USEA
United States Energy Association

USAID
FROM THE AMERICAN PEOPLE

NREL
Transforming ENERGY

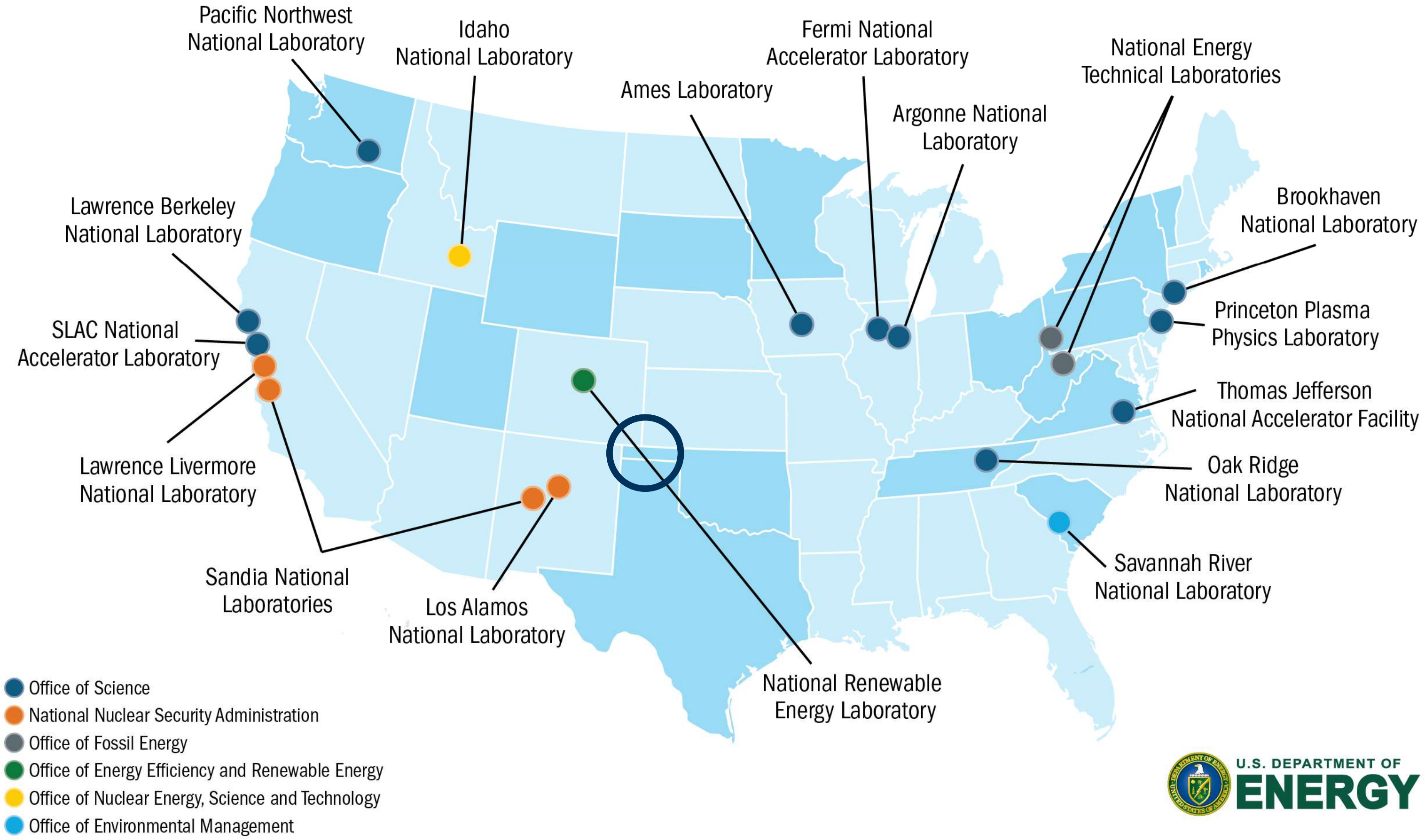
Power Sector Cybersecurity Building Blocks: Getting Started

Sept. 14, 2021

Maurice Martin

- National Renewable Energy Laboratory
- 13 years technology research for the electric utility industry
- Focus on impact analysis and experiment design
- Extensive experience working with small and under-resourced utilities on their cybersecurity challenges

Department of Energy National Laboratories


Pacific Northwest National Laboratory
Idaho National Laboratory
Ames Laboratory
Fermi National Accelerator Laboratory
Argonne National Laboratory
National Energy Technical Laboratories
Brookhaven National Laboratory
Lawrence Berkeley National Laboratory
SLAC National Accelerator Laboratory
Princeton Plasma Physics Laboratory
Thomas Jefferson National Accelerator Facility
Oak Ridge National Laboratory
Lawrence Livermore National Laboratory
Savannah River National Laboratory
Sandia National Laboratories
Los Alamos National Laboratory
National Renewable Energy Laboratory
● Office of Science
● National Nuclear Security Administration
● Office of Fossil Energy
● Office of Energy Efficiency and Renewable Energy
● Office of Nuclear Energy, Science and Technology
● Office of Environmental Management

U.S. DEPARTMENT OF ENERGY

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

CARILEC An Association Of Electric Energy Solution Providers

NREL Science Drives Innovation

Renewable Power

Solar

Wind

Water

Geothermal

Sustainable Transportation

Bioenergy

Vehicle Technologies

Hydrogen

Energy Efficiency

Buildings

Advanced Manufacturing

Government Energy Management

Energy Systems Integration

Grid Integration

Hybrid Systems

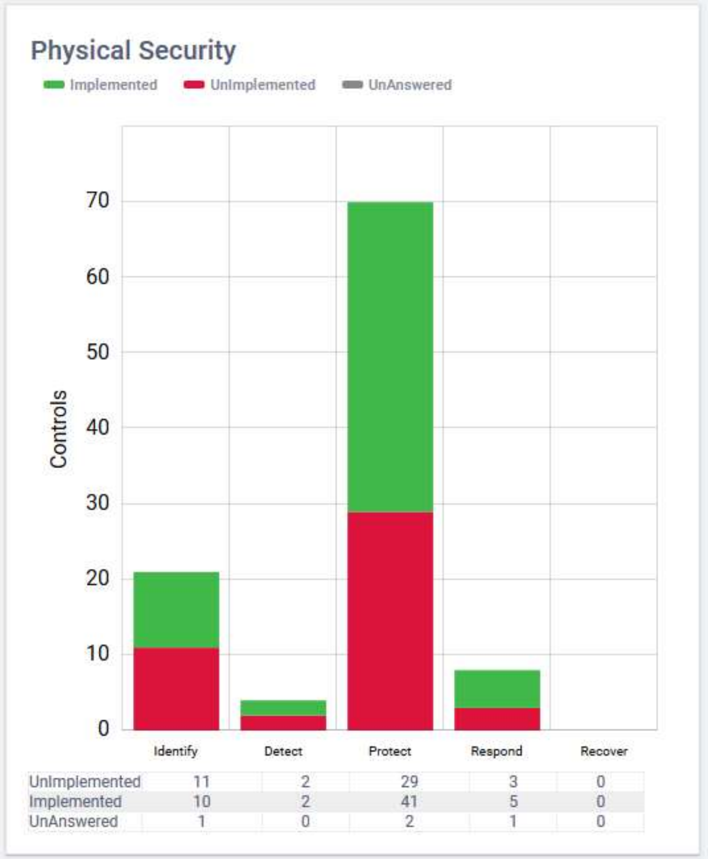
Energy Security and Resilience

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

CARILEC An Association Of Electric Energy Solution Providers

Based on Past Research…



	Identify	Detect	Protect	Respond	Recover
UnImplemented	11	2	29	3	0
Implemented	10	2	41	5	0
UnAnswered	1	0	2	1	0

Sample results from the DERCF cybersecurity assessment tool, https://dercf.nrel.gov

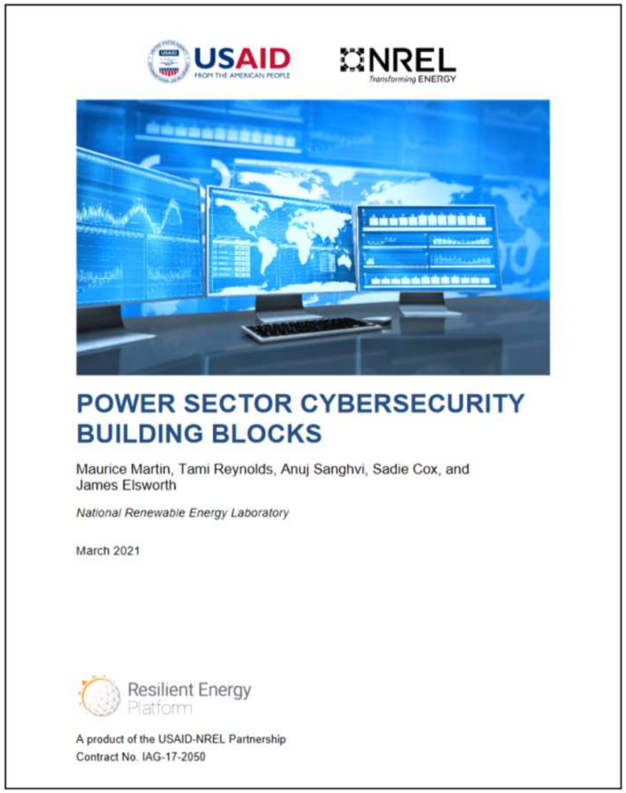
Utility cybersecurity program resources are often allocated unevenly. Some areas are under built, some are overbuilt.

This is especially true for small utilities that struggle for resources.

How can we address that problem?

Power Sector Cybersecurity Building Blocks

Building Blocks: Description



POWER SECTOR CYBERSECURITY BUILDING BLOCKS

Maurice Martin, Tami Reynolds, Anuj Sanghvi, Sadie Cox, and James Elsworth

National Renewable Energy Laboratory

March 2021

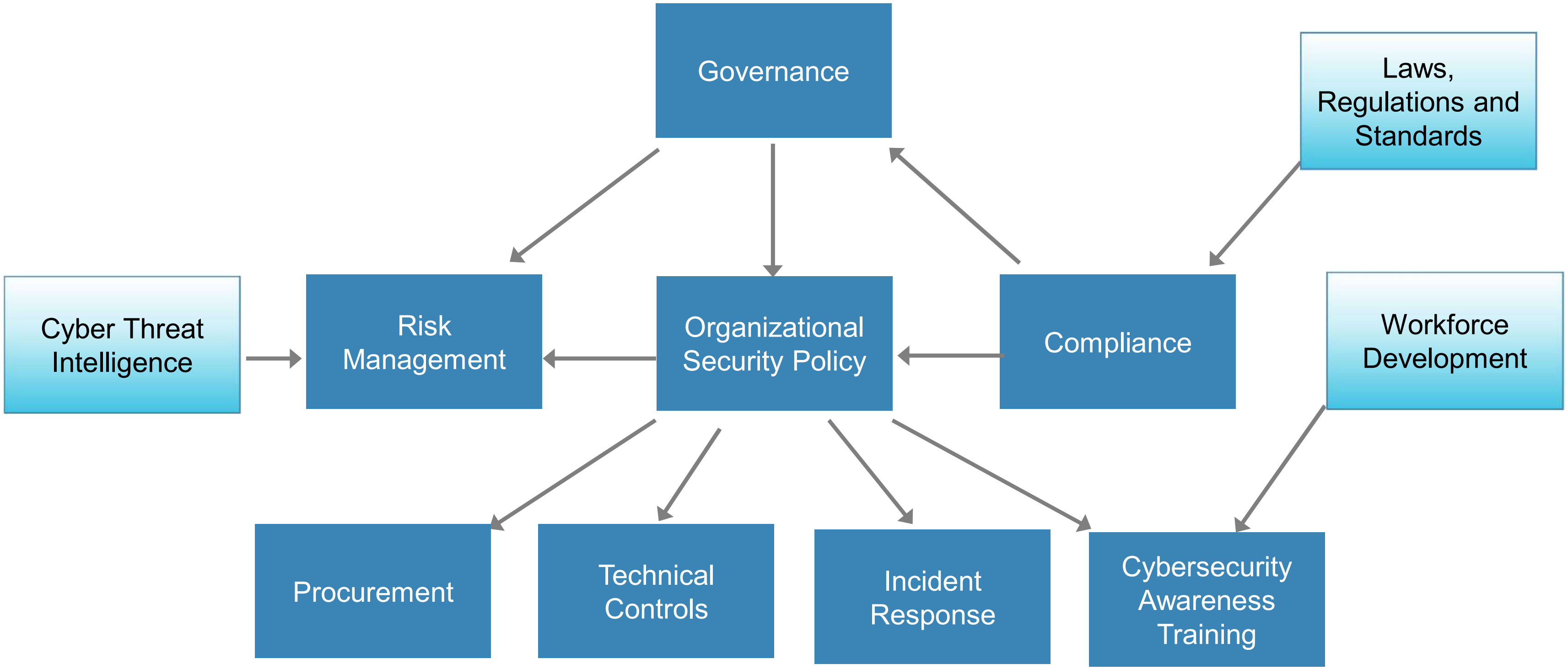
Resilient Energy Platform

A product of the USAID-NREL Partnership
Contract No. IAG-17-2050

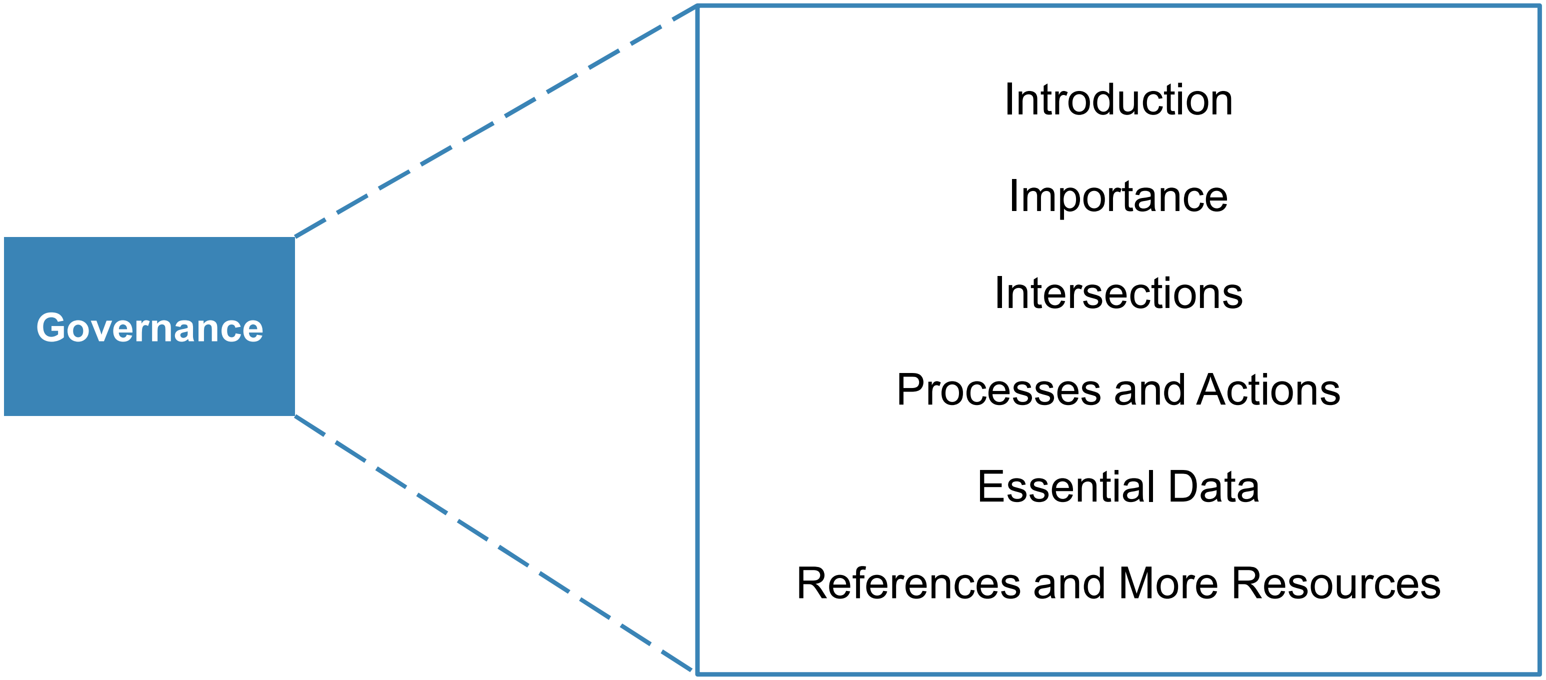
Read the full report at:
https://resilient-energy.org/cyber

- Clusters of related activities that support a well-rounded cyber program
- Encourage utilities to think about different areas of cybersecurity
- Draw from established best practices
- Span multiple stakeholders
- Interconnected & mutually supporting
- Not the last word!

Building Blocks: Structure


Governance
Laws, Regulations and Standards
Cyber Threat Intelligence
Risk Management
Organizational Security Policy
Compliance
Workforce Development
Procurement
Technical Controls
Incident Response
Cybersecurity Awareness Training

Within Each Building Block



Governance

Introduction

Importance

Intersections

Processes and Actions

Essential Data

References and More Resources

Where to Start?

Governance

Incident Response

Cybersecurity Awareness Training

Building Block: Governance

PHOTO FROM ISTOCK 1167131951

"The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk."

NIST *Framework for Improving Critical Infrastructure Cybersecurity*

Unique Activities

Resilient Energy Platform

Focus on Oversight:

- Prioritizing business requirements and risk objectives
- Reviewing organizational security policy
- Monitoring compliance
- Fostering a culture of cybersecurity
- Assigning roles and responsibilities
- Resource allocation
- Monitoring progress of the cybersecurity program

PHOTO FROM ISTOCK 1174366497

USAID FROM THE AMERICAN PEOPLE NREL Transforming ENERGY CARILEC An Association Of Electric Energy Solution Providers

Governance

The *Building Blocks* document includes references and resources

(examples at right)

- “Five Principles for Stronger Board Oversight of Cybersecurity.” BRINK – News and Insights on Global Risk. https://www.brinknews.com/five-principles-for-stronger-board-oversight-of-cybersecurity/

- *Cyber Security Governance: A Component of MITRE’s Cyber Prep Methodology*. MITRE Corporation. https://www.mitre.org/sites/default/files/pdf/10_3710.pdf

- “Cybersecurity Governance.” Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/cybersecurity-governance

- “Board Directors Need to Get Involved With Cyber Risk Governance.” *Security Intelligence*. https://securityintelligence.com/board-directors-need-to-get-involved-with-cyber-risk-governance/

Building Block: Incident Response

The actions taken by an organization to prepare for and respond to a cyberattack constitute incident response.

We can never be 100% secure, only 100% ready.

- Operational technologies are susceptible to cyber attack.
- Are you prepared if the critical assets are compromised? – Plan ahead!
- The organization is only as strong as the weakest link. (Staff/Group/Team)
- Embed cybersecurity in the work culture.

FROM ISTOCK 105607208

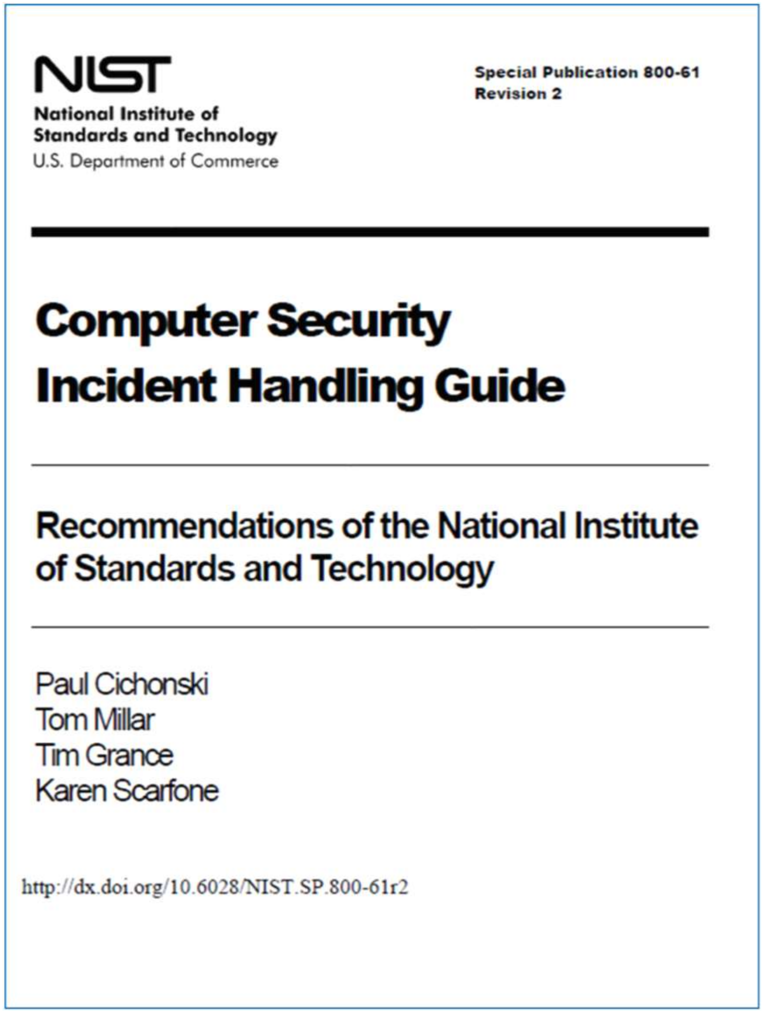
Incident Response Plan

- Driven by overall cybersecurity policy
- Resonates with applicable laws, regulations, and standards
  - *Notification/disclosure laws, privacy laws, compliance laws, reporting laws(?), other related laws*
- Identification of:
  - *Terms related to an incident*
  - *Appropriate roles and responsibilities for respective functions*
  - *Dependent operations*
  - *Standards and guidance documentation*
- Stakeholder identification and engagement
- Resilience and restoration
- Prioritization of mission critical assets
- Frequent and periodic updates and revisions

FROM ISTOCK 1157430519

Cybersecurity Incident Response

Sample Resource



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

Building Block: Cybersecurity Awareness Training

- Staff are the first and last line of defense
- Saves time, resources, and reputation
- 81% of data breaches are caused by stolen login credentials
- Average breach costs an organization $3.8M
- Critical infrastructure depends on informed employees to help manage risk

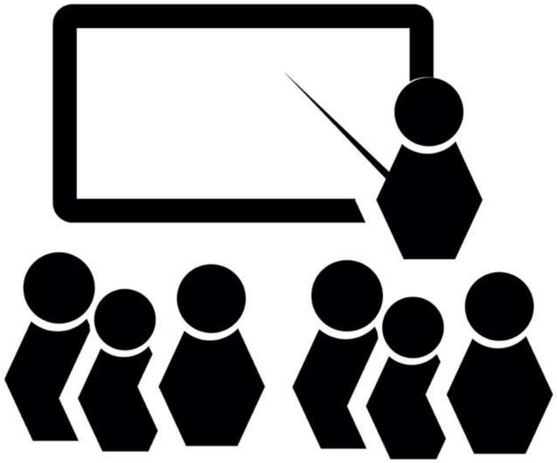
FROM ISTOCK 1204266239

Creating a Culture of Cybersecurity

Resilient Energy Platform

Annual Cybersecurity Awareness Campaign

- Mandatory training videos with knowledge tests
  - Must score 80% or higher, retake test until achieved
- Accountability structure in place
  - Needs manager sign off
- Internal phishing campaigns
  - Testing staff readiness and awareness
  - Free lunch party for the group with the best scores or has the training completed by the designated date
- Marketing campaign throughout entire organization
  - Hang posters
  - Create fun games – treasurer hunts, crossword puzzles, word searches, trivia



USAID FROM THE AMERICAN PEOPLE NREL Transforming ENERGY CARILEC An Association Of Electric Energy Solution Providers

Cybersecurity Awareness Training

The *Building Blocks* document includes references and resources

(examples at right)

- "Seven Tips For A Successful Security Awareness Training Program." *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2019/08/16/seven-tips-for-a-successful-security-awareness-training-program/

- "First Line of Defense: Are Humans Doing a Good Enough Job?" *InfoSecurity Professional*. https://blog.isc2.org/isc2_blog/2020/05/the-first-line-of-defense-are-humans-doing-a-good-enough-job.html

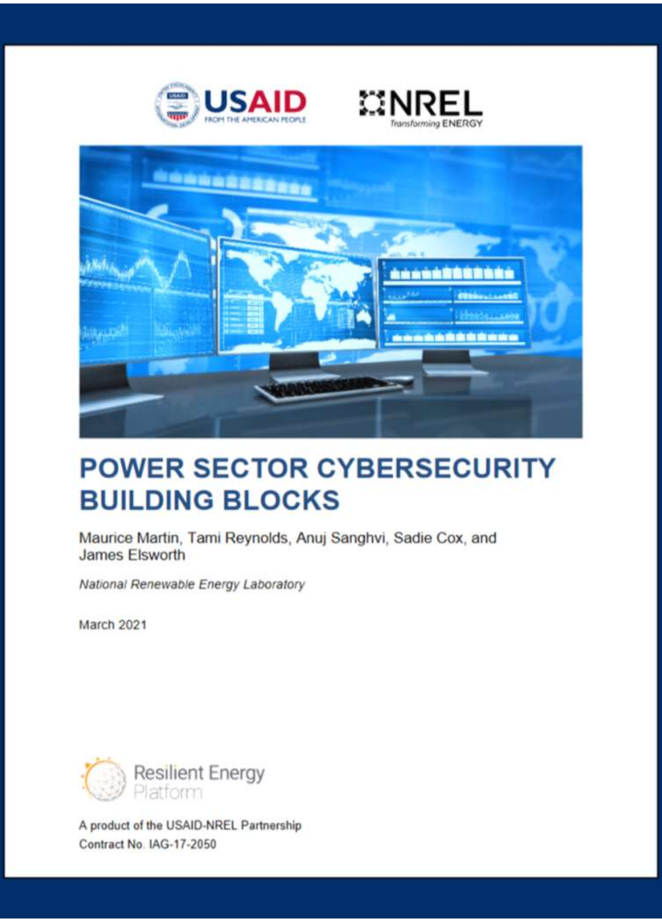
- *Best Practices for Protecting Against Phishing, Ransomware, and Email Fraud*. Osterman Research. 2018. https://www.knowbe4.com/hubfs/Best_Practices_for_Protecting_Against_Phishing_Ransomware_and_Email_Fraud.pdf?hsCtaTracking=67a14d06-dd12-49c7-8070-93fa017a2729%7C082896ec-48d5-4248-b50b-a38e0076ee1a

Power Sector Cybersecurity Building Blocks

Free Resources, Available Now

Available at: https://resilient-energy.org/cyber

Contact: Maurice.Martin@nrel.gov



POWER SECTOR CYBERSECURITY BUILDING BLOCKS

Maurice Martin, Tami Reynolds, Anuj Sanghvi, Sadie Cox, and James Elsworth

National Renewable Energy Laboratory

March 2021

A product of the USAID-NREL Partnership
Contract No. IAG-17-2050

Thank You!

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

CARILEC An Association Of Electric Energy Solution Providers

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.