Cybersecurity and Distributed Energy Resources

July 9, 2020

Housekeeping Items

- Listen through your computer.
  - Please select the “microphone and speakers” button on the right-hand audio pane display.
- Listen by telephone.
  - Please select the “telephone” option in the right-hand display, and a phone number and pin will display.
- Technical difficulties:
  - Contact the GoToWebinar Help Desk: 1-888-259-8414

www.nrel.gov/usaid-partnership

Housekeeping Items

- To ask a question
  - Select the ‘Questions’ pane on your screen and type in your question.
- Share with others or watch it again
  - A video/audio recording of this webinar and the slide decks will be emailed to all attendees shortly after the webinar has concluded.
- Recordings are also available on the USAID-NREL Partnership Learning Channel playlist on YouTube
  - https://www.youtube.com/playlist?list=PLmIn8Hncs7bEWpXMKTzTf3lzlx6kBp2a0

www.nrel.gov/usaid-partnership

The USAID-NREL Partnership

USAID and NREL partner to deliver clean, reliable, and affordable power to the developing world. The USAID-NREL Partnership addresses critical aspects of deploying advanced energy systems in developing countries through:

- Policy, planning, and deployment support.
- Global technical toolkits.

www.nrel.gov/usaid-partnership

Global Technical Platforms

The USAID-NREL Partnership's global technical platforms provide free, state-of-the-art support on common and critical challenges to scaling up advanced energy systems.

www.re-explorer.org

www.greeningthegrid.org

www.i-jedi.org

www.resilient-energy.org

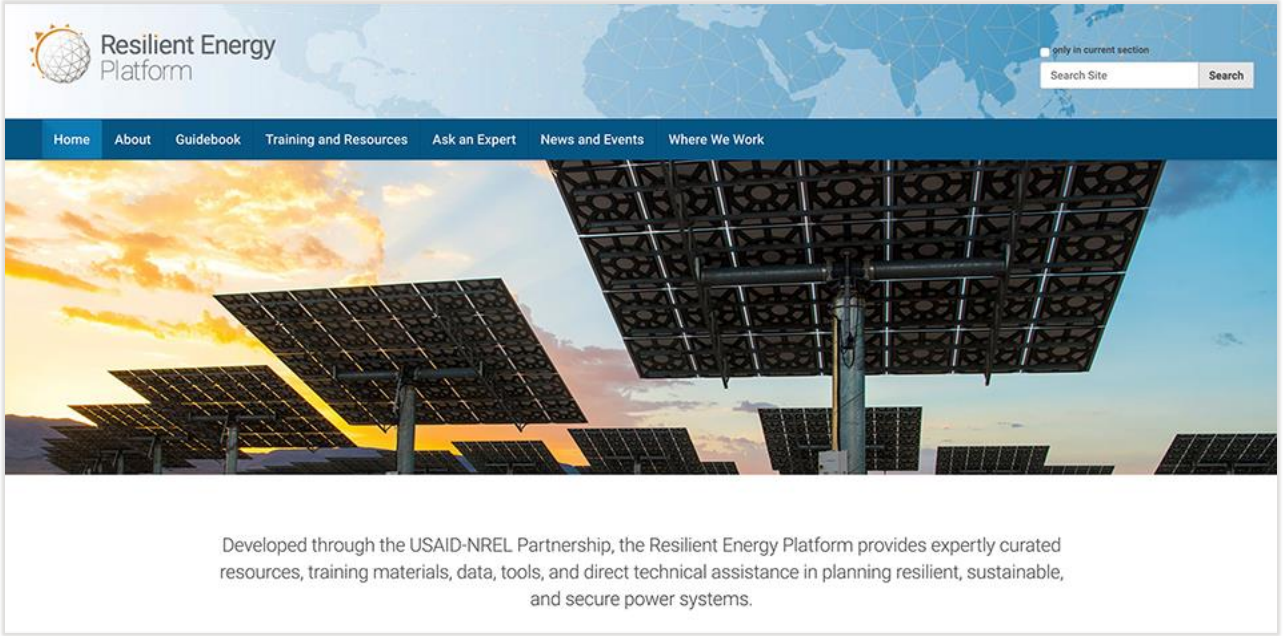
USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Resilient Energy Platform

Developed through the USAID-NREL Partnership, the Resilient Energy Platform provides expertly curated resources, training materials, tools, and technical assistance to enhance power sector resilience.

The platform enables decision makers to assess power sector vulnerabilities, identify resilience solutions, and make informed decisions to enhance power sector resilience at all scales.



www.resilient-energy.org

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Agenda

Opening

Jeremy Foster

Senior Energy Advisor,

USAID

Cybersecurity and Distributed Energy Resources

Maurice Martin

Senior Cybersecurity Research Leader, NREL

Tami Reynolds

Project Manager & Lead for Secure Cyber Energy Systems, NREL

Utility Perspective

Curley Henry

Executive Director, Cyber Security Strategy & Architecture

Southern Company

Q&A

James Elsworth

Research Engineer,

National Renewable Energy Laboratory

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Cybersecurity and Distributed Energy Resources

Maurice Martin

- National Renewable Energy Laboratory
- 12 years technology research for the electric utility industry
- Focus on security architectures for complex systems
- Previous work focused on small and under-resourced utilities and their cybersecurity challenges

Tami Reynolds

- National Renewable Energy Laboratory
- Technical lead on the Distributed Energy Resources Cybersecurity Framework (DERCF)
- Conducts cyber-governance assessments in the electric utility sector based on DOE's C2M2 and the NIST Cybersecurity Framework

Resilient Energy Platform

USAID FROM THE AMERICAN PEOPLE

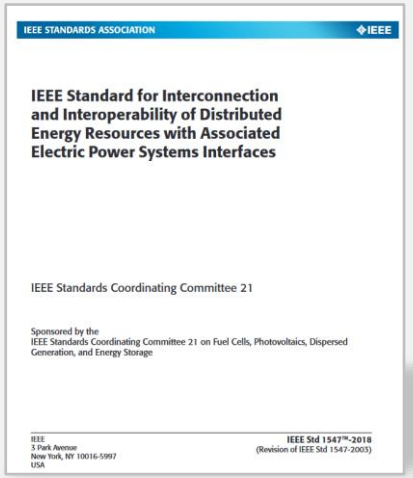
NREL Transforming ENERGY

Distributed Energy Resources (DERs)

Resilient Energy Platform

IEEE 1547-2018

- “A source of electric power that is not directly connected to a bulk power system. DER includes both generators and energy storage technologies capable of exporting active power to an [electric power system].”



Includes:

- Solar
- Wind
- Hydro
- Batteries
- Biogas
- Fossil Fuel

What about controllable loads or demand response?

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

DERs in Developing Countries

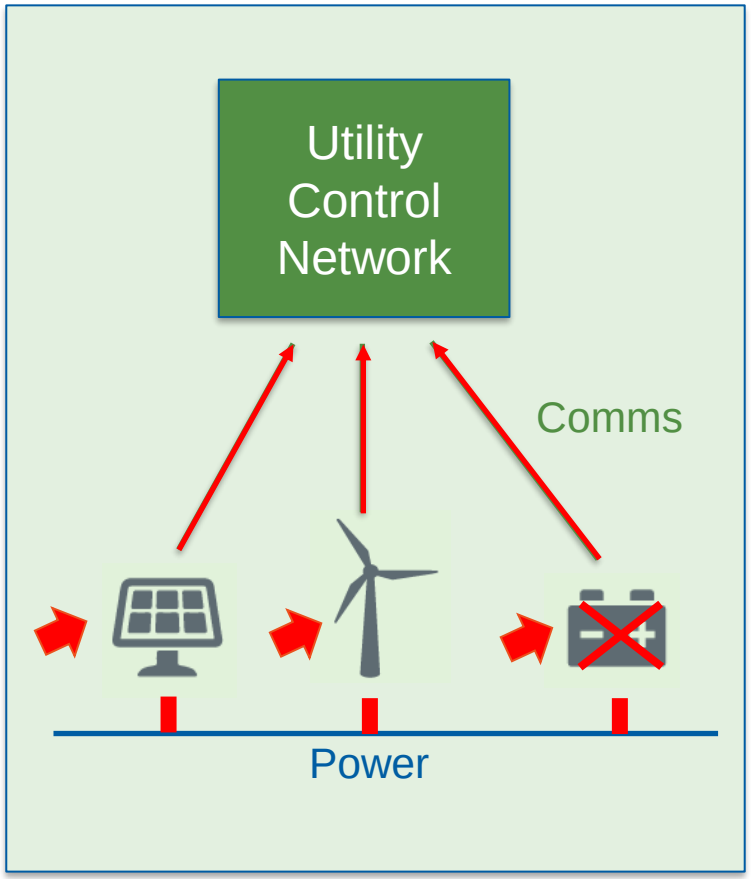
- Isolated rural areas may not have transmission/distribution infrastructure
- Fossil fuel supply may be uncertain
- Fossil fuels may be expensive
- Environmental concerns
- Market growth in Argentina, Costa Rica, Egypt, Indonesia, Kenya, Tanzania, Thailand, Tunisia, and Uruguay

DATA POINT

Kenya leads the world in solar power installations per capita.

Source: Wikipedia

DER Security Concerns



- Increase attack surface
- Mis-operation of resources to disrupt the grid
- Upstream attack
- Damage to equipment

Cyber Incident: Utah

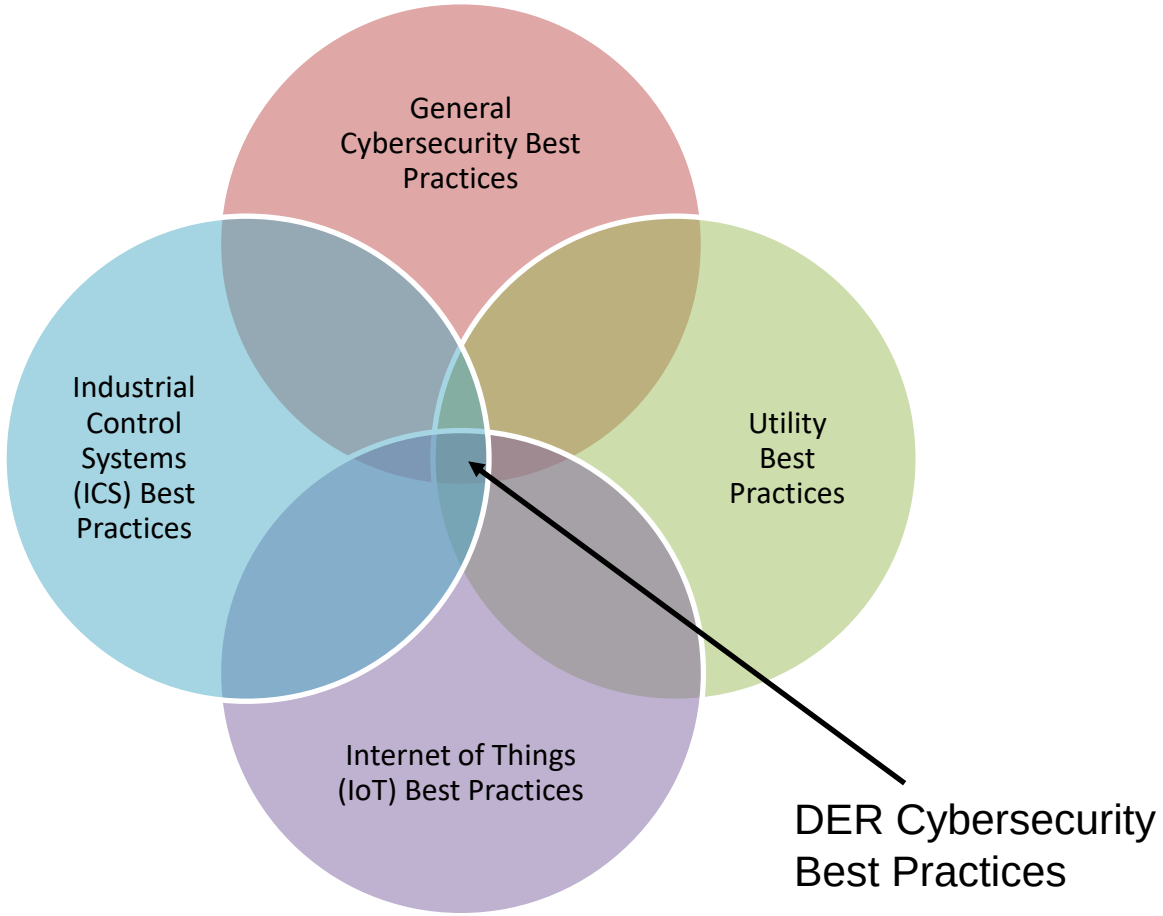
- March 2019: Utah-based renewable energy provider (sPower) hit with a cyber attack
- Lost communication to its power generation installations
- Root cause: unpatched firewall

QUESTION:

Was sPower the intended target? Or were they caught up in an attack on another target (or no target at all)?

Source: ZDNet

DER Cybersecurity: An Intersection of Best Practices

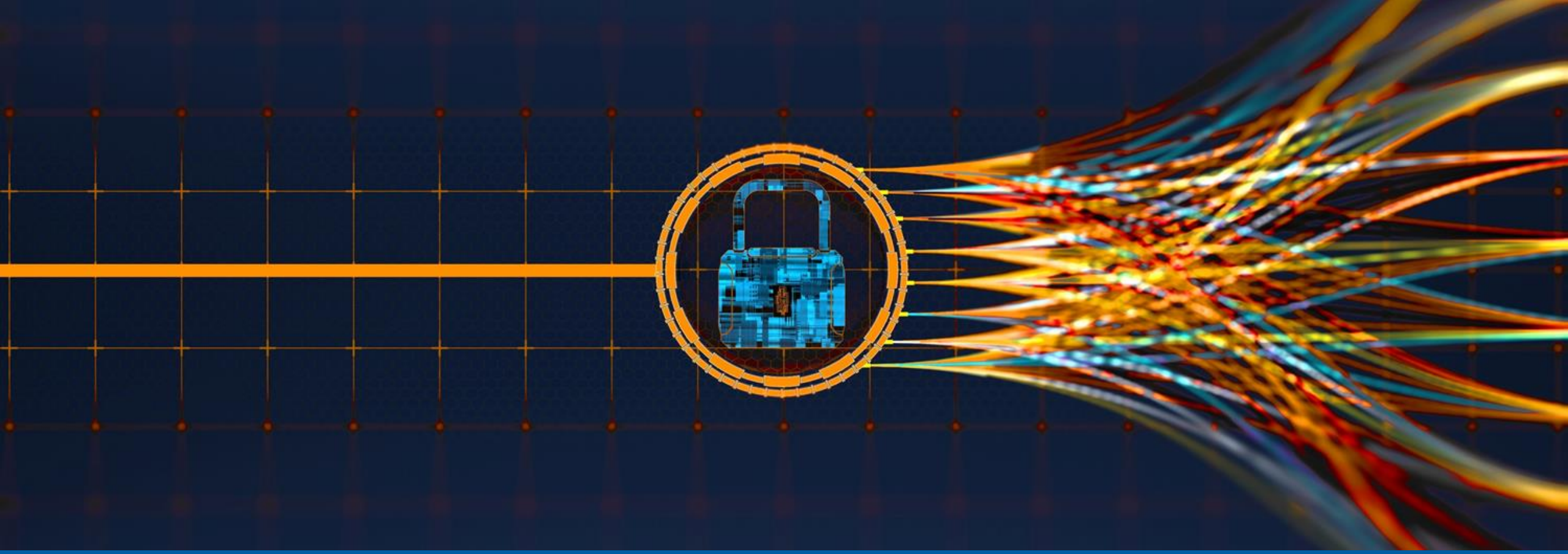


- Utility best practices
- Must also account for distributed nature of DERs…
  - Cyber physical devices
  - Remote locations
  - Unsupervised
  - Weak physical security

Cybersecurity Assessment Research at NREL

- Research has identified cybersecurity vulnerabilities in operational technology components of distributed energy resource (DER) systems, such as PV inverters.
- If hacked, the DER output could be compromised in a way that disrupts the stability of the local distribution system.
- With the prevalence of DER deployed at federal sites, and an ongoing initiative to enhance and ensure energy resilience, the cybersecurity vulnerabilities of DER must be understood and addressed.

The Distributed Energy Resources Cybersecurity Framework (DERCF)



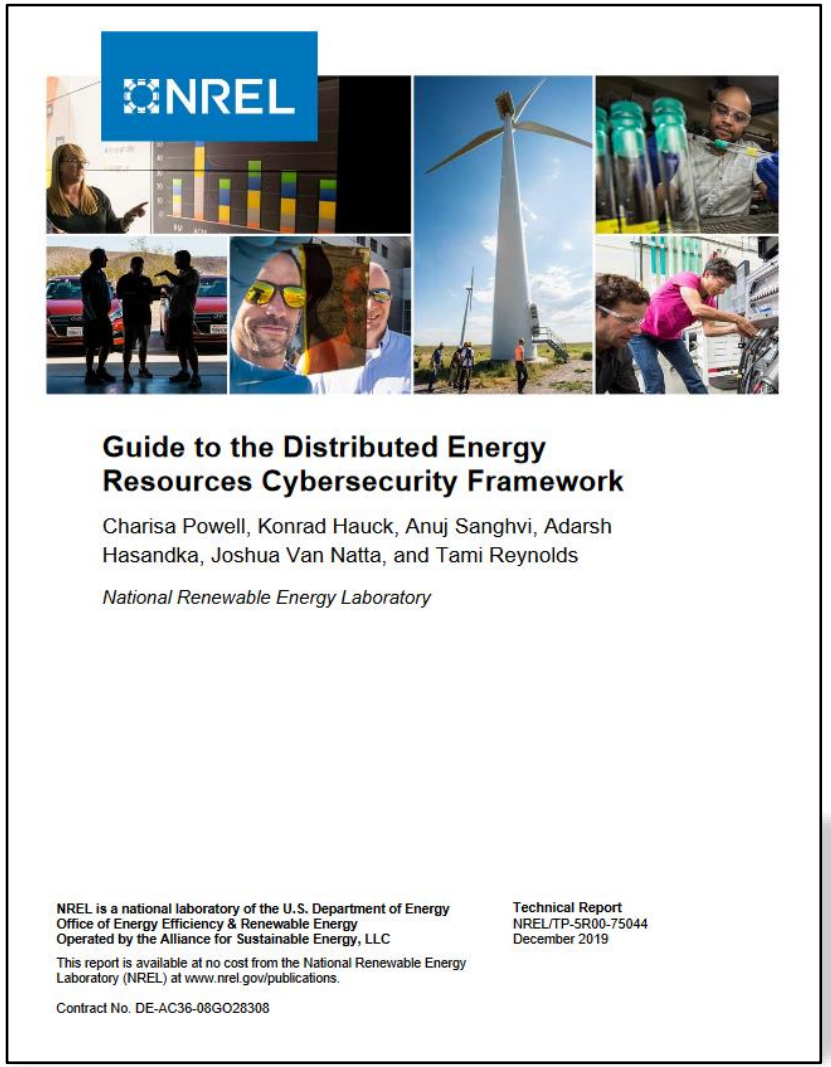
The Distributed Energy Resources Cybersecurity Framework (DERCF) was designed to help U.S. federal government agencies mitigate gaps in their cybersecurity posture for distributed energy systems.

DERCF: Both a Guide and an Online Tool

REexplorer
MAPPING OUR ENERGY FUTURE

Guide:

- PDF, free to download and use
- Core Concepts
- Model Pillars
- Respective Domains
- References
- https://www.nrel.gov/docs/fy20osti/75044.pdf



USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

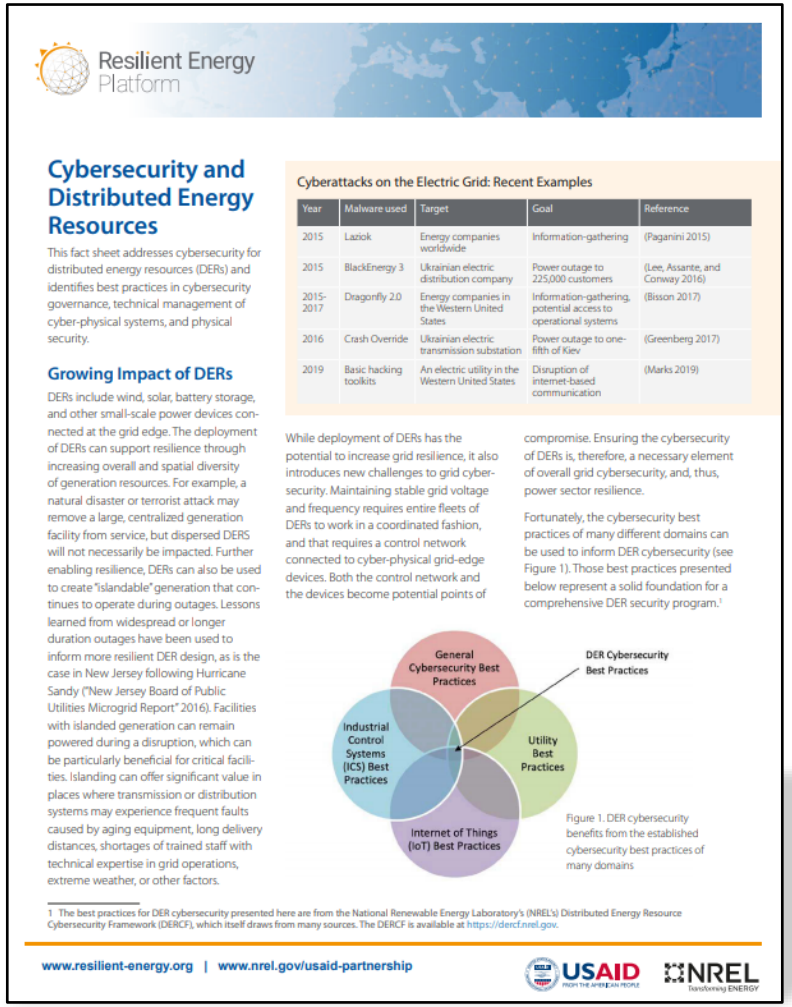
DERCF: Both a Guide and an Online Tool

Online Tool:

- Publicly available interactive version of the DER-CF framework
- Hosted by NREL at www.dercf.nrel.gov
- User-focused assessment
- Detailed results & action items
- Userbase: Site operations, energy managers, executive managers
- Tailor assessment to individual site

Also… a fact sheet!

- PDF, free to download and use
- Quick overview of DER cybersecurity
- English: https://www.nrel.gov/docs/fy20osti/76307.pdf
- Russian: https://www.nrel.gov/docs/fy20osti/76988.pdf



Resilient Energy Platform

Cybersecurity and Distributed Energy Resources

This fact sheet addresses cybersecurity for distributed energy resources (DERs) and identifies best practices in cybersecurity governance, technical management of cyber-physical systems, and physical security.

Growing Impact of DERs

DERs include wind, solar, battery storage, and other small-scale power devices connected at the grid edge. The deployment of DERs can support resilience through increasing overall and spatial diversity of generation resources. For example, a natural disaster or terrorist attack may remove a large, centralized generation facility from service, but dispersed DERS will not necessarily be impacted. Further enabling resilience, DERs can also be used to create "islandable" generation that continues to operate during outages. Lessons learned from widespread or longer duration outages have been used to inform more resilient DER design, as is the case in New Jersey following Hurricane Sandy ("New Jersey Board of Public Utilities Microgrid Report" 2016). Facilities with islanded generation can remain powered during a disruption, which can be particularly beneficial for critical facilities. Islanding can offer significant value in places where transmission or distribution systems may experience frequent faults caused by aging equipment, long delivery distances, shortages of trained staff with technical expertise in grid operations, extreme weather, or other factors.

Cyberattacks on the Electric Grid: Recent Examples

Year	Malware used	Target	Goal	Reference
2015	Laziok	Energy companies worldwide	Information-gathering	(Paganini 2015)
2015	BlackEnergy 3	Ukrainian electric distribution company	Power outage to 225,000 customers	(Lee, Assante, and Conway 2016)
2015-2017	Dragonfly 2.0	Energy companies in the Western United States	Information-gathering, potential access to operational systems	(Bisson 2017)
2016	Crash Override	Ukrainian electric transmission substation	Power outage to one-fifth of Kiev	(Greenberg 2017)
2019	Basic hacking toolkits	An electric utility in the Western United States	Disruption of internet-based communication	(Marks 2019)

While deployment of DERs has the potential to increase grid resilience, it also introduces new challenges to grid cybersecurity. Maintaining stable grid voltage and frequency requires entire fleets of DERs to work in a coordinated fashion, and that requires a control network connected to cyber-physical grid-edge devices. Both the control network and the devices become potential points of compromise. Ensuring the cybersecurity of DERs is, therefore, a necessary element of overall grid cybersecurity, and, thus, power sector resilience.

Fortunately, the cybersecurity best practices of many different domains can be used to inform DER cybersecurity (see Figure 1). Those best practices presented below represent a solid foundation for a comprehensive DER security program.[1]

Figure 1. DER cybersecurity benefits from the established cybersecurity best practices of many domains

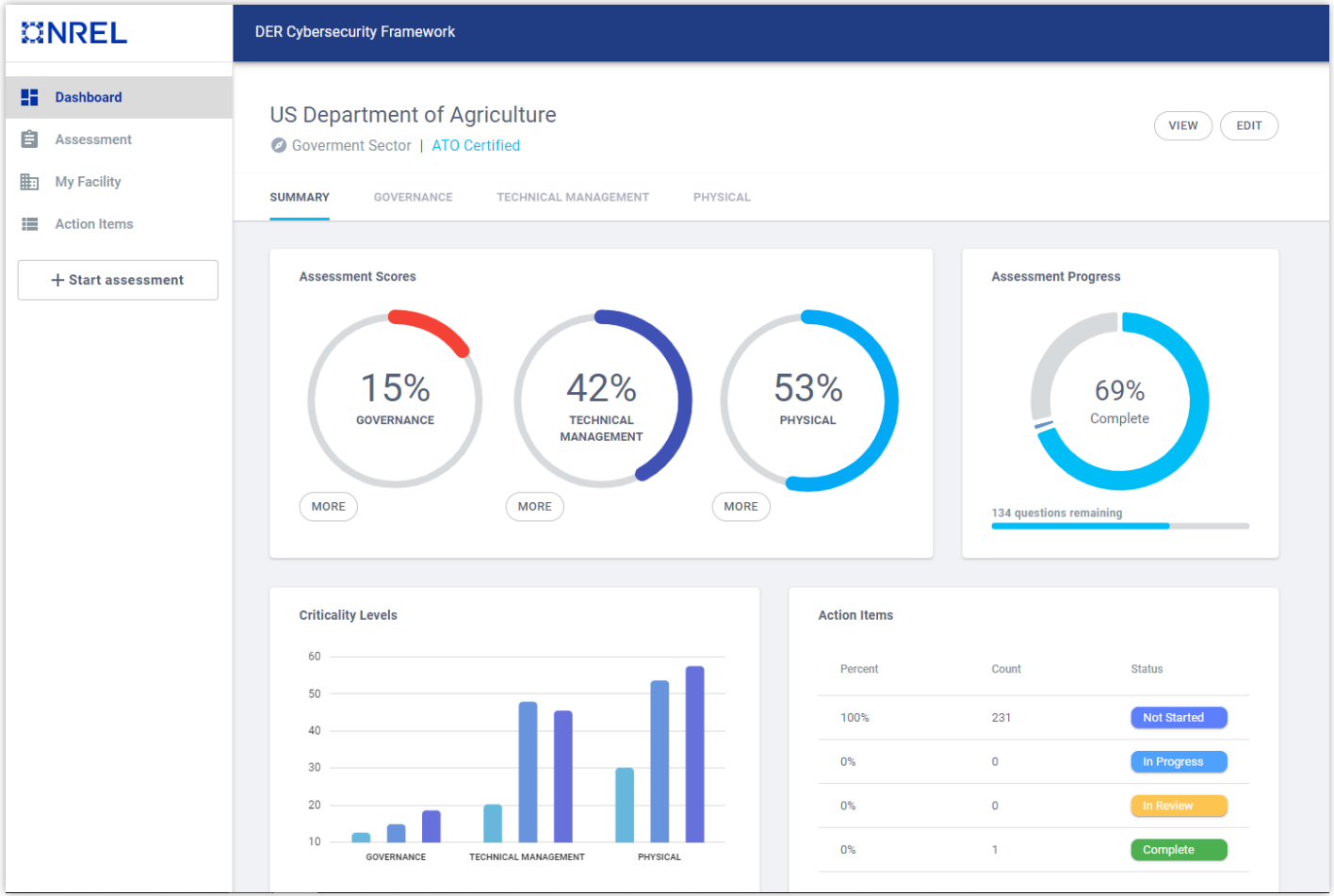
1 The best practices for DER cybersecurity presented here are from the National Renewable Energy Laboratory's (NREL's) Distributed Energy Resource Cybersecurity Framework (DERCF), which itself draws from many sources. The DERCF is available at https://dercf.nrel.gov.

www.resilient-energy.org | www.nrel.gov/usaid-partnership

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

DERCF Tool: Unique Features



- Dynamic content-driven approach
- Updated with evolution of research
- 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

Key Areas for DER Cybersecurity

Governance

Technical Management

Physical Security

Cyber Governance Security Assessment	Cyber-Physical Technical Management Security Assessment	Physical Security Assessment
Domains:	Domains:	Domains:
✓ • Risk Management • Asset, Change, and Configuration • Identity and Access Management ✓ • Threat and Vulnerability Management • Situational Awareness ✓ • Information Sharing and Communication Management ✓ • Incident Response • External Dependency Management ✓ • Cybersecurity Program Management	• Account Management *Role-based access control* *Anomalous behavior in system logs* • Configuration Management *Access restrictions* *Configuration settings* *Configuration change control* *Internal/external user management* • Systems/Device Management *Fail-safe procedures* *Ports and input/output device access* *Cryptographic protection* *Software integrity/patch management*	• Administration Controls *Audits* *Holistic security/contingency planning* *Personnel security planning* • Asset Controls *Equipment* *Maintenance* • Structure Controls *Distancing practices for sensitive assets* *Intrusion detection/prevention assets* *Response teams/force protection*

Example 1: Governance

Resilient Energy Platform

Cyber Governance Security Assessment

Domains:

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

Asset, Change, and Configuration Management

- What devices are on your system?
- What software is running on your system? (Which version on which device?)
- How are these devices/systems configured?
- How to you test changes to the system?
- How do you track changes in the system as new devices and software is added?

If you don't know what you have, you can't protect it.

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Example 2: Technical Management

Resilient Energy Platform

Cyber-Physical Technical Management Security Assessment

Domains:

- Account Management
  - *Role-based access control*
  - *Anomalous behavior in system logs*
- Configuration Management
  - *Access restrictions*
  - *Configuration settings*
  - *Configuration change control*
  - *Internal/external user management*
- Systems/Device Management
  - *Fail-safe procedures*
  - *Ports and input/output device access*
  - *Cryptographic protection*
  - *Software integrity/patch management*

Account Management

- Provisioning
- Role-based access
- Enforcing least privilege
- Preventing access “creep”
- Revoking access

How do you implement your security plan?

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Example 3: Physical Security

Domains:

- Administration Controls
  - *Audits*
  - *Holistic security/contingency planning*
  - *Personnel security planning*
- Asset Controls
  - *Equipment*
  - *Maintenance*
- Structure Controls
  - *Distancing practices for sensitive assets*
  - *Intrusion detection/prevention assets*
  - *Response teams/force protection*

Administrative Controls

- Procedures and policies
- Personnel security
- Contingency planning
- Auditing (internal)
- Planning physical security (based on risk)

How do you secure devices that are attached to houses, poles, offices, or other public structures?

Summary

- The DERCF is a holistic tool for evaluating cybersecurity posture of sites with DER systems.
- Networked grid devices are now being controlled by consumers or third parties who are not fully aware of the need for cybersecurity.
- The DERCF offers a sharper focus on distributed energy technologies – and greater emphasis on physical security and technical management.
- Users will access DERCF-guided assessments through a web-based application or a downloadable document, which presents users with questions about security controls and practices that relate to their use of DERs.
- The DERCF web application tool will generate a score from the user's responses that indicates their current state of DER cybersecurity – and how they can improve.

Resources

DERCF draws on the following standards and/or frameworks:

- **DOE Cyber Security Capability Maturity Model (C2M2)**
- **Security and Privacy Controls:** NIST 800-53,
- **Conducting Risk Assessments:** NIST 800-30
- **Industrial Control System Security:** NIST 800-82
- **NIST Cybersecurity Framework**
- **North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)**
- **Power Systems data and comms security:** International Electrotechnical Commission (IEC) 62351

Southern Company

Resilient Energy Platform

Managing Risk Related to New Distribution Energy Resources

Curley Henry
Executive Director
Southern Company Services

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Agenda

Resilient Energy Platform

01 Background

02 Cybersecurity Approach

03 Cybersecurity Characteristics & Risks

04 Cybersecurity Considerations

05 Q&A

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Background

Why DER?

Resilient Energy Platform

Expanding the Business
- Resiliency
- Energy services
- Renewables

Leverage C&I Relationships
- New products and services

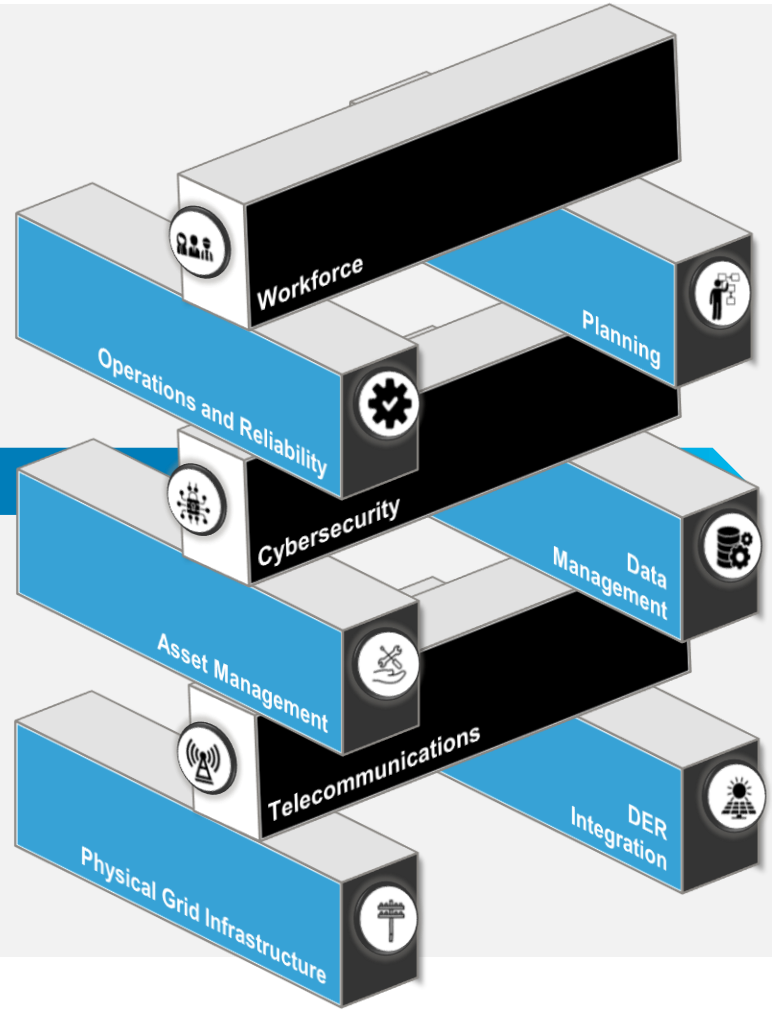
Technological Imperatives
- “Low-to-no carbon”
- Retire coal
- Build renewables, DER
- Carbon capture
- Storage

Reduce O&M
- Improve efficiencies
- Organizationally align

Regulated Capital
- Resiliency
- Grid Modernization
- Electrification

Regulator Innovation
- Rate design
- Regulatory entrepreneurship

Digitalization
- Technological efficiencies
- Big data
- Customer experience



USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Cybersecurity Approach

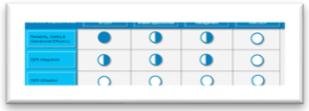
Technical Roadmap

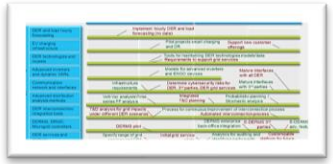
Resilient Energy Platform

Distribution System Platform (DSPx) Model

- Objectives — What do we want to accomplish?
- Capabilities — What capabilities do we need to do so?
- Functions — How do we develop those capabilities?
- Elements — Building blocks
- System Requirements — Implementation

Technology Roadmap

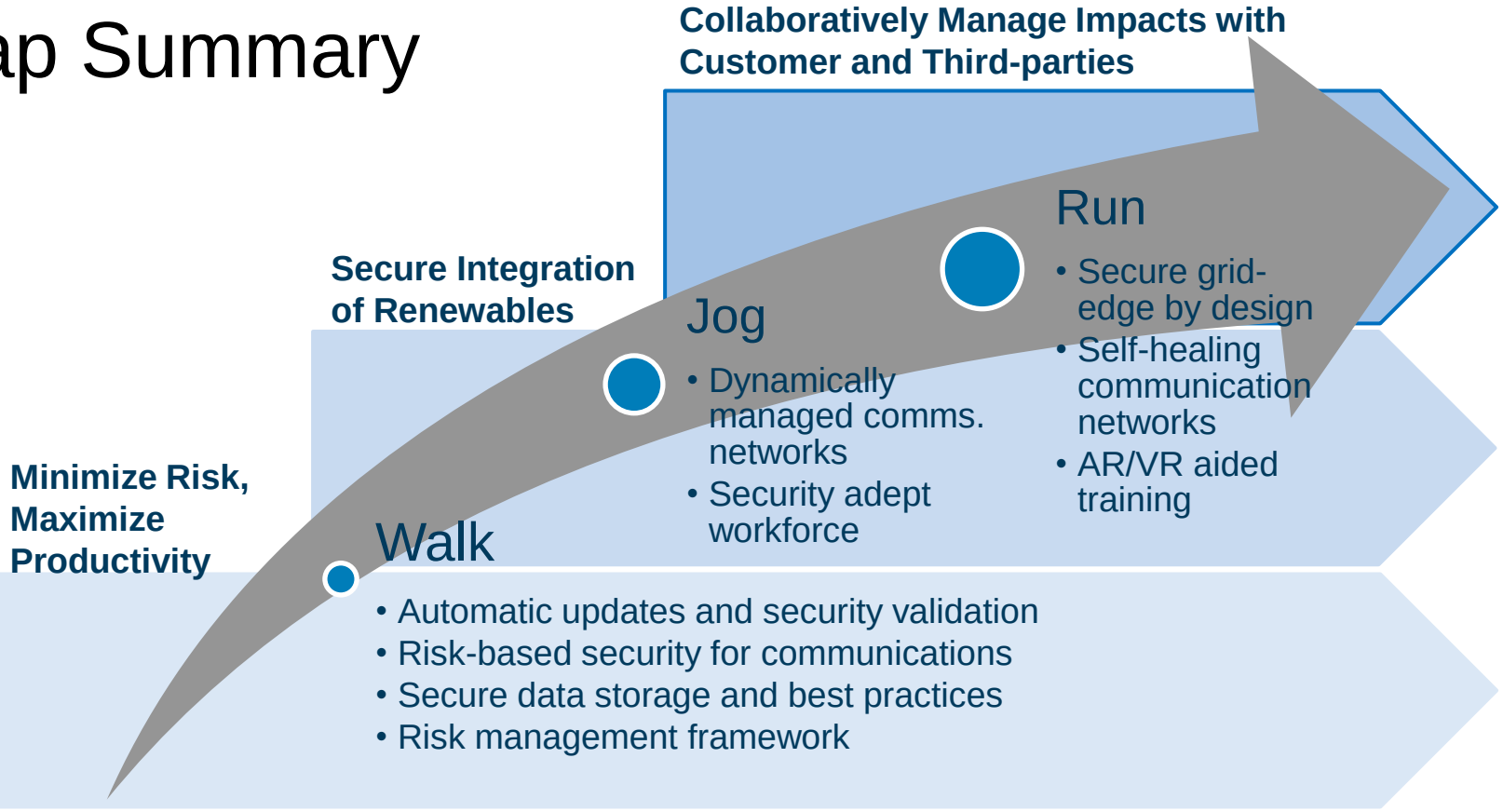





USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Roadmap Summary



* Walk, jog, run as defined by DSPx nomenclature

High Level Future States

Agile corporate decision making	Autonomous devices	Experienced & innovative workforce	Large-scale data management	Pervasive monitoring and controls

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Cybersecurity Characteristics and Risks

Cybersecurity Risk to the Distributed Grid

Resilient Energy Platform

Increased Cybersecurity Risk to the Distribution Grid

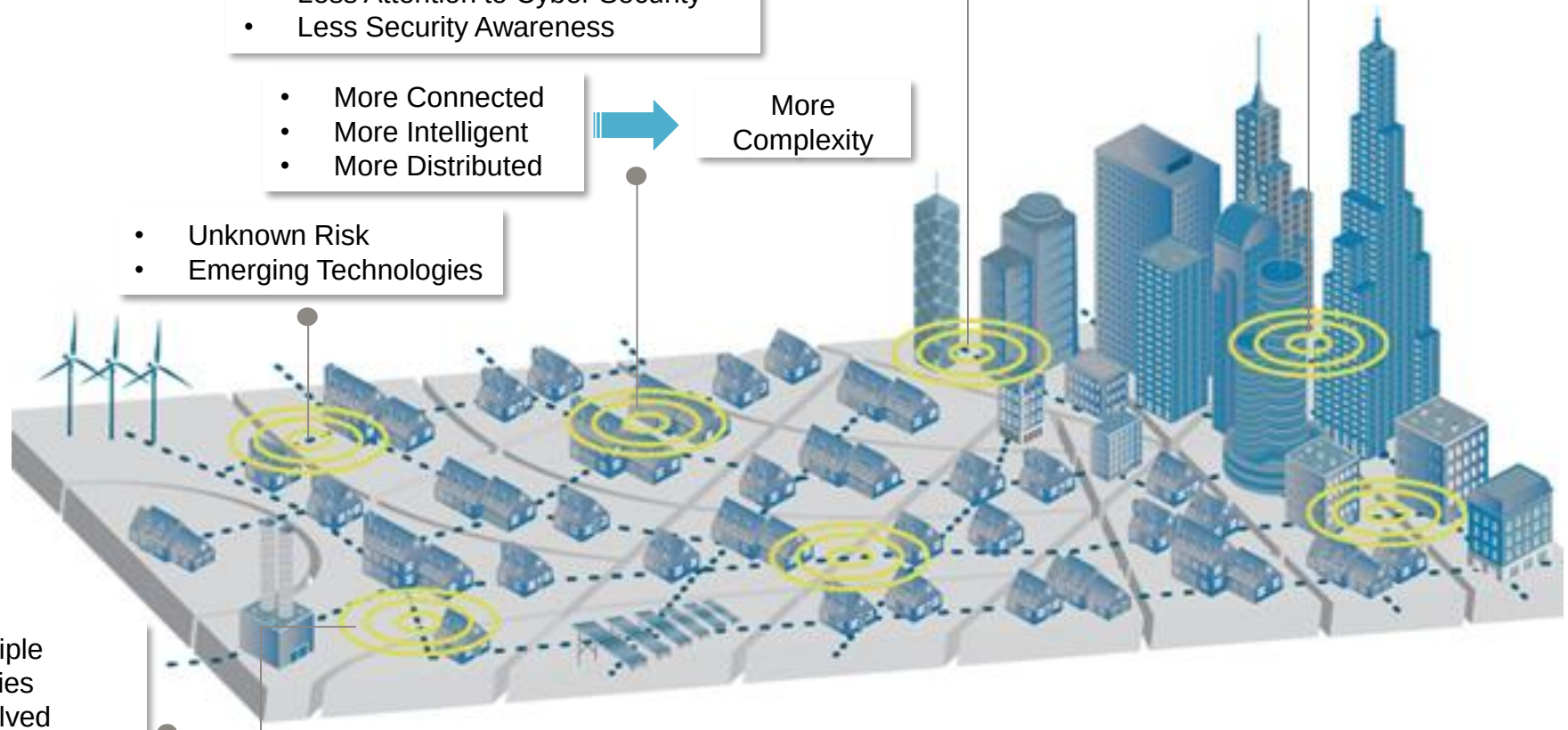
- No Mandatory Standards
- Less Attention to Cyber Security
- Less Security Awareness

More Reported Attacks

- More Connected
- More Intelligent
- More Distributed

More Complexity

- Unknown Risk
- Emerging Technologies



- Multiple Parties Involved
- Less Central Control

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Cybersecurity Characteristics & Risks

Resilient Energy Platform

Characteristics

Agile Corporate Decision-Making	Autonomous Devices	Experienced, Innovative Workforce	Large-scale Data Management	Pervasive Monitoring & Communications

Future State

- Decision makers tools to accurately & rapidly assess security risks
- Risk-based security for communication protection
- Strategic segmentation & isolation of communication network
- Self-healing communication network
- Security integration into operation and maintenance manuals
- AR/VR aided security training, incident response, and digital restoration
- Security training to OT personnel
- OT training for IT security personnel
- Clear common set of privacy regulations that are applicable to the majority of states
- Secure data storage and processing
- Effective anonymization / tokenization of data
- Devices are secure out-of-box
- Secure managed continuous automatic updates to software/firmware with in-time security validation
- Autonomous reporting and recovery

Risks

Attack Vectors

Comprisable Devices

Data Integrity, Privacy Risk, Liability

Insider Threat

IT/OT Integration

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Cybersecurity Considerations

Cybersecurity Considerations

Recommendations

- Evaluate current risk management process to ensure cybersecurity risk is appropriately reported
- Investigate ways to quantify security risks and operational performance to forecast the cyber investment in a long-term

External engagement with regulators and industry groups to influence emerging cybersecurity standards (i.e., IEEE 1547.3, NIST, IEC, …

- Ensure cyber security concerns are addressed at the strategic level
- Develop incident response plan for grid-edge systems (DER, DR, connected loads)

Summary

Summary

- **Cybersecurity delivers the following three strategic objectives:**
  - Minimize cybersecurity risks while maintaining productivity
  - Secure integration of clean energy resources
  - Manage impacts of cyber threats collaboratively with customers and 3rd parties
- **Key actions:**
  - Develop and socialize the risk management framework
  - Work with vendors and industry towards grid-edge security vision
  - Implement communication monitoring and assessment technologies for dynamic cybersecurity management
  - Develop data storage strategy to meet cybersecurity CIA triad (confidentiality, integrity, availability)
- **Processes and retraining personnel will be required:**
  - Work collaboratively with the industry on cybersecurity standards and best practices
  - Cybersecurity training for OT personnel and OT training for IT security personnel
  - Incident report processes incorporating customer and 3rd parties

Resilient Energy Platform

Questions & Answers

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Next Webinar in this Series

July 16 @ 11 a.m. U.S. EDT (1500 GMT)

- **The Corporate Culture and Importance of Cyber Hygiene**

More to be announced!

Register and check for updates at
https://usea.org/events

How to Stay In Touch

- Follow NREL on:
  - LinkedIn - National Renewable Energy Laboratory
  - Twitter - @NREL

- Join the USAID-NREL Partnership mailing list at:
  - https://www.nrel.gov/usaid-partnership/newsletter.html

www.nrel.gov/usaid-partnership

Thank you!

This work was authored, in part, by the National Renewable Energy Laboratory (NREL), 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 United States Agency for International Development (USAID) under Contract No. IAG-17-2050. The views expressed in this report do not necessarily represent the views of the DOE or the U.S. Government, or any agency thereof, including USAID. 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.