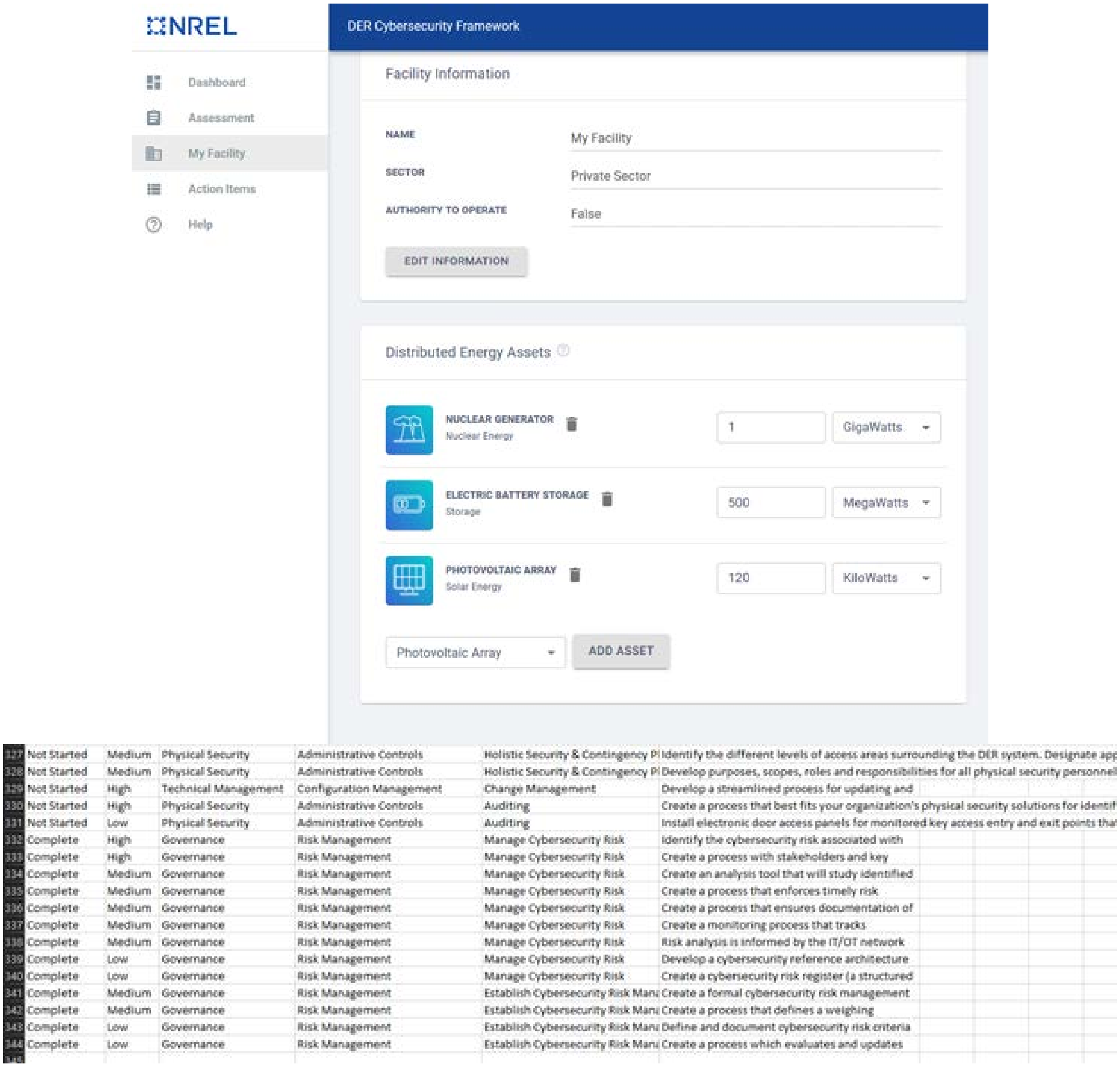
Further development of all tools is required to directly influence the emulation configuration. Next, we examined the DER-RM as a resource for emulation. Potential strategies for developing compliance visualization include templated visualizations to represent the user's choices from the DER-CF. Finally, we developed a budget for the integration and divided the tasks into three distinct phases, described in detail at the end of Section 4, Project Objective.

A large amount of data is required when showing cybersecurity compliance. There are a variety of tools that have been designed to collect and analyze these data. Before the integration of the DER-CF into the cyber range can be realized, further research on each FEMP tool (DER-CF, FCF, TRN) is needed to determine which data is being collected and the possibility of using that data in the cyber range. This will allow us to mitigate the "information overload" that users have reported experiencing when using these tools by, for example, merging duplicate information.

The research team operated each tool and documented which portions of the tools are relevant to the cyber range emulation. Following are the results of analysis provided with mock data to document the data relevance, data format, and tool interfaces to find machine-readable outputs for automatic input into the cyber range for visualization and emulation.

5.2 Available Distributed Energy Resource Cybersecurity Framework Resources

Although the DER-CF automatically generates files for download, the format was unusable without heavy modification. The output was an Extensible Markup Language (XML) file comprising a list of summary information about the tool; however, there did not appear to be any actionable outputs that could be used to influence an environment's generation. Additional development on the output is needed for the DER-CF. Some of the information gained by this tool can be used to generate compliance visualization. The project will initially focus on the development of the DER-CF and the cyber range application visualization before integrating other tools.



Facility Information

NAME: My Facility
SECTOR: Private Sector
AUTHORITY TO OPERATE: False

Distributed Energy Assets

NUCLEAR GENERATOR Nuclear Energy	1	GigaWatts
ELECTRIC BATTERY STORAGE Storage	500	MegaWatts
PHOTOVOLTAIC ARRAY Solar Energy	120	KiloWatts

Photovoltaic Array

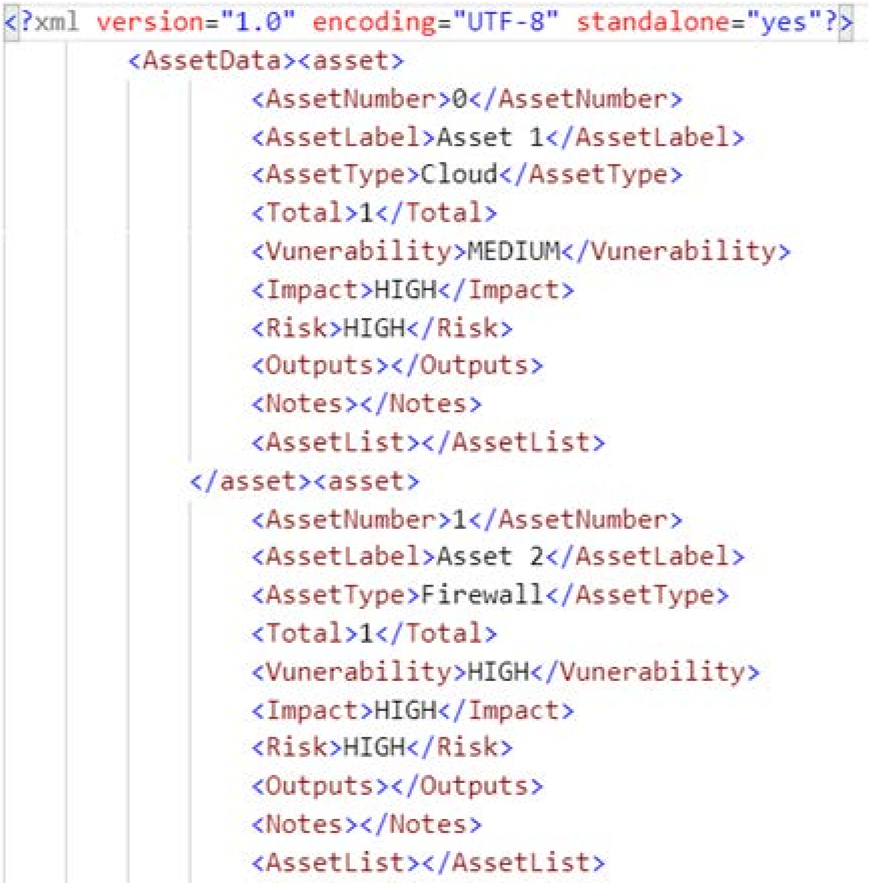
327	Not Started	Medium	Physical Security	Administrative Controls	Holistic Security & Contingency P	Identify the different levels of access areas surrounding the DER system. Designate app
328	Not Started	Medium	Physical Security	Administrative Controls	Holistic Security & Contingency P	Develop purposes, scopes, roles and responsibilities for all physical security personnel
329	Not Started	High	Technical Management	Configuration Management	Change Management	Develop a streamlined process for updating and
330	Not Started	High	Physical Security	Administrative Controls	Auditing	Create a process that best fits your organization's physical security solutions for identif
331	Not Started	Low	Physical Security	Administrative Controls	Auditing	Install electronic door access panels for monitored key access entry and exit points that
332	Complete	High	Governance	Risk Management	Manage Cybersecurity Risk	Identify the cybersecurity risk associated with
333	Complete	High	Governance	Risk Management	Manage Cybersecurity Risk	Create a process with stakeholders and key
334	Complete	Medium	Governance	Risk Management	Manage Cybersecurity Risk	Create an analysis tool that will study identified
335	Complete	Medium	Governance	Risk Management	Manage Cybersecurity Risk	Create a process that enforces timely risk
336	Complete	Medium	Governance	Risk Management	Manage Cybersecurity Risk	Create a process that ensures documentation of
337	Complete	Medium	Governance	Risk Management	Manage Cybersecurity Risk	Create a monitoring process that tracks
338	Complete	Medium	Governance	Risk Management	Manage Cybersecurity Risk	Risk analysis is informed by the IT/OT network
339	Complete	Low	Governance	Risk Management	Manage Cybersecurity Risk	Develop a cybersecurity reference architecture
340	Complete	Low	Governance	Risk Management	Manage Cybersecurity Risk	Create a cybersecurity risk register (a structured
341	Complete	Medium	Governance	Risk Management	Establish Cybersecurity Risk Mana	Create a formal cybersecurity risk management
342	Complete	Medium	Governance	Risk Management	Establish Cybersecurity Risk Mana	Create a process that defines a weighing
343	Complete	Low	Governance	Risk Management	Establish Cybersecurity Risk Mana	Define and document cybersecurity risk criteria
344	Complete	Low	Governance	Risk Management	Establish Cybersecurity Risk Mana	Create a process which evaluates and updates

Figure 3. DER-CF data output

5.3 Available Facility Cybersecurity Framework Resources

The user can download four files after completing the FCF. The first file is an assessment report. This contains mostly human-readable information summarizing the questionnaire and providing some analytics on that summary. This document does not integrate into the cyber range without modification because content cannot be imported into our system and parsed. Having the outputs in formats such as JSON or XML with context is required from each tool for a machine-readable output.

Although the content might need development for the project purposes, the format is compatible. The project team is currently testing methods on the DER-CF. After attaining proof of concept from these efforts, the team can explore ways to expand the cyber range to handle other tools, such as FCF. This tool is promising for implementation because its outputs closely align with desired inputs.

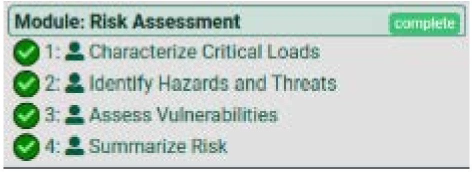


```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
        <AssetData><asset>
                <AssetNumber>0</AssetNumber>
                <AssetLabel>Asset 1</AssetLabel>
                <AssetType>Cloud</AssetType>
                <Total>1</Total>
                <Vunerability>MEDIUM</Vunerability>
                <Impact>HIGH</Impact>
                <Risk>HIGH</Risk>
                <Outputs></Outputs>
                <Notes></Notes>
                <AssetList></AssetList>
            </asset><asset>
                <AssetNumber>1</AssetNumber>
                <AssetLabel>Asset 2</AssetLabel>
                <AssetType>Firewall</AssetType>
                <Total>1</Total>
                <Vunerability>HIGH</Vunerability>
                <Impact>HIGH</Impact>
                <Risk>HIGH</Risk>
                <Outputs></Outputs>
                <Notes></Notes>
                <AssetList></AssetList>
```

Figure 4. FCF data output format

5.4 Available Technical Resilience Navigator Resources

This tool has the user input data into the risk assessment section—specifically, the critical load, hazards, and threats—and assess vulnerability pages. There were no generated outputs for this tool. Further development is required to enable the use of this tool in our integration. Having a machine-readable output much like DER-CF or FCF will allow us to use the information the user provided to this tool. Initially, the project will focus on DER-CF integration. Once that is finished, the focus will return to the TRN.



Module: Risk Assessment complete

✓ 1: Characterize Critical Loads

✓ 2: Identify Hazards and Threats

✓ 3: Assess Vulnerabilities

✓ 4: Summarize Risk

Figure 5.TRN risk assessment module

6 Conclusion

The integration of the cyber range and the DER-CF assessment tool will enhance how the energy sector infrastructure is installed, operated, maintained, and monitored. Current DER-CF capabilities will shift from asking human-based questions across governance, technical, and physical domains to serving as the source of supplemental data for technical, hands-on assessment.

Additionally, the cyber range will establish an implementation to emulate, virtualize, and place hardware-in-the-loop to recreate an environment at a federal site, utility, or private customer. This capability will enable users to overcome the information overload that results from the vast data collection involved in cybersecurity compliance tools. Using an interactive visualization environment, facilitated by integration with the cyber range, will provide a context for decision-making as well as a learning and training environment to understand the next steps needed to attain compliance. Through visualization, better understanding of compliance in a real system has the potential to increase an organization’s security posture in their pursuit of energy efficiency and decarbonization.

This paper described a plan to integrate the DER-CF, followed by related cybersecurity tools, with the NREL cyber range capability. We discussed how to design such virtual environments and how to integrate data resources from each tool. This plan will depend on constant user feedback to refine and improve the visualization capabilities so that federal facility energy managers have a customized environment to check cybersecurity compliance, perform education and training, and securely integrate new technologies.