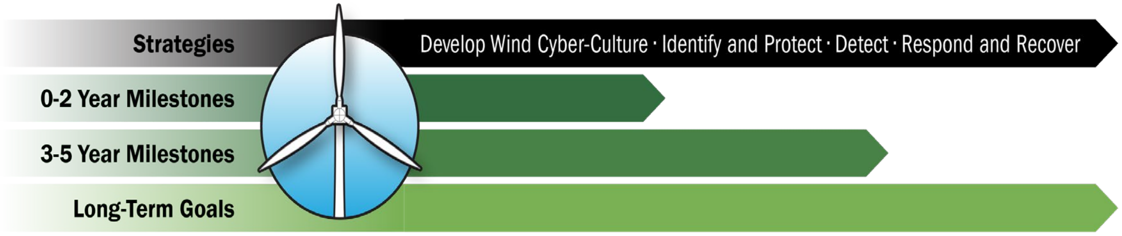
# E09 Roadmap for Wind Cybersecurity

Mitigate Market Barriers – Grid Integration

Jake P. Gentle
Idaho National Laboratory

August 3, 2021


Strategies
Develop Wind Cyber-Culture · Identify and Protect · Detect · Respond and Recover
0-2 Year Milestones
3-5 Year Milestones
Long-Term Goals

# FY21 Peer Review – Project Overview

**Project Summary:**

- As wind and other renewable energy systems grow across the United States, cybersecurity for such systems has become increasingly urgent
- Cyber incidents targeting wind energy systems have already occurred, and will likely increase in sophistication and number
- We developed a time-phased roadmap to address the challenges, building strategies, milestones for improving wind energy cybersecurity in the near-, mid-, and long- term.
- We outline steps to promote cybersecurity culture among the wind energy community, align with the US *National Cyber Strategy*, and leverage the commonly used National Institute of Standards and Technology (NIST) cybersecurity framework to outline steps for improving security in the wind industry

**Project Objective(s) 2019-2020:**

- Release the Roadmap for Wind Cybersecurity, which will motivate the need for wind energy cybersecurity through technology and threat analysis
- Contextualize the roadmap within national energy cybersecurity efforts
- Provide recommendations for improving wind cybersecurity

**Overall Project Mission Statement (Objective of project):**

- By 2030, wind energy systems will be designed, retrofitted and operated to be resilient to cyber-events, minimizing impacts to the power grid

Project Start Year: [2019]
Expected Completion Year: FY [2020]
Total expected duration: [1] years
FY19 - FY20 Budget: $450,000

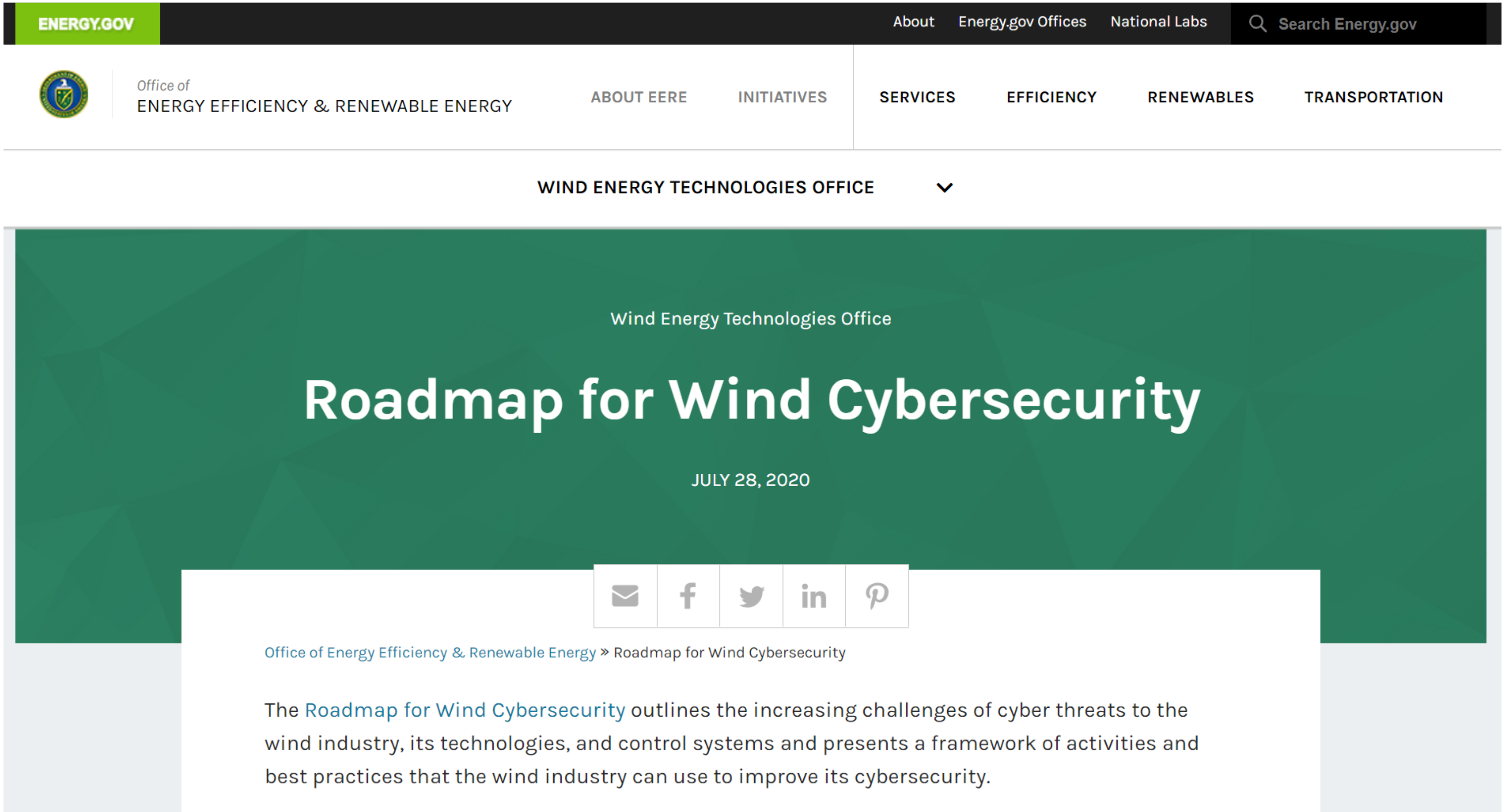
Key Project Personnel:

- INL: Jake Gentle (PI); Colleen Glenn, Shane Hansen, Jeremiah Stoddard, Sarah Freeman, et al.
- NREL: Anuj Sanghvi; Jon White
- SNL: Jay Johnson; Brian Naughton

Key DOE Personnel:

- Jian Fu

# Project Impact



Wind Energy Technologies Office

## Roadmap for Wind Cybersecurity

JULY 28, 2020

Office of Energy Efficiency & Renewable Energy » Roadmap for Wind Cybersecurity

The Roadmap for Wind Cybersecurity outlines the increasing challenges of cyber threats to the wind industry, its technologies, and control systems and presents a framework of activities and best practices that the wind industry can use to improve its cybersecurity.

# Project Impact

## Roadmap for Wind Cybersecurity addresses the following challenges:

- Cyber-incidents will continue to increase in sophistication and number
- Effective cybersecurity practices are difficult to establish, maintain, and trace:
  - construction → repowering → decommissioning
- Wind assets require robust cybersecurity practices for integration with bulk electric system
  - NERC CIP requirements are minimums, passing an audit does not ensure security
- Wind energy technologies and deployments are highly diverse
- Limited number of established cybersecurity standards specific to wind energy
- Effective and available cybersecurity options may be cost-prohibitive
  - This is only the case when you use existing “cost” metrics. What is the cost of a permanent outage? What is the cost due to loss in confidence from an industry-wide lens?
- Information sharing is limited among wind energy stakeholders
- Wind-specific cybersecurity services, products, and strategies are lacking
- Few incentives for stakeholders to prioritize cybersecurity

# Project Impact

## Wind Cybersecurity Roadmap Strategies

### 1. Develop Wind Cyber-Culture

Promote cybersecurity culture among wind energy community, encouraging cybersecurity information sharing including cyber-threats and vulnerabilities, cyber-incidents, lessons learned, and recommended practices

### 2. Identify and Protect

Develop an organizational understanding to manage cybersecurity risk to wind assets, data, and grid infrastructure; develop and implement appropriate cyber-safeguards to ensure delivery of wind energy

### 3. Detect

Develop and implement appropriate detection technologies to identify malicious or unintentional cybersecurity events impacting wind technologies and networks

### 4. Respond and Recover

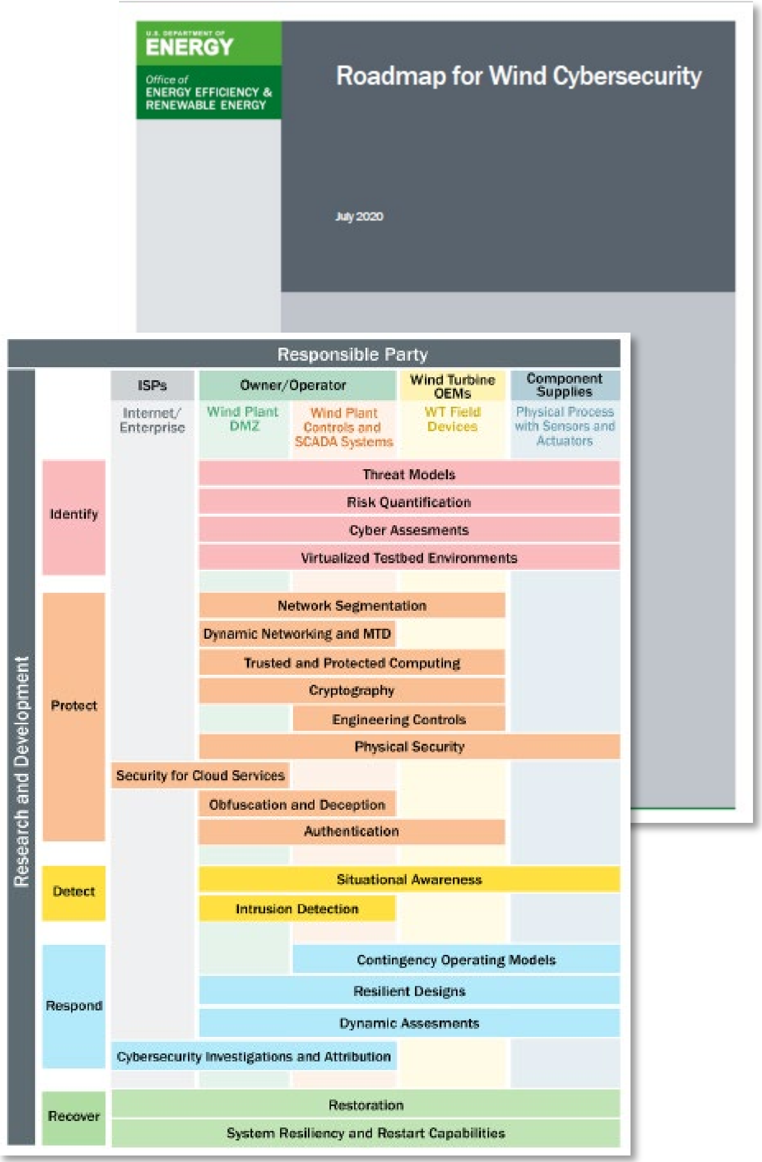
Encourage development and implementation of appropriate activities to take timely and effective action to mitigate cybersecurity incidents; execute plans for resilience and restore wind energy capabilities or services

# Program Performance – Scope, Schedule, Execution

| | Develop Wind-Cyber Culture | Identify and Protect | Detect | Respond and Recover |
|---|---|---|---|---|
| **0-3 Year Milestones** | Conduct cyber-focused workshops, trainings and working group engagements<br>Standardize cyber-threat and vulnerability sharing methods<br>Share cybersecurity alerts among wind community | Identify critical wind assets and impact on grid security<br>Identify adversaries and threat models for wind<br>Develop wind specific reference architectures<br>Design testbeds to evaluate wind technology | Implement standardized cyber-threat sharing<br>Research wind-specific intrusion detection systems and methods<br>Promote guidelines for effective situational awareness for operational technology security | Define cybersecurity roles and responsibilities among stakeholders<br>Coordinate with DHS and DOE to establish a wind-specific incident response capability<br>Develop dynamic assessment technologies for wind control networks |
| **3-5 Year Milestones** | Share mitigation strategies with others<br>Make software and tools available to secure wind energy systems<br>Regular participation in cybersecurity exercises | Validate existing wind reference architecture via onsite assessments<br>Identify attack pathways for wind and leverage from other sectors<br>Develop community-wide testbeds to investigate cyber-vulnerabilities | Establish public-private sector partnerships for threat sharing<br>Improve wind-specific anomaly-based intrusion detection technologies<br>Develop and deploy situational awareness tools | Develop cyber-incident response procedures<br>Implement coordination with system operator/ balancing authority/ reliability coordinator<br>Implement broad field testing of system restart and resiliency capabilities |
| **Long-Term Goals** | Sustain improvement to wind cybersecurity software and tools<br>Develop and standardize secure communication architectures and protocols, and equipment standards<br>Develop OT cybersecurity workforce for wind energy | Conduct processes to evaluate systems based on cyber-security posture<br>Develop cyber-resilient wind plant designs<br>Publish cybersecurity specific standards for wind plants<br>Establish a standards certification & authority | Educate government and private sector partners to understand wind technologies<br>Support continued R&D for intrusion detection for future wind technologies | Incorporate new or enhance existing cyber-threat, vulnerability, incident, and mitigation information sharing platform<br>Establish wind industry-specific guidelines for cyber-incident reporting and post-incident investigations |

# Program Performance – Accomplishments & Progress

- Workshops and presentations to raise industry awareness and seek feedback on priorities
  - Assessing Wind Cybersecurity Workshop: July 2019
  - Multiple conference presentations and workshops
- Feedback sought from DOE experts, industry partners, and other relevant stakeholders
  - DOE Office of Electricity formal reviews
    - November 2019 & February 2020
  - DOE-Office of Cybersecurity, Energy Security, and Emergency Response (CESER) formal reviews
    - November 2019 & February 2020
- Roadmap for Wind Cybersecurity published in July 2020
  - National Energy Cybersecurity Efforts
  - Wind Energy Technology Landscape
  - Wind Cyber Threat Landscape
  - Wind Cybersecurity R&D (using NIST Framework)
  - Standards Development
  - Best Practices



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

Roadmap for Wind Cybersecurity

July 2020

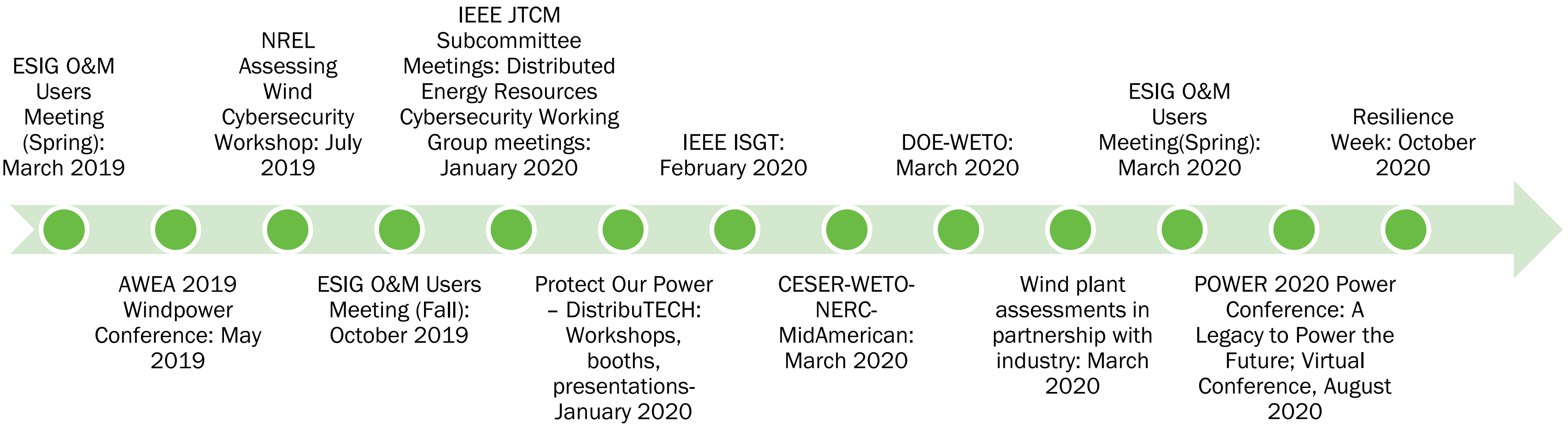
Responsible Party

Research and Development

| | ISPs | Owner/Operator | | Wind Turbine OEMs | Component Supplies |
|---|---|---|---|---|---|
| | Internet/ Enterprise | Wind Plant DMZ | Wind Plant Controls and SCADA Systems | WT Field Devices | Physical Process with Sensors and Actuators |
| Identify | | Threat Models | | | |
| | | Risk Quantification | | | |
| | | Cyber Assesments | | | |
| | | Virtualized Testbed Environments | | | |
| Protect | | Network Segmentation | | | |
| | | Dynamic Networking and MTD | | | |
| | | Trusted and Protected Computing | | | |
| | | Cryptography | | | |
| | | | Engineering Controls | | |
| | | Physical Security | | | |
| | Security for Cloud Services | | | | |
| | | Obfuscation and Deception | | | |
| | | Authentication | | | |
| Detect | | Situational Awareness | | | |
| | | Intrusion Detection | | | |
| Respond | | | Contingency Operating Models | | |
| | | Resilient Designs | | | |
| | | Dynamic Assesments | | | |
| | Cybersecurity Investigations and Attribution | | | | |
| Recover | Restoration | | | | |
| | System Resiliency and Restart Capabilities | | | | |

# Stakeholder Engagement & Information Sharing

## ROADMAP ENGAGEMENT TIMELINE



ESIG O&M Users Meeting (Spring): March 2019

AWEA 2019 Windpower Conference: May 2019

NREL Assessing Wind Cybersecurity Workshop: July 2019

ESIG O&M Users Meeting (Fall): October 2019

IEEE JTCM Subcommittee Meetings: Distributed Energy Resources Cybersecurity Working Group meetings: January 2020

Protect Our Power – DistribuTECH: Workshops, booths, presentations- January 2020

IEEE ISGT: February 2020

CESER-WETO-NERC-MidAmerican: March 2020

DOE-WETO: March 2020

Wind plant assessments in partnership with industry: March 2020

ESIG O&M Users Meeting(Spring): March 2020

POWER 2020 Power Conference: A Legacy to Power the Future; Virtual Conference, August 2020

Resilience Week: October 2020

### Engagement Strategies

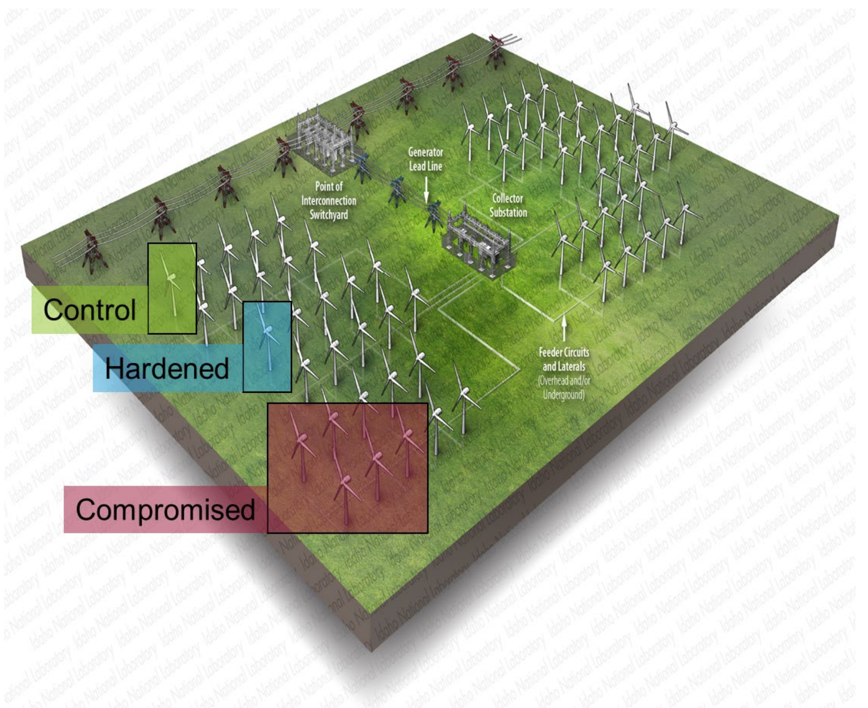
- Information Sharing
- Workforce Development
- Working Groups
- Vendor Engagement
- Cybersecurity Exercises
- Incident Response
- Power System Contingency Planning

### Expert Reviews

- DOE-Office of Energy Efficiency & Renewable Energy
- DOE-Office of Electricity (OE) formal reviews
- DOE-Office of Cybersecurity, Energy Security, and Emergency Response (CESER) formal reviews
- Requests from a large list of industry partners to review
  - NERC, NIST, EEI, National Grid, NYPA, Xcel, Xtec, E&E News, SCE, PG&E, OPPD, OG&E, NRECA, NARUC, ARESCA, Duke, EDF, etc

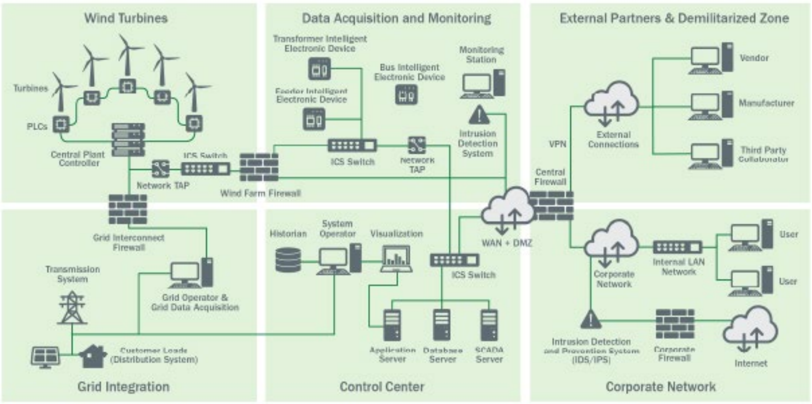
# Program Performance – Upcoming Activities

- Roadmap was published by DOE WETO on-time with significant stakeholder reviews
  - Roadmap was identified as “model” for EERE
- Roadmap needs to be continuously updated
  - Seek feedback from industry
  - Make updates as standards evolve
  - Incorporate lessons learned from current and future wind cybersecurity events


Control
Hardened
Compromised
Point of Interconnection Switchyard
Generator Lead Line
Collector Substation
Feeder Circuits and Laterals (Overhead and/or Underground)
Idaho National Laboratory

Follow-on R&D efforts that follow the recommendations from the *Roadmap for Wind Cybersecurity*

- Field Demonstration Opportunities with Industry
  - INL, SNL, Industry partners
  - FY21 initiated, long term partnership focused
- Cybersecurity for Wind Workshop
  - Collaboration with Wind Consortium
  - September 2021, Washington DC



# Key Takeaways and Closing Remarks

## Project Impact:

- WETO’s plan for the use of the roadmap is 5-fold, and cybersecurity remains a DOE cross-cut priority:
  1. Raise awareness and foster a wind-cyber culture for the wind industry
  2. Provide a time-phased framework for near-, mid- and long-term efforts
  3. Illuminate best practices as they may apply to the wind industry
  4. Identify research needs, gaps and opportunities that will securely advance technology
  5. Inform DOE and WETO to guide its future R&D investments.

## Project Performance:

- Considered a “model” for other roadmaps to follow – Former Deputy Assistant Secretary for Renewable Power
- Published on time

## Stakeholder Engagement:

- Official engagement with DOE-Office of Energy Efficiency & Renewable Energy, DOE-Office of Electricity (OE) and DOE-Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
- Reviews from a large list of industry partners spanning utilities, governmental agencies, cooperatives, and standards makers
- Presentation of Roadmap to stakeholders at industry conferences and workshops to work towards core goal of building wind-cyber community

# Key Takeaways and Closing Remarks

## Conclusions

- Research is needed to develop better technologies, methods, and tools for wind energy cybersecurity
- Define and implement basic cyber-hygiene
- Develop robust, consistent cybersecurity programs
- Develop and encourage greater participation in wind-specific cybersecurity information sharing
- Conduct routine cyber-assessments
- Further develop cybersecurity standards for wind energy technologies
- Define and sustain cybersecurity roles and responsibilities throughout industry