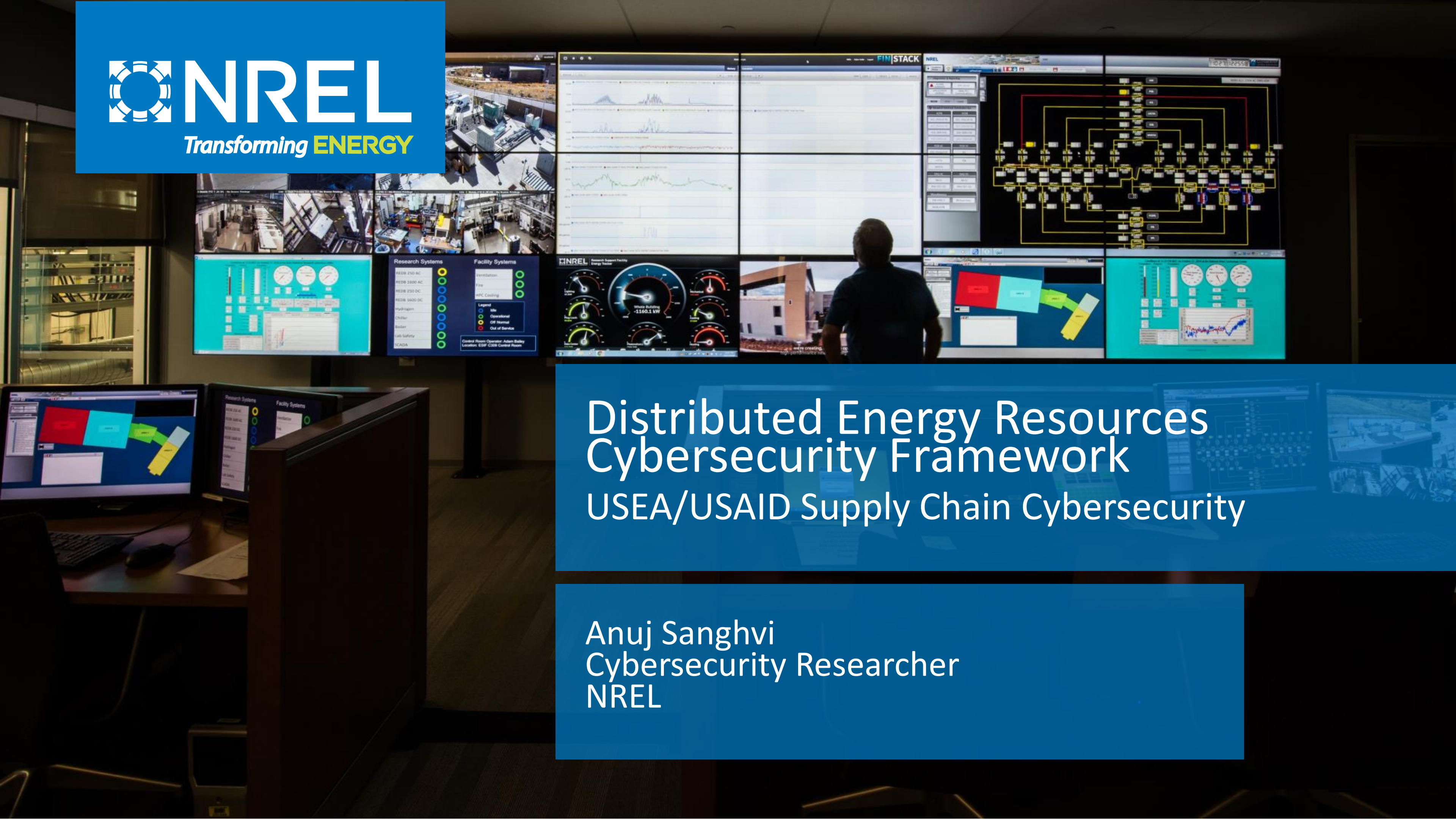


NREL
Transforming ENERGY

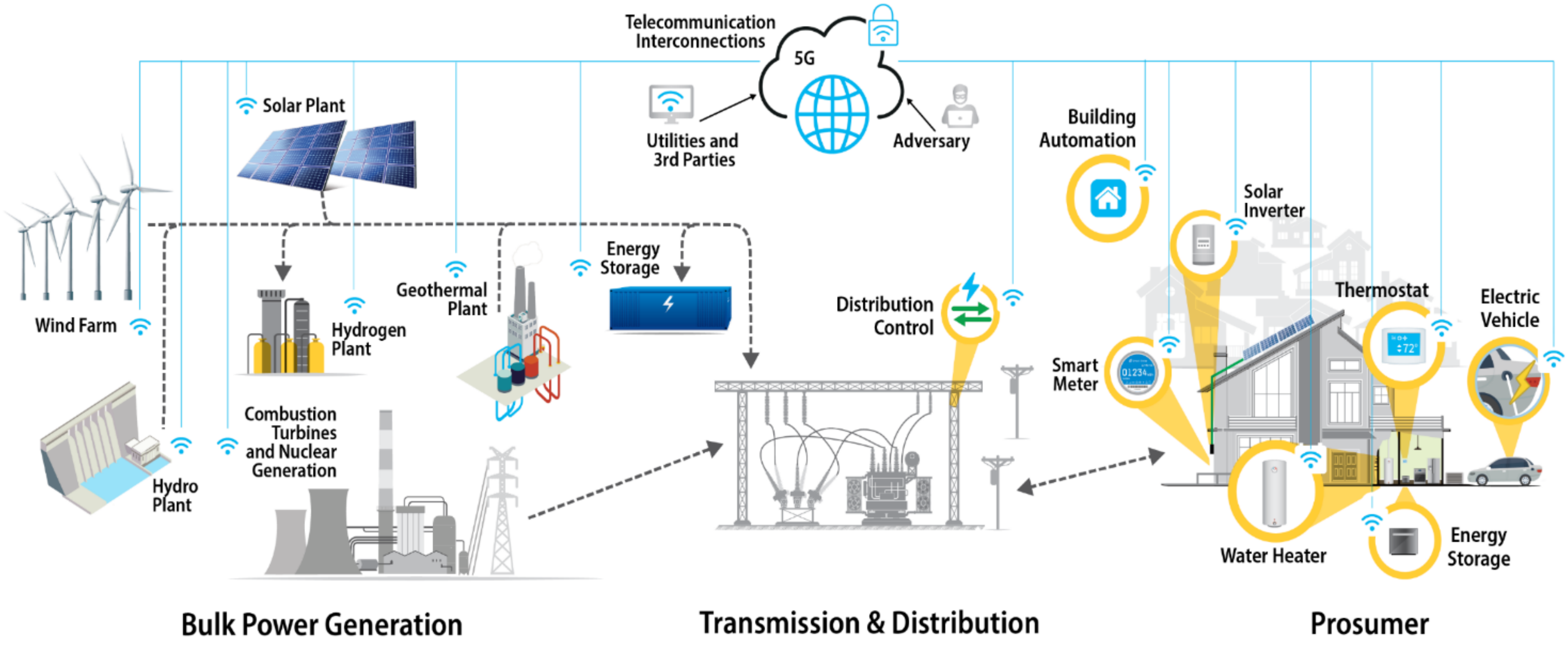
Distributed Energy Resources Cybersecurity Framework

USEA/USAID Supply Chain Cybersecurity

Anuj Sanghvi
Cybersecurity Researcher
NREL

Energy Systems Across the Globe Are Changing

NREL is advancing those future systems—and ensuring the safety, reliability, security, and resilience of those systems.



The grid is changing quickly

Cost-competitive renewables are making up a larger share of the energy mix. The **grid edge** is transforming into a dynamic space where energy isn’t just passively consumed, but **generated,** stored, managed, and traded.

Cybersecurity for Distributed Energy Resources (DERs)

Modern energy systems are increasingly reliant on smaller decentralized generation sources, i.e., DERs such as solar, wind, and storage

- DERs are equipped with complex, data-driven communications networks to connect with the energy grid.
- This growing number of smart devices that support DERs can increase the number of access points outside a utility’s administrative domain, which can increase the potential for cyberattack.

Cybersecurity Assessment for Distributed Energy Resources

- NREL conducted over 30 assessments for utilities across the United States with a cybersecurity assessment tool based on the DOE Cyber Security Capability Maturity Model (C2M2) and the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) and focused on business process.
- With funding from the U.S. Department of Energy (DOE) Office of Renewable Energy and Energy Efficiency Federal Energy Management Program (FEMP), NREL modified the current cyber governance assessment tool to include an assessment process specifically for DERs.

The Distributed Energy Resources Cybersecurity Framework (DER-CF) was developed to help federal agencies mitigate gaps in their cybersecurity posture for distributed energy systems.

Assessing Three Key Areas for Cybersecurity

Governance

Technical Management

Physical Security

Cyber Governance Security Assessment

Domains

- Risk Management
- Asset, Change, and Configuration
- Identity and Access Management
- Threat and Vulnerability Management
- Situational Awareness
- Cybersecurity Architecture
- Incident Response
- External Dependency Management
- Cybersecurity Program Management

Cyber-Physical Technical Management Security Assessment

Domains

- Account Management
  - Authentication, authorization, and accounting
  - Role-based access control
  - Remote access
  - Monitoring and logging
- Configuration Management
  - Change management
  - Access control
  - System settings
  - Cloud security
- Systems/Device Management
  - Software integrity
  - Cryptography
  - System protections

Physical Security Assessment

Domains

- Administration Controls
  - Audits
  - Awareness training
  - System security testing
  - Operational management
  - Security plan
  - Secure data
- Physical Access Controls
  - Perimeter security
  - Building security
  - Lighting
  - Signage
  - Intrusion alarm/motion detector
- Technical Controls
  - Intrusion detection/prevention assets
  - Smart card/keying/badges
  - Sensor system/proximity reader/radio-frequency identification
  - Communication system
  - Closed-circuit television

Cyber Governance Security Assessment

Domains

- Risk Management
- Asset, Change, and Configuration
- Identity and Access Management
- Threat and Vulnerability Management
- Situational Awareness
- Cybersecurity Architecture
- Incident Response
- External Dependency Management
- Cybersecurity Program Management

Cyber-Physical Technical Management Security Assessment

Domains

- Account Management
  - Authentication, authorization, and accounting
  - Role-based access control
  - Remote access
  - Monitoring and logging
- Configuration Management
  - Change management
  - Access control
  - System settings
  - Cloud security
- Systems/Device Management
  - Software integrity
  - Cryptography
  - System protections

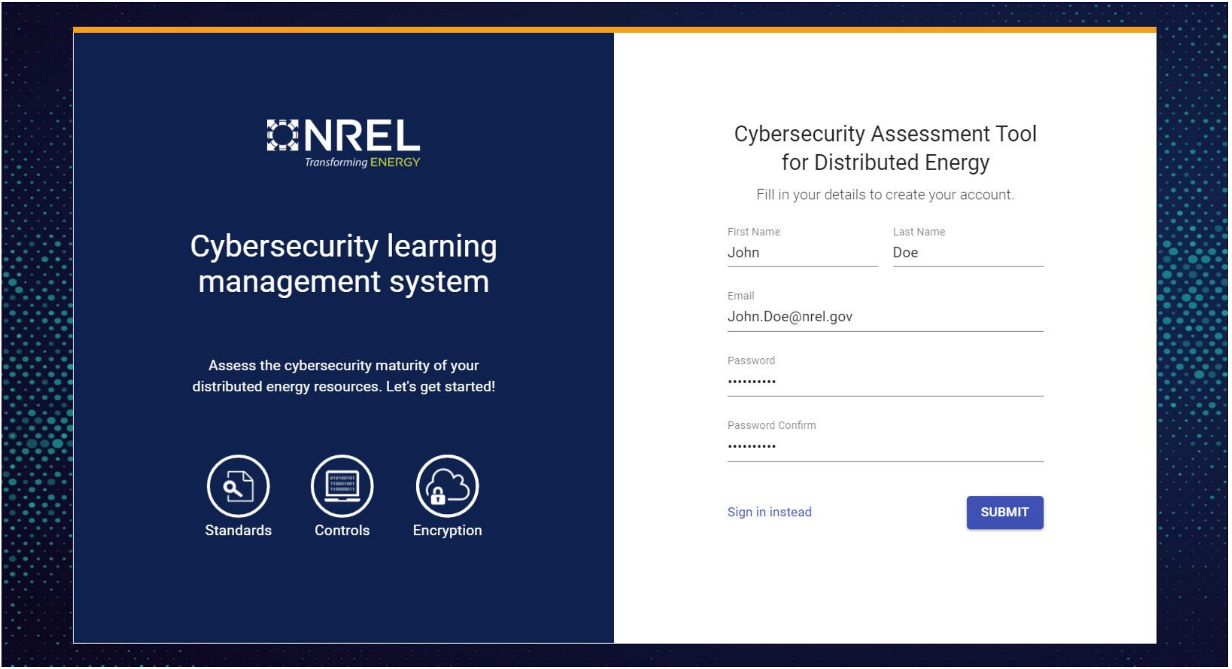
Physical Security Assessment

Domains

- Administration Controls
  - Audits
  - Awareness training
  - System security testing
  - Operational management
  - Security plan
  - Secure data
- Physical Access Controls
  - Perimeter security
  - Building security
  - Lighting
  - Signage
  - Intrusion alarm/motion detector
- Technical Controls
  - Intrusion detection/prevention assets
  - Smart card/keying/badges
  - Sensor system/proximity reader/radio-frequency identification
  - Communication system
  - Closed-circuit television

DERCF Tool: Overview

- Publicly available interactive version of the DERCF framework
- User-focused assessment
- Detailed results and action items
- Userbase: Site operations, energy managers, executive managers
- Tailored assessment to individual site



Cybersecurity learning management system

Assess the cybersecurity maturity of your distributed energy resources. Let's get started!

Cybersecurity Assessment Tool for Distributed Energy

Fill in your details to create your account.

First Name: John

Last Name: Doe

Email: John.Doe@nrel.gov

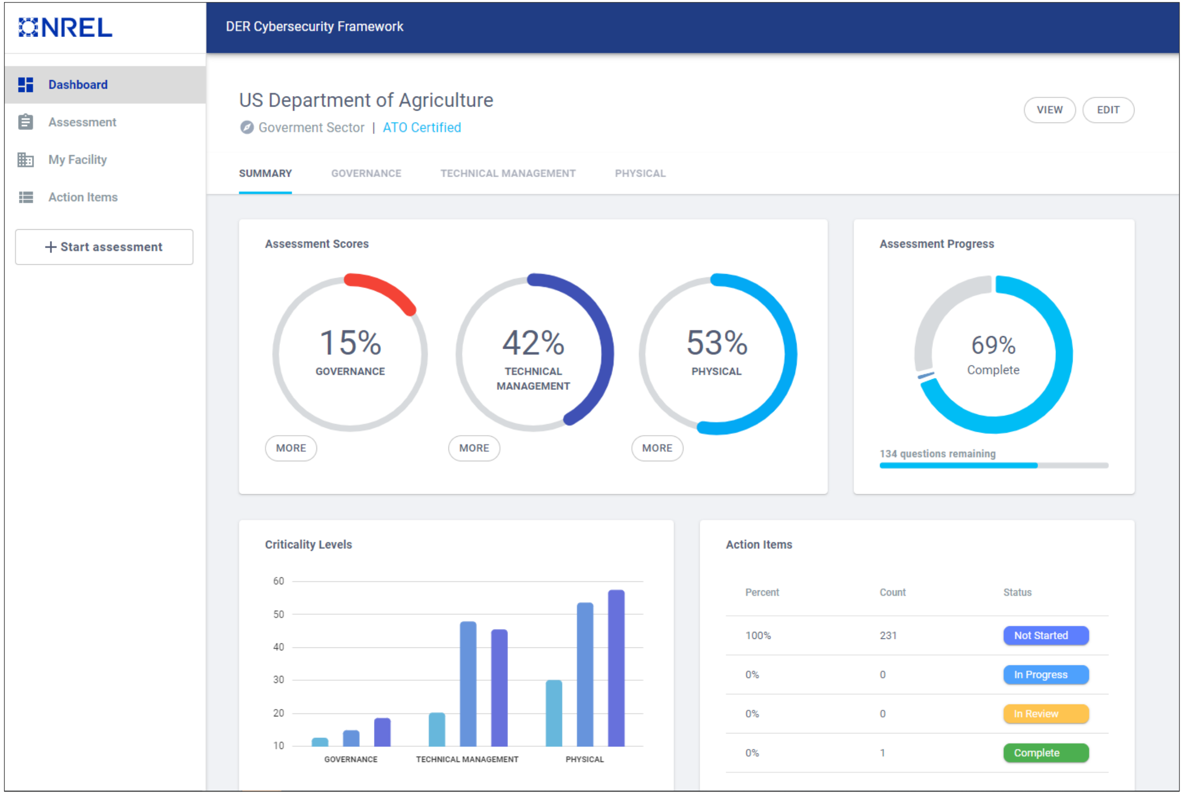
Password: ••••••••••

Password Confirm: ••••••••••

Hosted by NREL at www.dercf.nrel.gov

DERCF Tool: Unique Features

- Dynamic content-driven approach
- Internal-facing application to aid researchers based on user behavior
- User experience focused application, encourages re-use
- Data secured to meet FIPS-199 medium standards



US Department of Agriculture

Goverment Sector | ATO Certified

Percent	Count	Status
100%	231	Not Started
0%	0	In Progress
0%	0	In Review
0%	1	Complete

Third Party Risks

C2M2 Domain: External Dependency Management

Governance – Supply Chain Risks

- Identify and Prioritize Third Parties
- Internal and External Parties for IT and OT
- Dependence to Delivery of the Function
- Document and Manage Third-Party Risks
- Define Triggers – Events, System Changes, etc
- Prioritization of Suppliers, Vendors, and other Third Parties

Technical Management – Supply Chain Risks

- Define Safeguards against Counterfeit or Compromised Software, Hardware, and Services
- Evaluation of Bills of Material for Key Asset Elements
- Third-Party Hosting Environments and Source Data
- System Life-Cycle Management
- Cybersecurity Site Acceptance Testing

References

- NREL’s DER-CF: https://dercf.nrel.gov/
- Power System Cybersecurity Building Blocks: https://resilient-energy.org/cybersecurity-resilience
- USAID/NREL/CARILEC Cybersecurity Webinar Series: https://resilient-energy.org/cybersecurity-resilience/resources/webinars
- Gap Analysis of Supply Chain Cybersecurity for DERs: https://www.nrel.gov/docs/fy23osti/84752.pdf
- Supply Chain Cybersecurity Recommendations for Solar PV: https://www.nrel.gov/docs/fy23osti/87135.pdf

Q&A

Tami.Reynolds@nrel.gov

Anuj.Sanghvi@nrel.gov

www.nrel.gov

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 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.