Distributed Energy Resources Cybersecurity Report and Threat Briefing

November 7, 2022

U.S. DEPARTMENT OF ENERGY

Housekeeping

Technical issues?

If you have technical issues, please put them in the chat box for the host.

Optimal Viewing:

Distributed Energy Resources Cybersecurity Report and Threat Briefing

November 7, 2022

U.S. DEPARTMENT OF ENERGY

Nov 7, 2022

Meg Egan
Control Systems Cybersecurity Analyst
Megan.egan@inl.gov

Cyber Threats to Renewable and Distributed Energy Technologies

INL is managed by Battelle Energy Alliance
for the US Department of Energy

Idaho National Laboratory

INL/CON-22-69152

Renewable Energy Cyber Incidents

- 2014: **SolarWorld AG:** Chinese cyber espionage for economic advantage
- March 5, 2019: **sPower:** Denial-of-service attack
- Feb. – April 2020: **Azerbaijani wind turbines:** PoetRAT malware
- April 18, 2020: **EDP Renewables:** Ransomware
- June 2021: **Invenergy:** REvil ransomware
- August 2021: **ERG:** LockBit 2.0 ransomware
- Sep. 2021: **Swedish renewable manager**: LockBit 2.0 ransomware
- Nov 19, 2021: **Vestas:** LockBit 2.0 ransomware
- Feb. 24, 2022: **Enercon:** Russian state-sponsored SATCOM attack
- March 31, 2022: **Nordex Group:** Conti ransomware
- April 11, 2022: **Deutsche Windtechnik:** Ransomware
- April – June 2022: **South China Sea wind turbines:** Chinese ScanBox malware
- August 28, 2022: **GSA:** BlackCat ransomware

Current Adversary Capabilities

- Russia:
  - "Particularly focused on improving its ability to target critical infrastructure including ICS"
  - Utilizing cyber as a foreign policy lever, including as deterrence and as a military tactic

- China:
  - "Almost certainly capable of launching cyber attacks to disrupt critical infrastructure services"
  - Broad, persistent espionage threat

Current Adversary Capabilities

- Iran:
  - “Opportunistic approach to cyber attacks makes critical infrastructure owners susceptible to being targeted”
  - Successful targeting in Israel reflects growing willingness to take risks

- Criminal Actors:
  - “Innovating targeting to focus on victims whose business operations lack resilience or whose customers cannot sustain service disruptions, driving ransomware payouts up”

Recent Incidents

- March 5, 2019: Utah renewable energy company sPower intermittently lost communications with solar and wind installations due to a denial-of-service attack
  - Unidentified attackers exploited a known vulnerability in a Cisco firewall
  - Disabled communications with a dozen generation sites in five-minute intervals over several hours
  - Did not impact control systems, power generation
- Lesson: Publicly known vulnerabilities can be exploited within hours to days if internet-exposed by unsophisticated or state-sponsored actors

S·POWER
SUSTAINABLE POWER GROUP

Recent Incidents

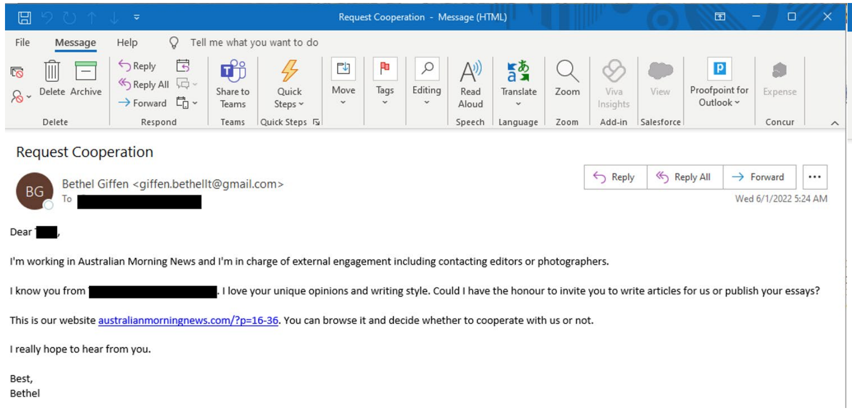
- March 31, 2022: Nordex Group, a major wind turbine manufacturer, hit by Conti ransomware
- April 11, 2022: Deutsche Windtechnik, a wind turbine maintenance company, hit by ransomware

NORDEX Deutsche Windtechnik

- Both companies lost remote connectivity to monitor health and operations of turbines
  - Assets remained operational and were not damaged
- Lesson: Widespread ecosystem of trusted partners provides many access vectors; entire network is as secure as its least secure partner

Recent Incidents

- April – June 2022: TA423, a China-based cyber threat group, targets vendor, installation, and maintenance companies for offshore wind turbines in the South China Sea
  - Began with phishing e-mails, delivered ScanBox malware
- Lesson: Entire supply chain of renewables targeted; Reconnaissance/espionage is a first step to various follow-on activities



Request Cooperation - Message (HTML)

Request Cooperation

Bethel Giffen <giffen.bethellt@gmail.com>
To [redacted]
Wed 6/1/2022 5:24 AM

Dear [redacted],

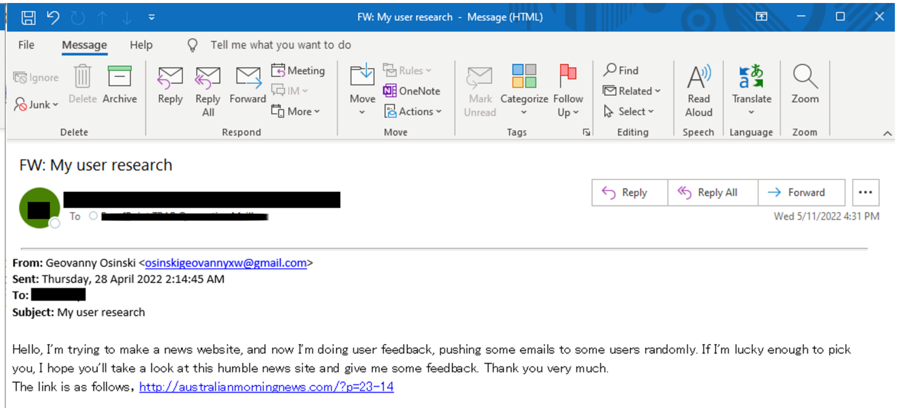
I'm working in Australian Morning News and I'm in charge of external engagement including contacting editors or photographers.

I know you from [redacted]. I love your unique opinions and writing style. Could I have the honour to invite you to write articles for us or publish your essays?

This is our website australianmorningnews.com/?p=16-36. You can browse it and decide whether to cooperate with us or not.

I really hope to hear from you.

Best,
Bethel



FW: My user research - Message (HTML)

FW: My user research

[redacted]
To [redacted]
Wed 5/11/2022 4:31 PM

From: Geovanny Osinski <osinskigeovannyxw@gmail.com>
Sent: Thursday, 28 April 2022 2:14:45 AM
To: [redacted]
Subject: My user research

Hello, I'm trying to make a news website, and now I'm doing user feedback, pushing some emails to some users randomly. If I'm lucky enough to pick you, I hope you'll take a look at this humble news site and give me some feedback. Thank you very much.
The link is as follows, http://australianmorningnews.com/?p=23-14

Phishing e-mails from TA423. Source: Proofpoint

Recent Incidents

- February 24, 2022: Enercon wind turbines in Germany lose remote monitoring connection from Russian SATCOM attack
  - Required replacement of modems at 5800 turbines
  - Spillover effect from Russian attack on Ukrainian command and control communications during invasion

- Lesson: Attacks at scale in both breadth and impact are possible
- Lesson: Mass recovery efforts are more difficult with distributed, offshore assets

Current and Future Security Considerations

- Remote and distributed nature of renewable energy assets emphasizes requirements for secure communications
  - Maintenance generally organized and directed from a remote control center, many trusted partners
- DERs for specific critical facilities can be targeted individually
- Physical damage to renewables may be less concerning for human safety than in other industries
- Individually, renewables pose little threat to owner/operator and grid but collectively, impact is far larger – networks generally widespread
- Efficiency is critical – possible to disrupt in a cyber incident
- Renewables in grid-forming mode – reliability will become increasingly important

Sources

- “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage”. U.S. Department of Justice. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor
- S. Lyngaas. “Utah renewables company was hit by rare cyberattack in March”. CyberScoop. https://www.cyberscoop.com/spower-power-grid-cyberattack-foia/
- W. Mercer. “PoetRAT: Python RAT uses COVID-19 lures to target Azerbaijan public and private sectors”. Cisco Talos. https://blog.talosintelligence.com/poetrat-covid-19-lures/
- “Cyber attack on Deutsche Windtechnik“. Deutsche Windtechnik. https://www.deutsche-windtechnik.com/press-information/item/463-Cyber-attack-on-Deutsche-Windtechnik
- C. Stupp. ”European Wind-Energy Sector Hit in Wave of Hacks”. Wall Street Journal. https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000
- “Update on cyber security incident”. Nordex. https://www.nordex-online.com/en/2022/04/update-on-cyber-security-incident/
- “General notification from Vestas Wind Systems A/S”. Vestas. https://www.vestas.com/en/pages/personal-data-notification
- J. Guerrero-Saade. “Acid Rain | A Modern Wiper Rains Down on Europe”. Sentinel Labs. https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
- “KA-SAT Network cyber attack overview”. Viasat. https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/
- “Over 95 per cent of WECs back online following disruption to satellite communication”. Enercon. https://www.enercon.de/en/news/news-detail/cc_news/show/News/over-95-per-cent-of-wecs-back-online-following-disruption-to-satellite-communication/
- M. Culler et al. “Cybersecurity Guide for Distributed Wind”. INL. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_52997.pdf
- A. Sanghvi et al. “Roadmap for Wind Cybersecurity”. DOE EERE. https://www.energy.gov/sites/prod/files/2020/08/f77/wind-energy-cybersecurity-roadmap-2020v3.pdf
- “Taking remote control: a day in the life of US wind operations”. BP. https://www.bp.com/en/global/corporate/news-and-insights/reimagining-energy/houstons-wind-remote-operations-centre.html
- D. Kominek. “Case Study: Using OPC Software To Operate Wind Farms in Spain”. Renewable Energy World. https://www.renewableenergyworld.com/om/case-study-using-opc-software-to-operate-wind-farms-in-spain/
- H. Toren. “LightsOn: Remote Wind Energy SCADA Control System”. Electric Energy Online. https://electricenergyonline.com/energy/magazine/548/article/LightsOn-Remote-Wind-Energy-SCADA-Control-System.htm
- M. Raggi and S. Scenarelli. “Rising Tide: Chasing the Currents of Espionage in the South China Sea.” Proofpoint. https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea
- “J. Staggs. “Adventures in Attacking Wind Farm Control Networks”. BlackHat USA 2017. https://www.blackhat.com/docs/us-17/wednesday/us-17-Staggs-Adventures-In-Attacking-Wind-Farm-Control-Networks.pdf
- “Wind Energy Technologies Office. “Wind Turbines Can Stabilize the Grid”. DOE. https://www.energy.gov/eere/wind/articles/wind-turbines-can-stabilize-grid

For More Information:

Meg Egan
Control Systems Cybersecurity Analyst
MEGAN.EGAN@INL.GOV

Jake P. Gentle
Program Manager
JAKE.GENTLE@INL.GOV

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.

Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid

DOE Report Briefing

Guohui Yuan, Office of Energy Efficiency and Renewable Energy (EERE)
Michael Toecker, Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

November 7, 2022

U.S. DEPARTMENT OF ENERGY

Agenda

Part 1 – DOE Report Overview

Part 2 – Approach and Findings

Part 3 – Other R&D Activities

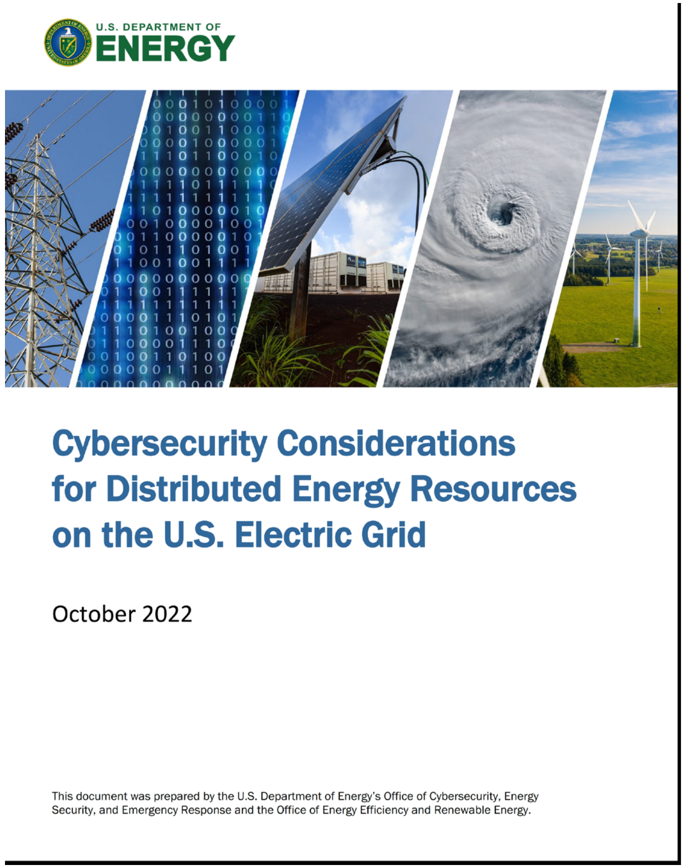
Overview

- **What:** This report provides an overview of cybersecurity considerations that should be considered by the electric sector. It is meant to encourage a dialogue and further conversations between industry and government stakeholders.

- **Why:** While a cyberattack on today's DER may have a limited effect, large amounts of grid-connected DERs in the future could present cybersecurity challenges for the electric power grid.

- **Who:** Utilities and distributed energy resources (DER) operators, providers, integrators, developers, and vendors (collectively, "the DER industry"), as well as policymakers. as we embark on this transformational change to the U.S. electric grid.

- **Team:** DOE program offices (CESER and EERE SETO), NREL, SNL, and a utility partner.


U.S. DEPARTMENT OF ENERGY

Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid

October 2022

This document was prepared by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response and the Office of Energy Efficiency and Renewable Energy.

Major Findings and Recommendations

- **Adopt best practices and meet minimum security requirements.** DER providers can utilize multifactor authentication encryption, and other tools to secure their devices. Many cybersecurity standards exist and can be used to develop security technologies and measures appropriate for their use.
- **Implement good governance.** Design security into utility and DER systems from the beginning and make security a priority for all employees, suppliers, and customers.
- **Incentivize cyber resilience.** Go beyond the standards and work to actively detect threats and adopt a zero-trust approach to verify commands and data.

Definition of DER

Definitions of DER have varied widely; however, for this report, DER are small-scale power generation, flexible load, or storage technologies (typically from 1 kilowatt to 10,000 kilowatts) that can provide an alternative to, or an enhancement of, the traditional electric power system.

These can be located on an electric utility's distribution system, a subsystem of the utility's distribution system, or behind a customer's meter. They may include electric storage, variable generation, distributed generation, demand response, energy efficiency, thermal storage, or electric vehicles and their charging equipment. The main focus of this report is DER from solar, renewables, and battery storage.

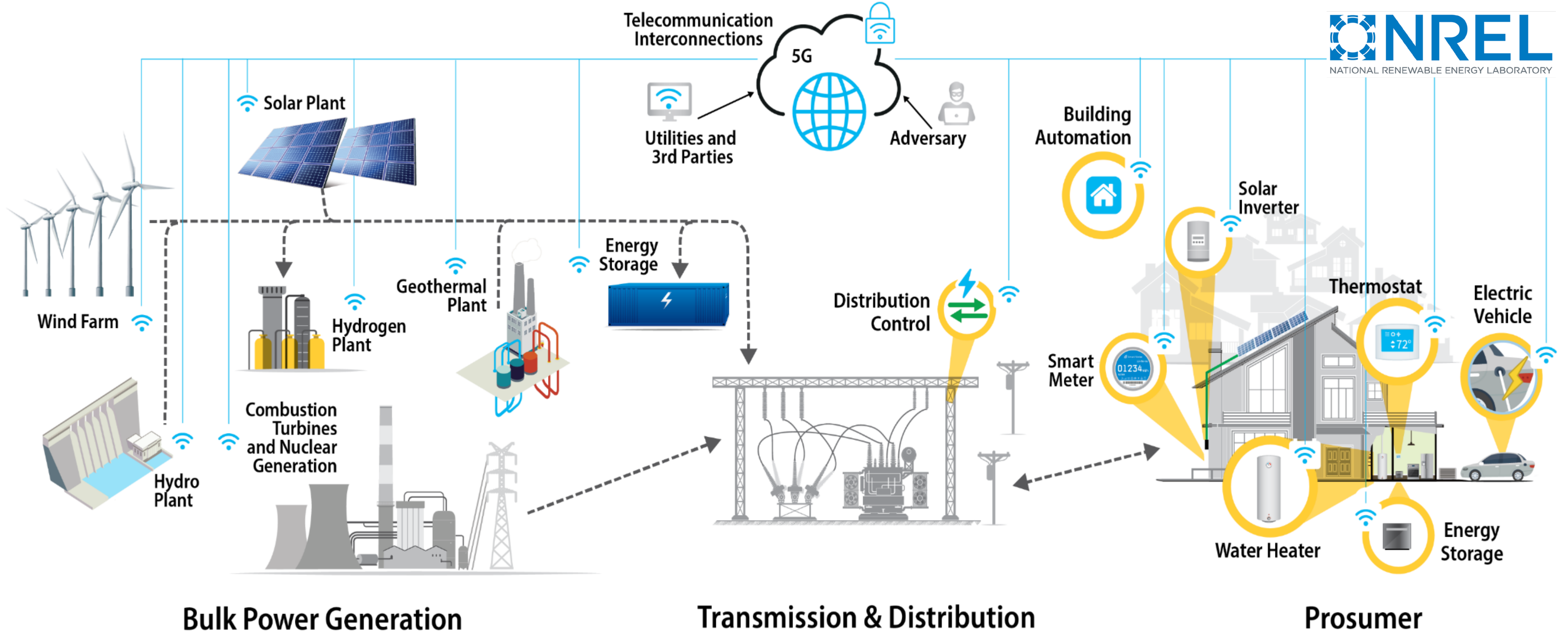
DER deployment is expected to grow from approximately 90 gigawatts (GW) today, to approximately 380 GW by 2025. Nearly half of DERs today are solar photovoltaic (PV) systems, with over 3 million PV arrays on homes across the country. - Wood Mackenzie

The DOE Approach

- The Department of Energy has a leading role in both the cybersecurity of the electric power system, and the transition to cleaner forms of energy
  - The Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is responsible for vulnerability assessment and rapid risk mitigation for energy, including research and development on next generation cyber technologies
  - The Office of Energy Efficiency and Renewable Energy (EERE) is responsible for formulating and directing programs designed to increase the production and utilization of renewable energy
- Both CESER and EERE collaborated on this evaluation, and brought unique viewpoints to the conversation on distributed energy resources

U.S. DEPARTMENT OF ENERGY
Office of Cybersecurity, Energy Security, and Emergency Response

U.S. DEPARTMENT OF ENERGY
Office of ENERGY EFFICIENCY & RENEWABLE ENERGY



NREL
NATIONAL RENEWABLE ENERGY LABORATORY

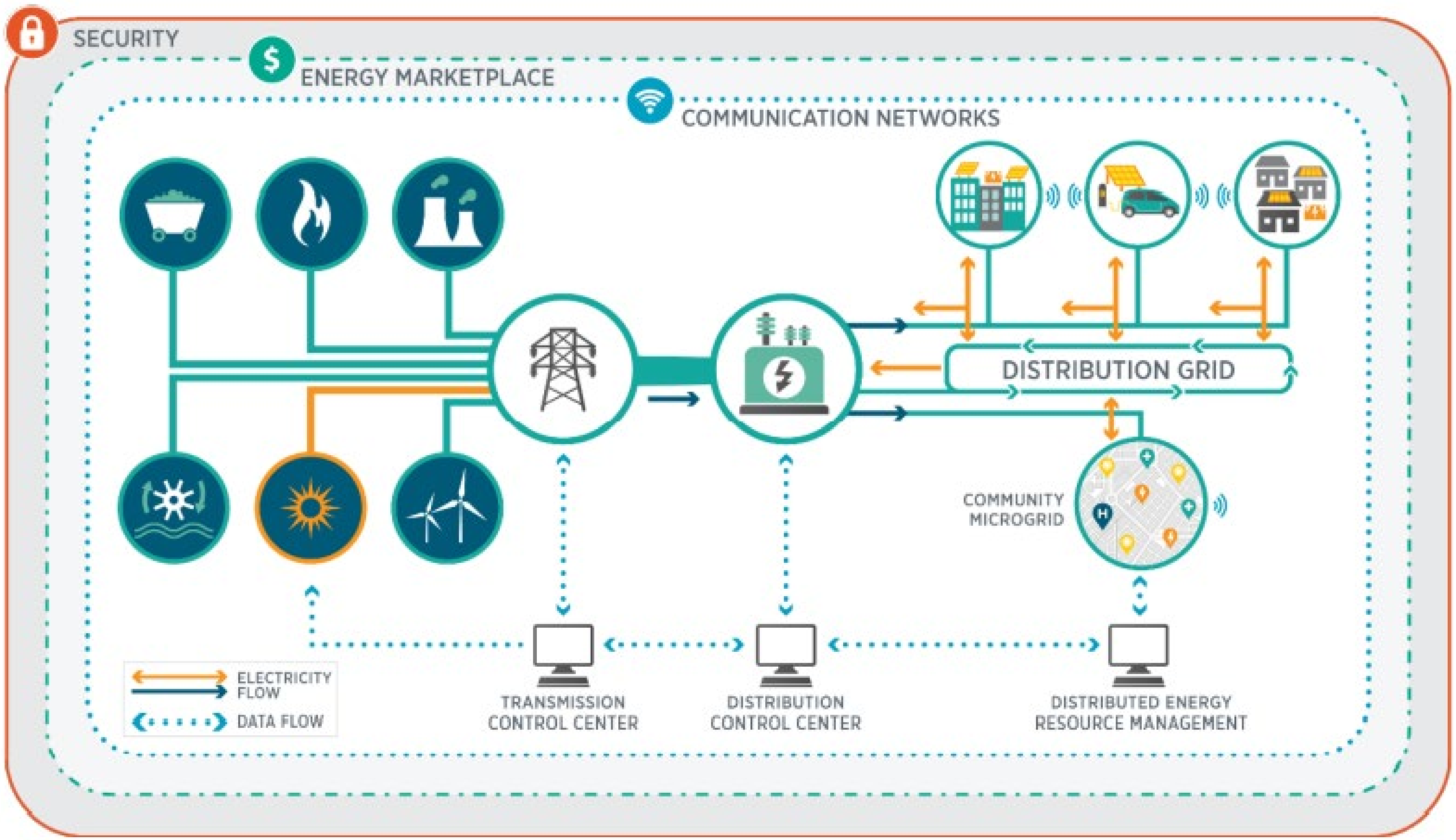
At the Edge of Energy Transformation

The grid is evolving to become more distributed, intelligent, and complex. Coupled with aging infrastructure, the vulnerabilities of emerging energy systems to disruption are not yet well understood.

The Future of DER

The electric grid is undergoing significant, rapid transformation, unprecedented in both transformational nature and rapid pace[1]

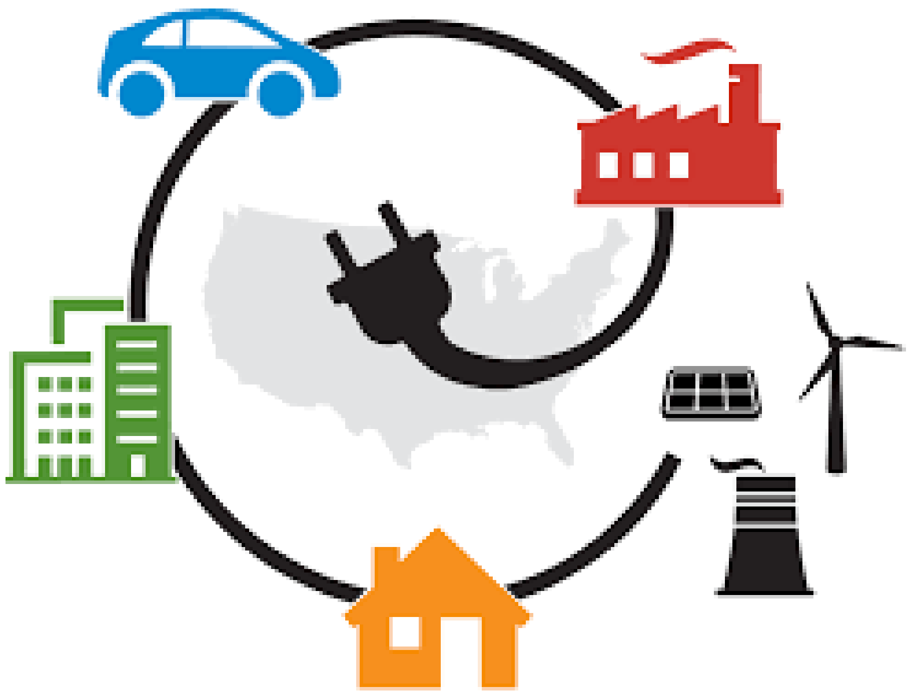
Adoption of Internet of Things (IoT) energy devices for controlling and monitoring consumer use of energy are projected to increase



1) North American Electric Reliability Corporation. (December 2020). 2020 Long-Term Reliability Assessment.

Benefits and Responsibilities for DER

- Most DER are different from traditional generation, their output is highly configurable in unique and powerful ways
  - Because output is software-driven and digital-controlled, DER may react swiftly to provide important services
- This benefit comes with a responsibility to prevent use that could degrade services and capabilities

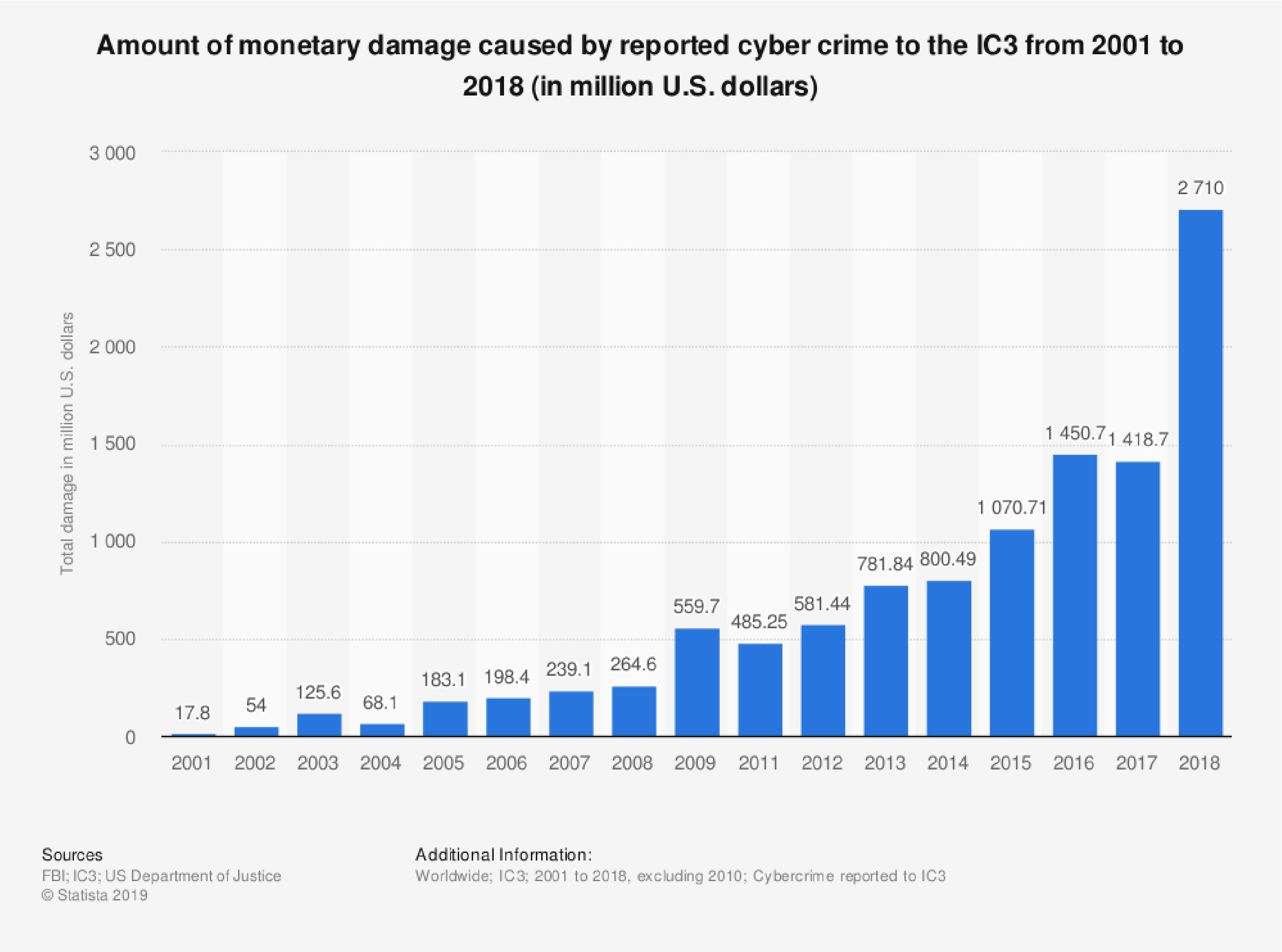


Roles and Responsibilities

- As part of the transition to a more DER-based power grid, new players will be entering the electric power sector
  - Federal Energy Regulatory Commission Order 2222 aims to enable DER aggregators to compete in all regional organized wholesale electric markets.
  - DER services marketed to consumers provide considerable choice in selection, use, and timing of electricity consumption
- DER aggregators, owners, and vendors are expected to play a greatly expanded role in how resources are operated, maintained, and connected
- Coordination and cooperation between the traditional utility role and the forecasted DER role are vital for taking advantage of the positive developments of DER.

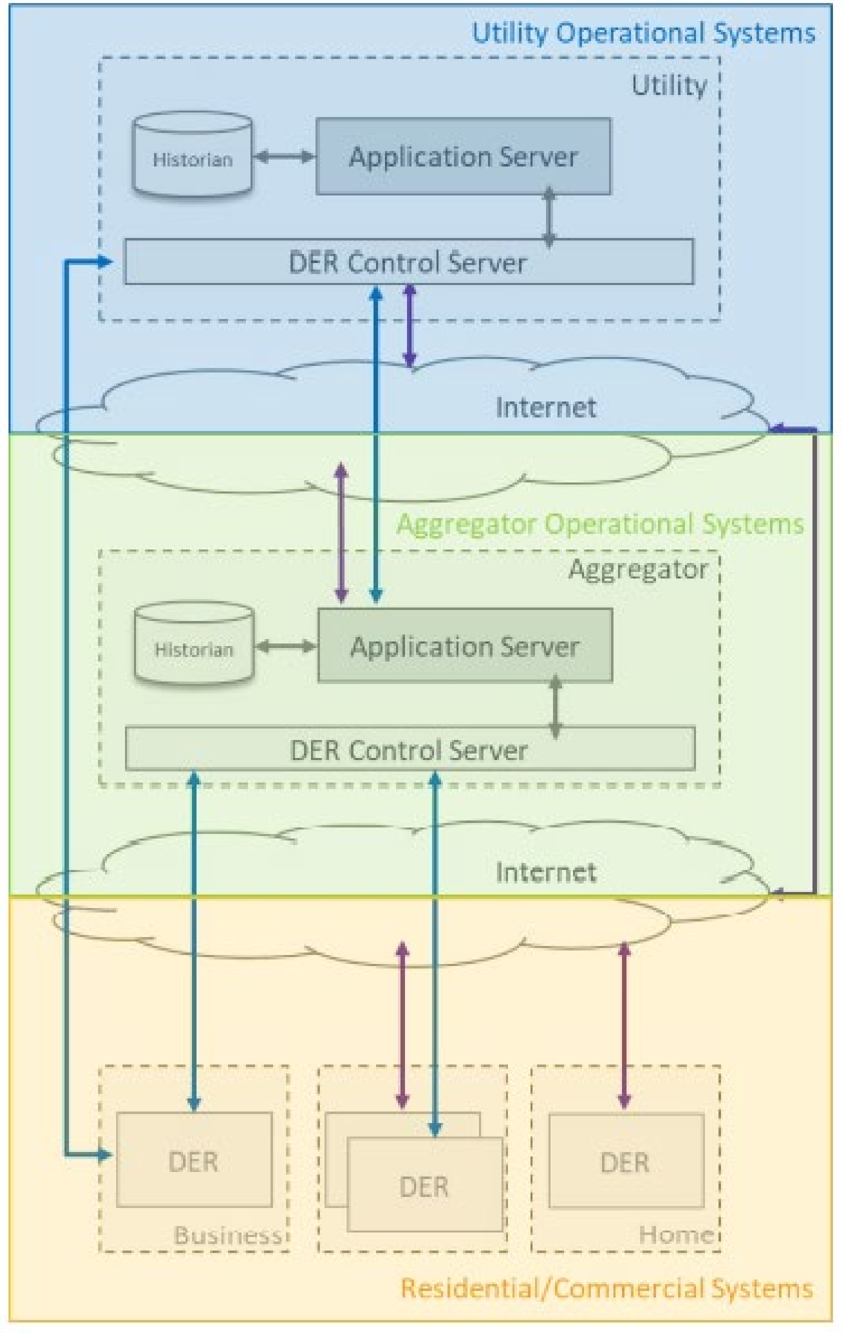
Cybersecurity Trends

- The past 20 years have seen the threat from malicious cyber attackers increase substantially
  - Attackers are powered by new incentives, most notably digital ransom
- Cybersecurity challenges are not anticipated to abate, and will likely increase
  - The future of DER includes significant digitalization and communication
  - Cyber adversaries tend to seek new ways to exploit systems and networks



Cyber Resilience in DER

- The sheer scale of DER deployment, the wide range of communications options, and the level of access needed by various stakeholders requires a zero trust model
  - Zero trust is a set of security design principles, which enforces continuous verification and rejects implicit trust on single points of security failure
- There is an opportunity to design security at the earliest development stages, rather than attempt fixes later.



Future Work

BIPARTISAN INFRASTRUCTURE LAW

- Electricity Distribution Report to Congress, led by CESER
  - As part of the IIJA, U.S. Congress requested the development of a report on enhancing the physical security and the cybersecurity of electricity distribution systems, scheduled to be completed in May 2023.
  - First workshop hosted by NREL on October 5-6, 2022
  - DOE National Labs are tasked with collecting the information and generating a draft
  - Additional stakeholder feedback engagement is under development.
- Clean Energy Cybersecurity Accelerator (CECA)
  - The Clean Energy Cybersecurity Accelerator advances cyber innovation to defend modern, renewable energy technologies against high-priority cybersecurity risks to the energy sector
- Cyber Testing for Resilient Industrial Control Systems (CyTRICS)
  - Leveraging strategic partnerships and facilities and analytic capabilities at six National Laboratories to test cyber resilience of energy technologies.

CECA CLEAN ENERGY CYBERSECURITY ACCELERATOR

CyTRICS

Office of Energy Efficiency and Renewable Energy (EERE)
Solar Energy Technologies Office (SETO)
Cybersecurity R&D

Contact info:
Guohui.Yuan@ee.doe.gov

S2G: Securing Solar for the Grid

VISION

Achieving high cybersecurity maturity levels for solar technologies, equipment, supply chains, facilities, as well as the bulk and distribution electric power grids.

GOAL

Ensure the cybersecurity of electric grids with high penetration levels of solar PV and other DERs

APPROACH

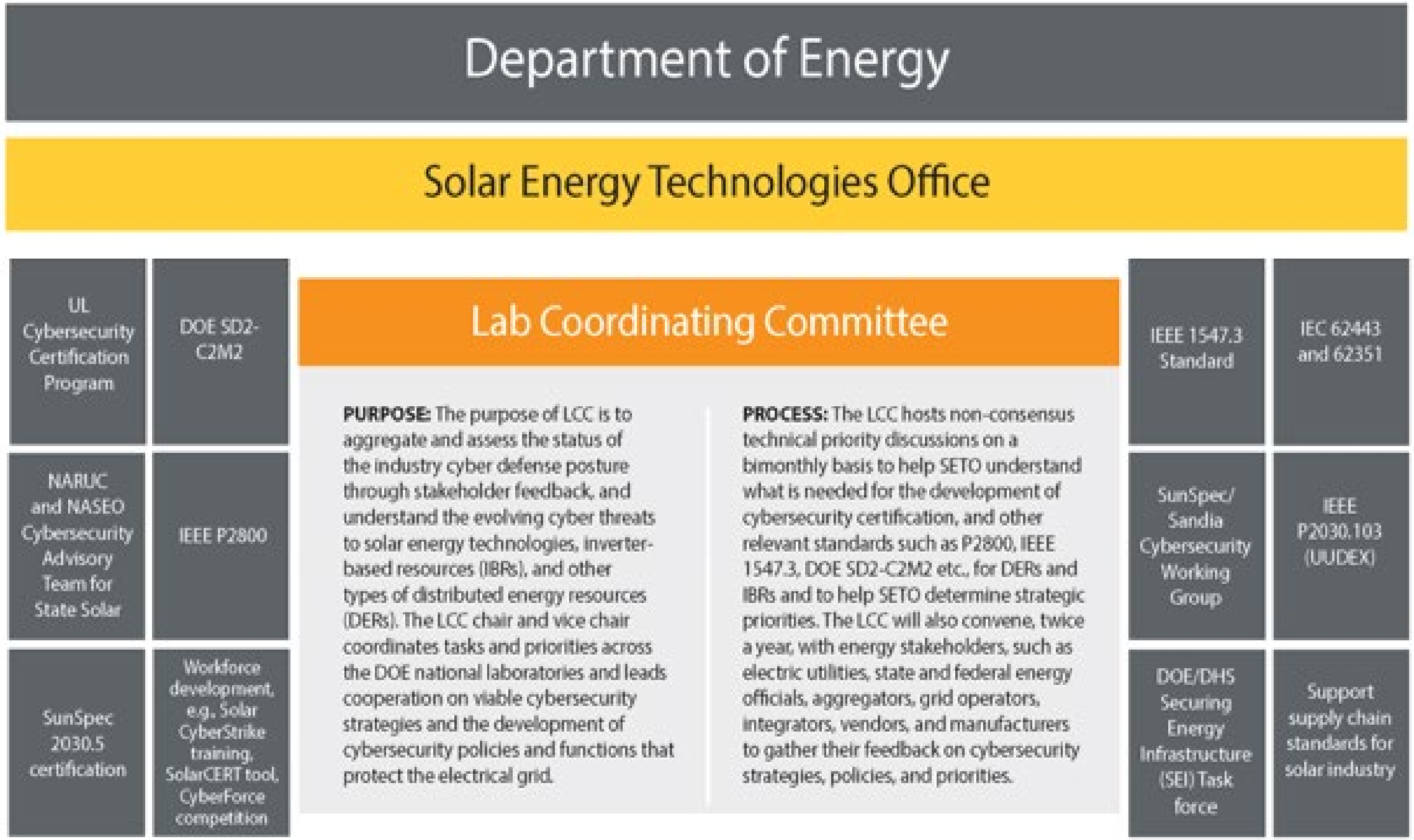
A collaborative effort by multiple national labs, DOE offices, and industry to address gaps in requirement standards, best practices, testing and analysis for solar PV and DERs cybersecurity

EXPECTED OUTCOMES

Development and dissemination of **requirement standards, best practices, equipment testing procedures, assessment tools, as well as education and training materials** for cyber defense, posture and maturity tailored to solar technologies.

S2G Program Activities

- Regularly meet to assess current industry trends and facilitate non-consensus discussion and debate on project priorities.
- Coordinate activities and promotes collaboration with CESER and EERE offices.
- Facilitate Industry Advisory Board meetings.
- Facilitate periodic informational webinars, led or supported by the national labs.



Sandia National Laboratories

Idaho National Laboratory

NREL Transforming ENERGY

Pacific Northwest NATIONAL LABORATORY

Research Thrusts Areas

STANDARDS DEVELOPMENT & BEST PRACTICES

Stakeholder engagement to investigate gaps and develop best practices that can become standards to enable the secure integration of inverter-based resources and DERs.

EDUCATION & WORKFORCE DEVELOPMENT

Development of educational modules and training to increase cybersecurity awareness and knowledge within solar stakeholders.

CYBERSECURITY TOOL KIT & SUPPLY CHAIN

R&D of tools to understand cybersecurity posture, risk assessment to inform investments, and device design security & maturity model for cyber supply chain.

DEVICE

- CyberStrike for Solar
- S2D-C2M2
- Alignment with CESER activities
- ePV-CT
- CAS methods

PLANT

- SolarCERT
- Cyber Strike for Solar
- ePV-CT

SYSTEM

- CyberStrike for Solar
- ePV-CT
- CPYDAR
- UUDEX for solar
- SOAR
- DERMS cyber requirements

INCREASING CYBERSECURITY LEVELS OF SOLAR TECHNOLOGIES

NASEO/NARUC Cybersecurity Advisory Team for State Solar (CATSS)

Engage, educate, and share

Actionable solar cybersecurity strategies and tools for State Energy Officials and Public Utility Commissioners.

Create

Collaborative frameworks and model approaches that can be easily replicated by other states.

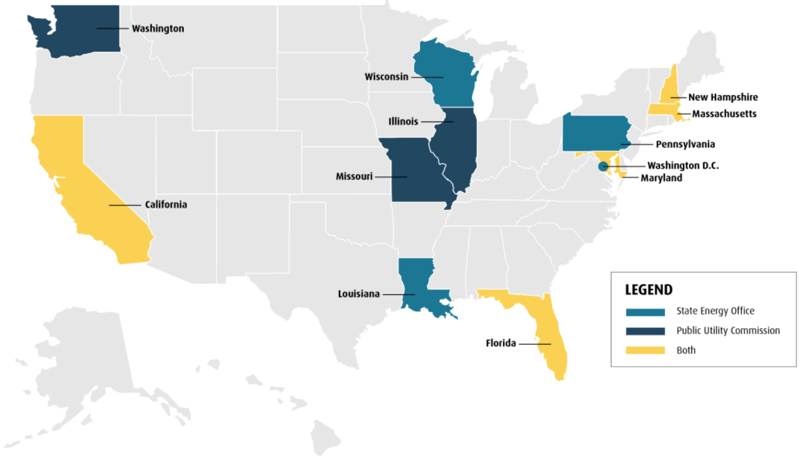
Identify and enable

Pathways for state decision-makers to enhance the security of behind the meter solar systems.

Facilitate

The creation of stronger intra- and interstate relationships, stakeholder communities, collaborative frameworks, and model approaches.

https://naseo.org/issues/cybersecurity/catss



Ongoing Standards and References

- The North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection Standards
- The National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST 2018)
- The Cybersecurity and Infrastructure Security Agency's Securing Industrial Control Systems: A Unified Initiative FY 2019–2021
- The draft IEEE Standard 1547.3 for DER cybersecurity interconnected with electric powersystems
- If approved, an IEEE P2800 standard for securing IBR interconnected with transmission electric power systems
- NERC's Reliability and Security Technical Committee working groups
- The Sandia/SunSpec DER cybersecurity working group
- The International Electrotechnical Commission's (IEC) standards, especially the IEC 62351 standards for securing power system communications
- IEEE 2030 standards, especially the 2030.5 standard for smart energy profile application protocol
- NIST SP 800-82, Guide to Industrial Control Systems Security
- V2G – Bidirectional V2G SAE Suite 3778 (New SAE 3000 Series of V2G)
- NIST SP800-213, IoT Device Cybersecurity Guidance for the Federal Government
- The U.S. DOE Office of Scientific and Technical Information's Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators (SAND2017-13113)

Stay in Touch

twitter.com/ENERGY

energy.gov

instagram.com/energy

facebook.com/energygov

https://www.linkedin.com/company/u-s--department-of-energy/