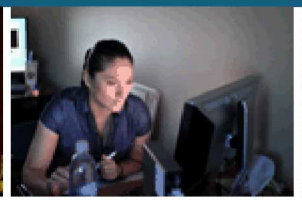
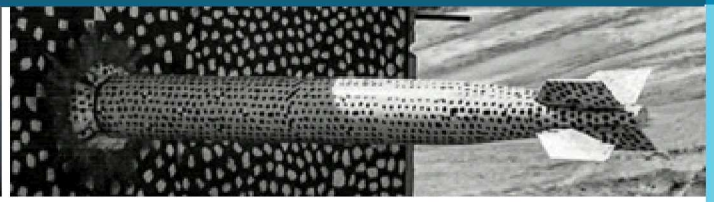
SAND2020-11215C

Roadmap for Solar Cybersecurity





Resilience Week
Salt Lake City, 19-22 Oct 2020

Jay Johnson

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Motivation for the Solar Cybersecurity Roadmap

DER must provide critical reliability services going forward

Interconnection and interoperability standards in the US require DER to provide communication-based grid services

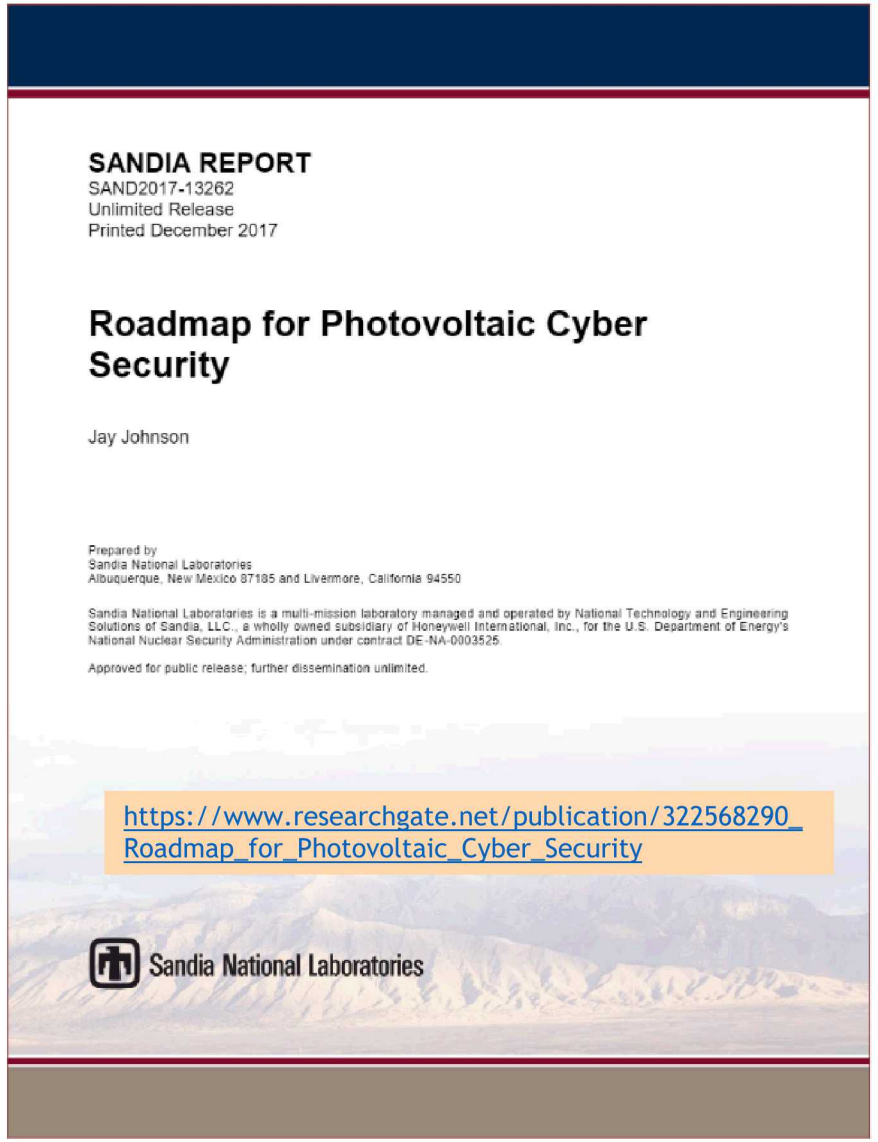
- IEEE 1547-2018 includes communication-enabled grid-support functions for DER
- California Electric Rule 21 requires DER communications

DER cybersecurity is inherently different than 'business-as-usual' because:

- Unlike bulk generators, DER often connected to grid operators via public internet
- Unlike most internet-of-things (IoT) devices, DER can directly impact power system operations
- DER typically have limited processing capabilities, so they often do not natively support encryption or other security features

Why should DOE and the national labs have a role here?

- Address long-term and short-term threats
- Promote harmonization across the broader DER and utility sectors
- Assist with orderly evolution of standards



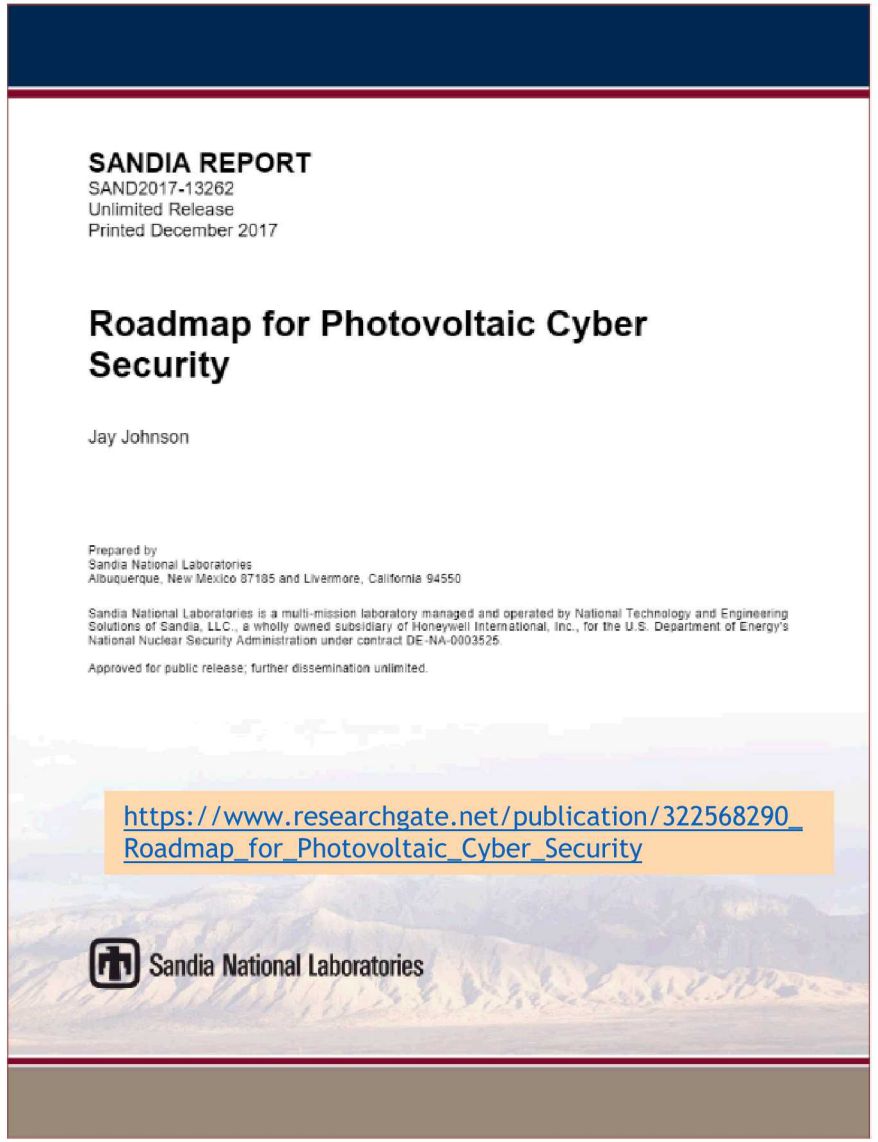
Roadmap for PV Cyber Security

Roadmap

- Published in Dec 2017, it outlines a **5-year strategy** for DOE, industry, and standards development organizations in areas of Identify/Protect, Detect, and Respond/Recover
- Focused on PV, but highly **extensible to other DER**
- Closely aligned with 2011 "Roadmap to Achieve Energy Delivery Systems Cybersecurity"
- Explores existing research by DOE, other agencies, and industry

Major recommendations

- Engage in cross-industry communication and collaborations (e.g., information sharing programs)
- Develop standards, guidelines, and best practices (leveraging existing work)
- Foster R&D programs to develop solutions for protecting infrastructure, detecting threats, and recovering from attacks
- Work to harden infrastructure, conduct self-evaluations, and practice good cyber hygiene to stay ahead of adversaries



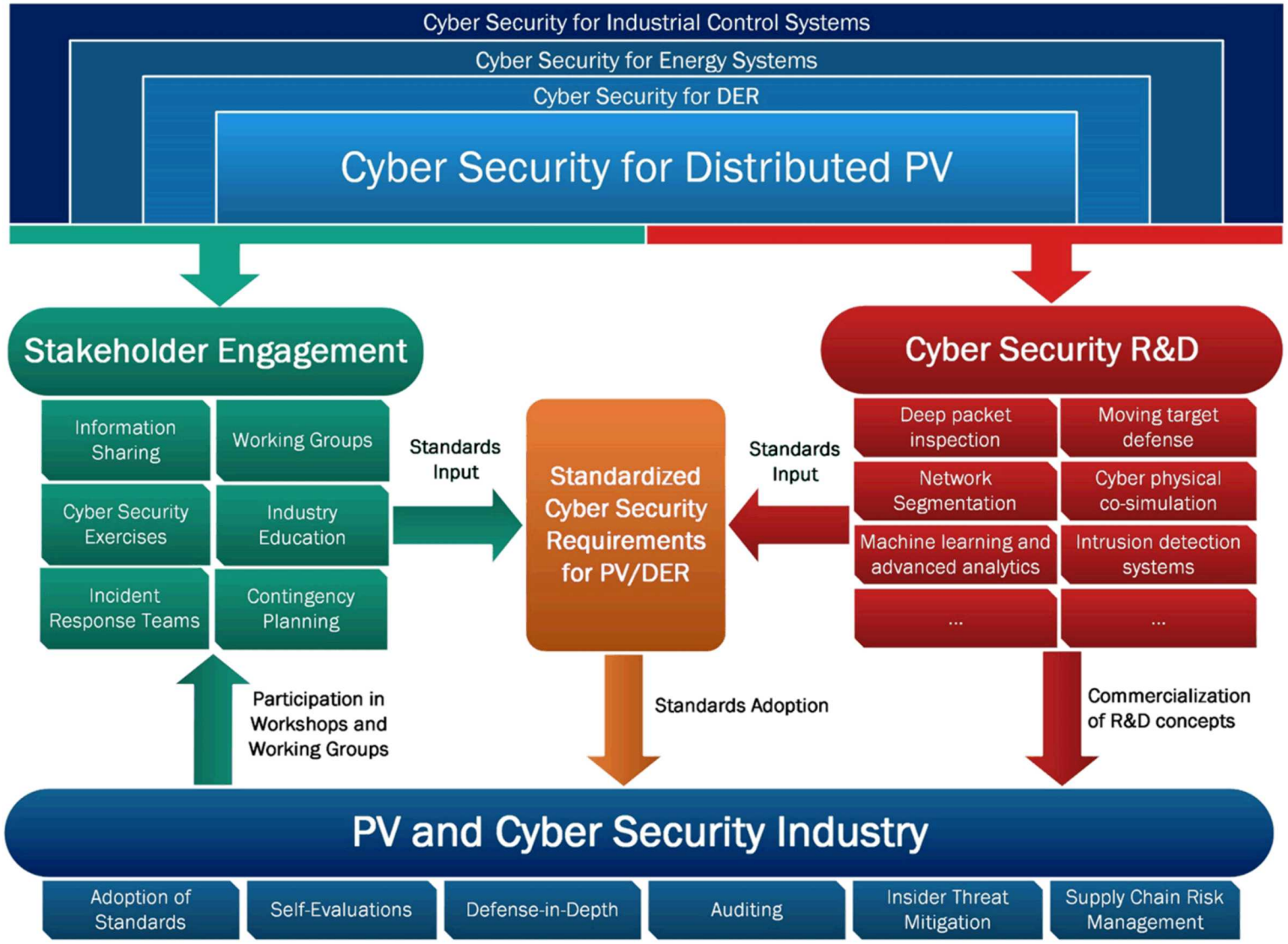
Roadmap

- **Vision:** By 2023, grid operators, system owners, and aggregators communicate with interoperable photovoltaic systems using safe, secure, resilient networks with high availability, data integrity, and confidentiality.
- **Broken into 3 strategy areas:**
  - Identify and Protect
  - Detect
  - Respond and Recover
- **Focused on 4 areas/user groups:**
  - Stakeholder Engagement
  - Research and Development
  - Industry (grid operators, aggregators, and PV vendors)
  - Standards and Guidelines
- **Major goals:**
  - Commercialize security R&D
  - Create cyber security standards
  - Use situational awareness and intrusion detection systems
  - Standardize response procedures

Table 1: Photovoltaic Cyber Security Roadmap.

Vision	By 2023, grid operators, system owners, and aggregators communicate with interoperable photovoltaic systems using safe, secure, resilient networks with high availability, data integrity, and confidentiality.		
Barriers	• Cyber threats are unpredictable and evolve faster than the industry's ability to develop and deploy countermeasures • Security upgrades to legacy systems are constrained by inherent limitations of the equipment and architectures • Performance/acceptance testing of new control and communication solutions is difficult without disrupting operations • Threat, vulnerability, incident, and mitigation information sharing is insufficient among government and industry • Weak business case for cybersecurity investment by industry • Regulatory uncertainty in photovoltaic cyber security		
Strategies	**Identify and Protect:** Improve security posture and harden PV communication infrastructure to protect PV assets	**Detect:** Implement tools with protective measures which automatically recognize and warn operators of security breaches	**Respond and Recover:** Create tools and contingency plans to maintain critical operations and recuperate from cyber security attacks
Stakeholder Engagement	- Establish awareness trainings and information sharing programs for protecting critical infrastructure - Create working groups to establish industry best practices (e.g., patch management)	- Establish public-private information sharing program and industry education programs for detecting malicious network activities - Conduct cyber security exercises	- Establish incident response teams and associated incident command structure between industry and government agencies - Create contingency plans for the loss of DER due to cyber attack
Research and Development	- Create threat models based on risk quantification, red team assessments on virtualized testbeds - Design new segmentation schemes, software defined networks, engineering controls, cryptographic and obfuscation approaches for PV control networks - Assess and protect PV systems with novel physical security, supply chain, and authentication approaches	- Establish situational awareness for PV OT networks using advanced analytics and visualization - Design intrusion detection systems using out-of-band data, deep packet inspection, trust monitors, trust-weighting schemes, etc. - Create machine learning-based cyber detection tools which identify atypical network traffic or operations	- Design resilience into PV equipment so devices fail gracefully and power system operations are not impacted - Create intrusion detection systems to act after detection - Create dynamic assessment tools to manage failures, initiate cyber security remedial action schemes, and regain control given controller compromise or failure - Create forensics and investigatory tools to attribute attacks to those responsible in a timely manner
Industry Best Practices (Grid Operators and Aggregators)	- Implement risk management plan - Implement cyber security maintenance and hygiene practices - Use role-based access controls - Implement defense-in-depth approaches to cyber security	- Implement situational awareness and intrusion detection systems at the grid operator and aggregator levels - Conduct continuous security monitoring with warning and alarm systems	- Document and eradicate intrusion footholds - Design and implement response, recovery, and contingency plans - Work with government to conduct investigations - Document & share lessons learned
Industry Best Practices (PV Industry)	- Harden PV inverters through aggressive in-house and external testing - Create patching release methodology and assign personnel to rapidly respond to new vulnerabilities	- Establish anti-tamper mechanisms - Participate in information sharing programs to determine if vulnerabilities detected in other products or networks affect PV equipment	- Design PV equipment to fail in predictable, safe manner - Maintain trusted gold master firmware for re-flashing equipment after cyber attack - Respond to newfound vulnerabilities with patches
Standards and Guidelines	- Develop and standardize secure communication architectures and protocols, access rules, and certification procedures	- Create recommendations for situational awareness programs and best practices for intrusion detection system software	- Establish industry-wide guidelines for contingency operations, restoration procedures, and cyber investigations
0-2 Year Milestones	- Widespread industry engagement in working groups, trainings, and workshops	- IDS technologies field tested for aggregator and grid operator PV networks	- Industry recommendations for PV operations and recovery strategies based on simulations
3-5 Year Milestones	- Create standards or guideline recommendations for cyber-secure protocols, architectures, and certification procedures - Threat intelligence and data sharing between stakeholders	- All grid operators and aggregators have situational awareness capabilities and intrusion detection systems - Anonymize and publicize operational datasets for security analytics	- Standardize resilient design for PV/DER and associated control networks - Established cyber response teams - Field tests of automated response and recovery
Goals	- Commercialization and adoption of protection R&D solutions - Publication of cyber security standards for PV control networks	- Commercialization of intrusion detection R&D solutions - Widespread use of situational awareness and IDS technologies	- Commercialization and adoption of recovery R&D solutions - Standardize response and recovery procedures for grid operators

Roadmap for Cybersecurity for Building Technologies



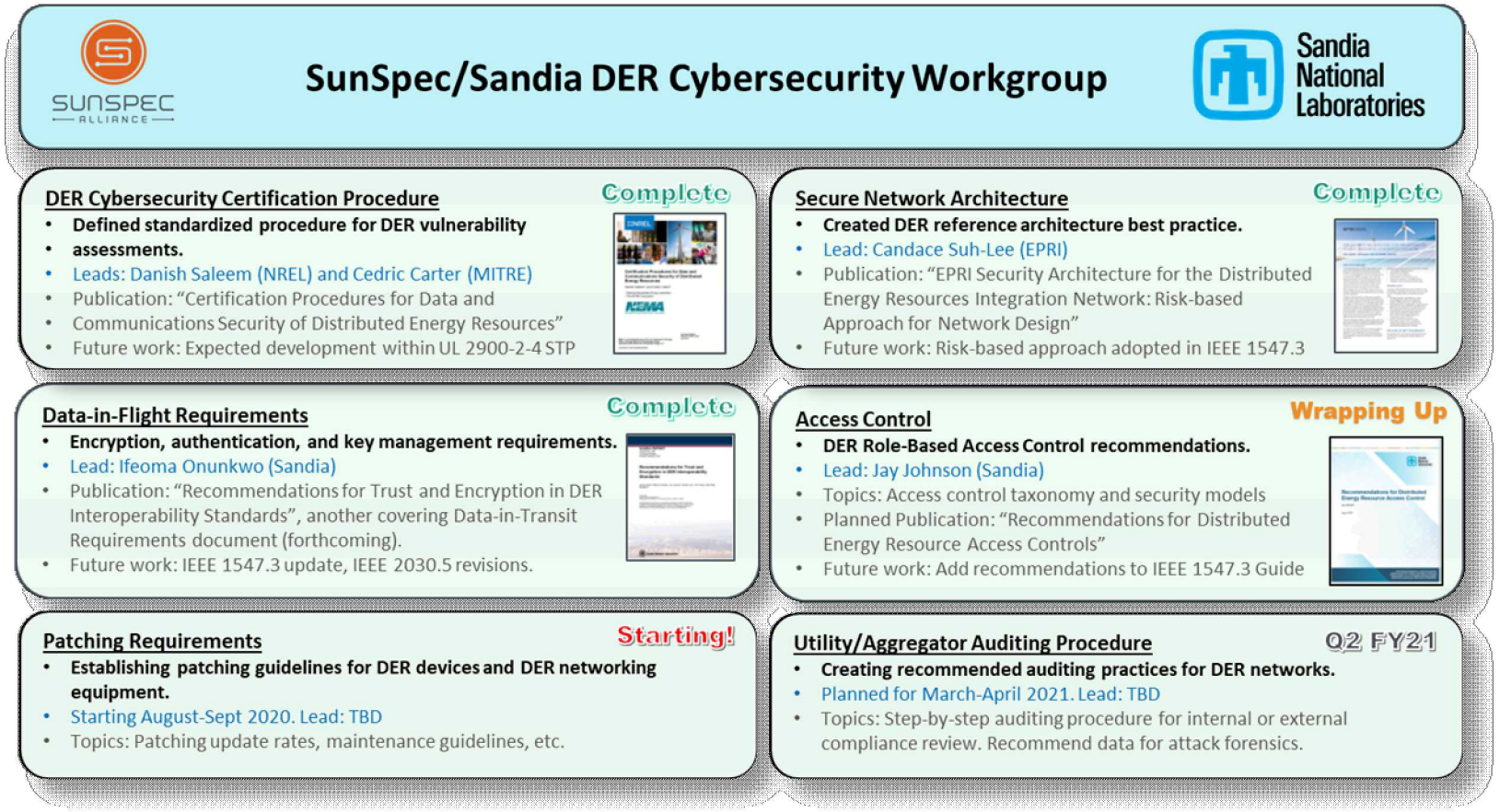
Stakeholder Engagement

Engagement activities bring together individuals across industry, academia, and government to exchange ideas and learn

- Typically government (e.g., DOE), industry groups, or NGOs will organize gatherings

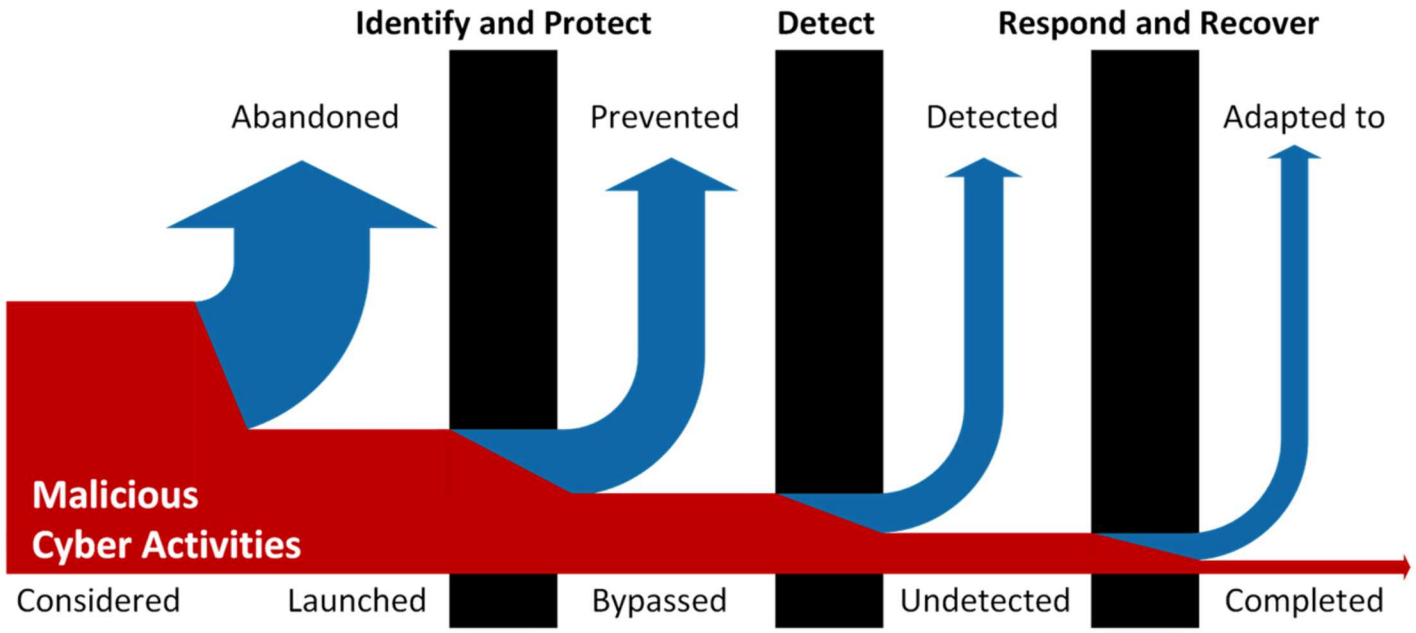
Types of stakeholder engagement

- **Information sharing programs**: sharing actionable threat information
- **Industry education**: workshops, webinars, conferences, etc.
- **Working groups**: e.g., the DER Cybersecurity Workgroup
- **Cybersecurity exercises**: industry participates in simulated cyber security attacks to discover system weaknesses (e.g., GridEx)
- **Incident response**: public-private coordination to contain, eradicate, and recover from attacks



Workgroup information: https://sunspec.org/cybersecurity-work-group/
Email: support@sunspec.org to participate!

Cybersecurity R&D



- Threat Models
- Risk Quantification
- Cyber Assessments
- Network Segmentation
- Dynamic Networking and Moving Target Defense
- Trusted and Protected Computing
- Cryptography
- Virtualized Testbed Environments
- Engineering Controls
- Physical Security
- Security for Cloud-Services
- Obfuscation and Deception
- Authentication

- Situational Awareness
- Intrusion Detection

- Resilient Designs
- Dynamic Assessment
- Contingency Operating Modes
- Restoration
- Investigations and Attribution

Industry Best Practices

DER operators and vendors must make cybersecurity a priority at all levels of their organizations:

- **Adopt industry standards and guidelines**, e.g., NIST SP 800-82 "Guide to ICS Security"
- **Cybersecurity self-evaluations**: use DHS US-CERT Cyber Security Evaluation Tool (CSET) or DOE/DHS Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) to identify critical assets and protect them appropriately
- **Audit control networks** to ensure the system is appropriately architected, patched, and monitored
- **Cyber security hygiene and patching**:
  - Fully document inventories, system topologies, controls, and security practices
  - Use strong passwords
  - Define roles and responsibilities for patching known vulnerabilities
- **Employ defense-in-depth** (layering multiple security features) so the system is less attractive to would be attackers
- Address **supply chain** management and **insider threats**

So how are we doing after 3 years? (my personal scorecard)

Strategies	Identify and Protect: Improve security posture and harden PV communication infrastructure to protect PV assets	Detect: Implement tools with protective measures which automatically recognize and warn operators of security breaches	Respond and Recover: Create tools and contingency plans to maintain critical operations and recuperate from cyber security attacks

0-2 Year Milestones	- Widespread industry engagement in working groups, trainings, and workshops
	  - **Improving representation at DER Cybersecurity Workgroup meetings, Rule 21 SIWG Cyber calls, etc. Many attend but few engage in conversation.**
		- IDS technologies field tested for aggregator and grid operator PV networks
		  - **DOE funded projects investigating intrusion detection systems for PV/DER applications. Little progress in commercialization/ deployment.**
			- Industry recommendations for PV operations and recovery strategies based on simulations.
			  - **Many papers investigating power system impacts from DER cybersecurity attacks. Power system recovery (black start) is known, but few address cybersecurity breach recovery strategies.**

3-5 Year Milestones	- Create standards or guideline recommendations for cyber-secure protocols, architectures, and certification procedures
	  - **IEEE 1547.3 Guide is a start, but need to create a national standard for the solar industry**
	- Threat intelligence and data sharing between stakeholders
	  - **No program at this time. A newly starting DOE TCF project will investigate the creation of a DER-CERT and DER-ISAC.**
		- All grid operators and aggregators have situational awareness capabilities and intrusion detection systems
		  - **Discussed extensively. Operational systems are not wide-spread.**
		- Anonymize and publicize operational datasets for security analytics.
		  - **No known data sharing programs.**
			- Standardize resilient design for PV/DER and associated control networks
			  - **There's a start with the EPRI reference architecture and IEEE 1547.3 guidance.**
			- Established cyber response teams
			  - **Nothing specific to DER, but the DHS ICS-CERT could respond.**
			- Field tests of automated response and recovery
			  - **No known demonstrations of cyber response and recovery drills. No automated recovery (e.g., Security Orchestration, Automation and Response) tools exist for PV.**

Goals	- Commercialization and adoption of protection R&D solutions
	  - **PV industry, service providers, and utilities are adding new security features to fielded hardware and OT networks. Much more should be done.**
	- Publication of cyber security standards for PV control networks
	  - **No standard, but a growing collection of guides for PV applications.**
		- Commercialization of intrusion detection R&D solutions
		  - **Many products on the market, but none specifically tailored to PV/DER applications.**
		- Widespread use of situational awareness and IDS technologies
		  - **Utilities and 3rd party aggregators/DER service providers are exploring options. Implemented systems are for generic OT networks.**
			- Commercialization and adoption of recovery R&D solutions
			  - **No known solutions.**
			- Standardize response and recovery procedures for grid operators
			  - **Extensive guidance for grid recovery, but no procedures for DER cyber-attacks.**

Conclusion

Roadmap highlighted a 5-year strategy focused on:

- Stakeholder engagement
- Codes and standards development
- Research and development
- Industry best practices

Many reasons for government to engage in cybersecurity activities

- Harmonize security practices and standards across the nation
- Accelerate the research, development, and adoption of secure technologies

We're making progress as a community, but there is still substantial work to do in this area. We need prioritize:

- Commercialization of R&D technologies
- Acceleration of codes and standards for DER
- Industry education programs, best practice dissemination, etc.

Thank you!

Questions?

Jay Johnson
Renewable and Distributed Systems Integration
Sandia National Laboratories
P.O. Box 5800 MS1033
Albuquerque, NM 87185-1033
Phone: 505-284-9586
jjohns2@sandia.gov