USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

CARILEC An Association Of Electric Energy Solution Providers

Cybersecurity Awareness Training:
A Building Block for Power Sector Cybersecurity

May 26, 2021

Housekeeping-Zoom

Welcome to our webinar! Here are a few notes about using Zoom:

- You will be **automatically muted** upon joining and throughout the webinar
- Please add comments or ask questions in the **chat box**
- You can adjust your audio through the **audio settings**
- If you have **technical issues**, please send a message directly to Britton Marchese
- To **mute** or **unmute** yourself (during the Q&A portion), use the microphone icon

Mansfield Blackwood
Partner Country Systems (G2G) Advisor
USAID

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, and
- 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

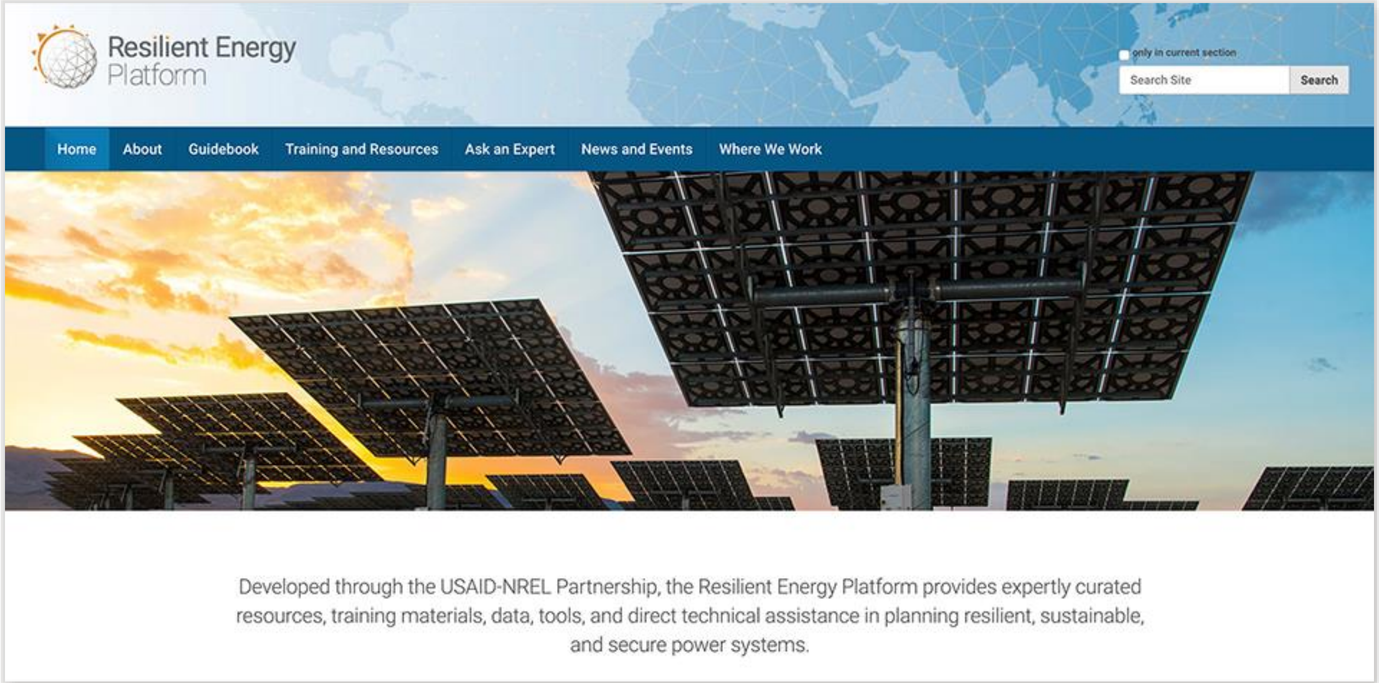
www.i-jedi.org

www.resilient-energy.org

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 Resilient Energy Platform enables decision makers to **assess power sector vulnerabilities**, **identify resilience solutions**, and **make informed decisions** to enhance power sector resilience at all scales.



Developed through the USAID-NREL Partnership, the Resilient Energy Platform provides expertly curated resources, training materials, data, tools, and direct technical assistance in planning resilient, sustainable, and secure power systems.

www.resilient-energy.org

Dr. Cletus Bertin
Executive Director
CARILEC

Cybersecurity Awareness Training Presenter

Tami Reynolds

- National Renewable Energy Laboratory
- 6 years cybersecurity research in the electric sector
- Technical lead on the Distributed Energy Resources Cybersecurity Framework (DER-CF)
- Conducts cyber-governance assessments in the electric utility sector based on DOE’s C2M2 and the NIST Cybersecurity Framework

Agenda

- Building Block Overview
- Why is cybersecurity awareness training important?
- Cybersecurity Awareness Training Building Block Intersections
- Setting Up a Cybersecurity Awareness Program
- All staff training exercises
- Creating a culture
- Different metrics: frequency, cost and measuring successes and failures
- Data
- Resources

FROM ISTOCK 1211806047

Power Sector Cybersecurity Building Blocks

Impacts of a Cyber Attack

For all types of business…

- Deleted data — cost to restore
- Theft of sensitive data (e.g., customer records, employee records, trade secrets) — credit monitoring, fines, loss of revenue
- Reputational damage (consumers, regulators, investors, others)
- Loss of productivity
- Ransomware — cost to restore…or pay the ransom!

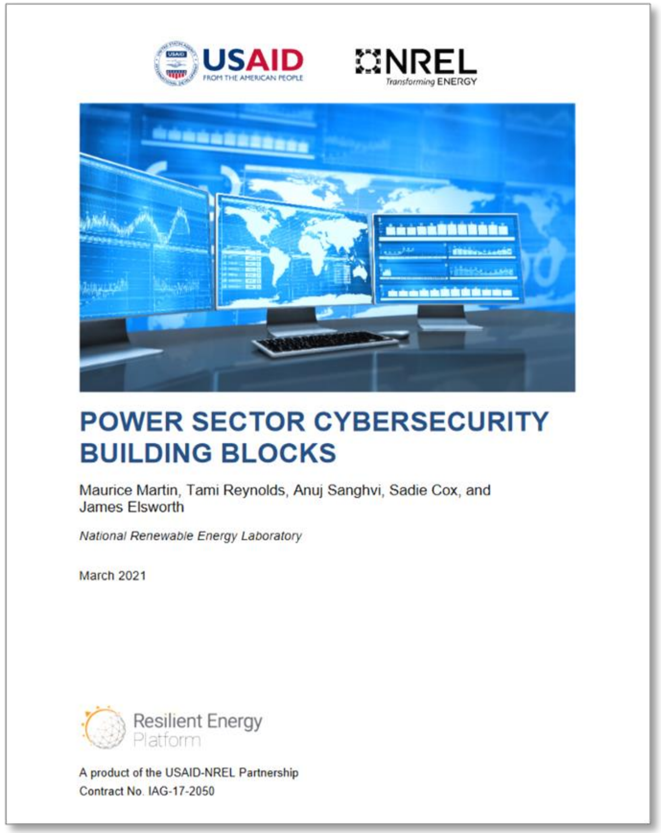
For utilities, all the above plus *cyber-physical* consequences…

- Safety concerns
- Interrupted service
- Damaged/destroyed physical assets — cost to repair/replace

FROM ISTOCK 11144604245

Building Blocks: Description

- 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!



USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

POWER SECTOR CYBERSECURITY BUILDING BLOCKS

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

National Renewable Energy Laboratory

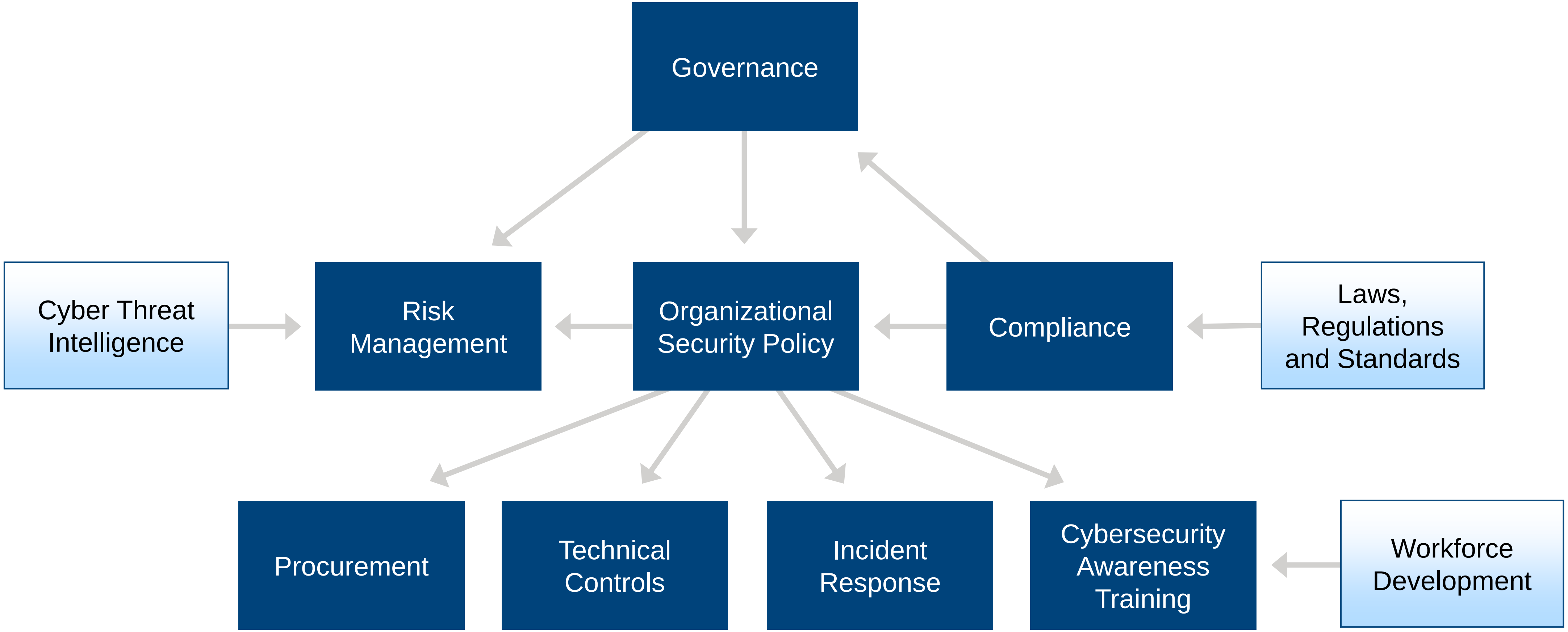
March 2021

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

Building Blocks: Structure



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

Cybersecurity Awareness Training

Building a Cybersecurity Awareness Program

“You are an essential ingredient in our ongoing effort to reduce Security Risk.”
— Kirsten Manthorne

“The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: "Cybersecurity is much more than an IT topic.”
— Stephane Nappo

FROM ISTOCK1167131951

Why is cybersecurity awareness training important?

Human mistakes:

- Phishing attempts
- USB devices
- Insecure WiFi Networks
- Security hygiene – password sharing, device sharing
- Online safety-visiting unsafe websites
- Human error-misconfiguration

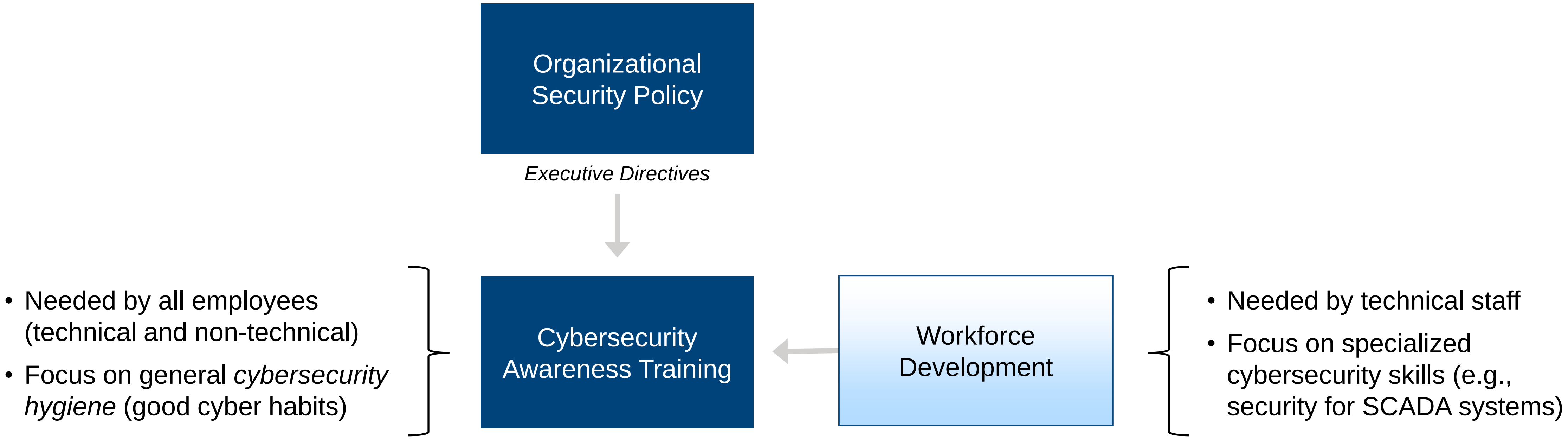
FROM ISTOCK 526555752

Why is cybersecurity awareness training important?

- 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

Cybersecurity Awareness Training Building Block



Organizational Security Policy

Executive Directives

- Needed by all employees (technical and non-technical)
- Focus on general *cybersecurity hygiene* (good cyber habits)

Cybersecurity Awareness Training

Workforce Development

- Needed by technical staff
- Focus on specialized cybersecurity skills (e.g., security for SCADA systems)

Workforce Development Intersects Building Block

- Advanced skills for technical staff that can mentor and monitor non-technical staff
- Provide internal workforce incentives for advancing education in cybersecurity
  - Financial reimbursement for college level courses
- Work with government agencies to help create incentive programs (STEM) for recruiting graduates

FROM ISTOCK 905106562

Intersection with Organizational Security Policy Building Block

Also known as organizational policy or master security policy

- Captures the executive directives on cybersecurity
- Elaborates on these directives and includes specific guidance on implementation
- The “go to” document for a utility’s cyber program
- Can be one big document, or reference smaller, “issue-specific” policies. Examples:
  - Data breach response policy
  - Internet usage policy
  - Remote access policy

FROM ISTOCK 905106562

Processes and Actions

Process and Actions

Setting up a Cybersecurity Awareness Program

- Understand and align with mission and vision of the organization
- Identify Key Stakeholders and Assign Roles and Responsibilities
- Who needs training?

FROM ISTOCK 1287662408

Setting Up a Cybersecurity Awareness Program

Understand and align with mission and vision of the organization

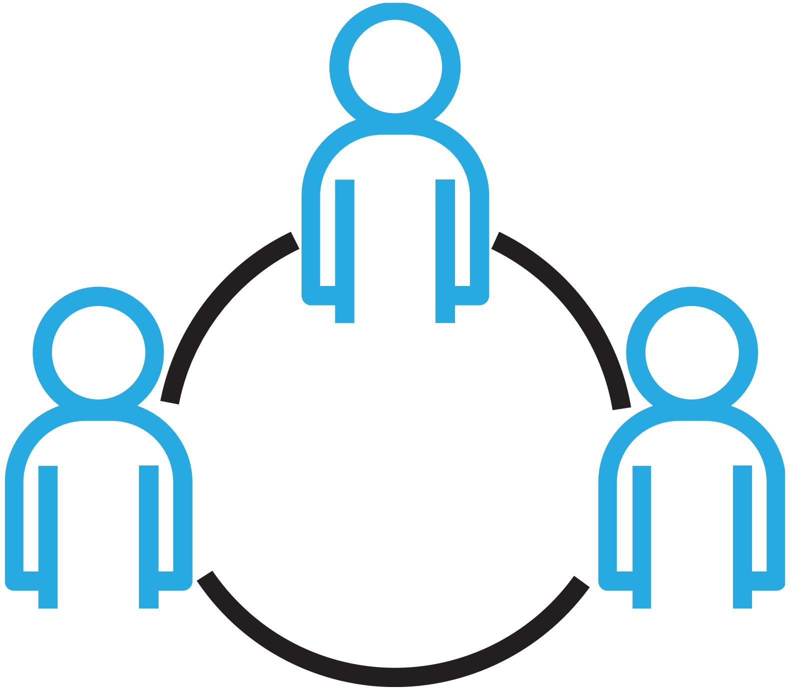
- What are your cybersecurity policies and procedures
- Evaluate your weak points
- Know your own risks

FROM ISTOCK 1174366497

Setting Up a Cybersecurity Awareness Program

Identify Key Stakeholders and Assign Roles and Responsibilities

- Get Management buy in
  - – Use internal data on attempts to breach system
  - – Use external information on breaches
    - o Ex: SolarWinds supply chain breach
  - – Use analogies with safety… "build security in" similar to "build safety in"
- Get Employee buy in
  - – explain the importance of secure practices productivity, safety and job protection



Setting Up a Cybersecurity Awareness Program

Who Needs Training?

- EVERYONE!!!- Anyone who has access to a computer or device that connects to the network
- Different training dependent on role and responsibility
- “Train Early, Train Often”

FROM ISTOCK 1291238350

Setting Up a Cybersecurity Awareness Program

Who Needs Training? (continued…)

Those who handle sensitive information

- Data operations
- Personally Identified Information (PII)
- Intellectual property protection
- Financial information
- Trade secrets
- Software licenses
- Network configurations
- NDA’s
- Email security and privacy
- SCADA operations

FROM ISTOCK 1223297685

Setting Up a Cybersecurity Awareness Program

Who Needs Training? (continued…)

IT & OT staff – in depth training of all building blocks:

- Governance
- Risk Management
  - Cyber Threat Intelligence
- Organization Security Policy
- Compliance
  - Laws, Regulations and Standards
- Procurement
- Incident Response
- Technical Controls
  - Network Architecture
  - Pen testing

FROM ISTOCK 1305990986

All Staff Annual Training Exercise

Classes/Workshops

- In person
- Incident response exercise
- Best practices guide
- Mandatory tests

Social Engineering

- Set up a regular phishing campaign
- Rewards for proper usage
- Insider threat awareness and reporting

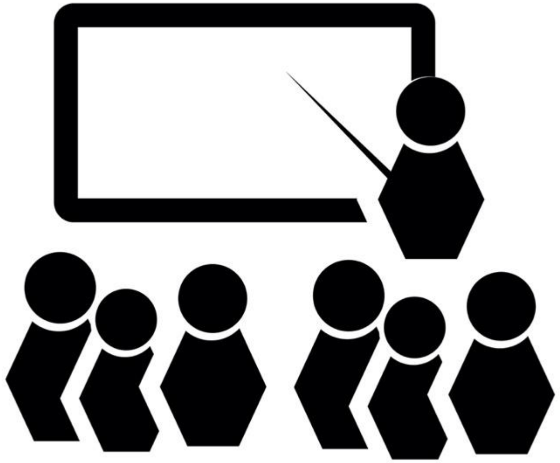
Webinars

- Operating workstation in OT environment
- Understanding of legacy equipment
- Awareness of CIA (availability emphasis)

Creating a Culture of Cybersecurity

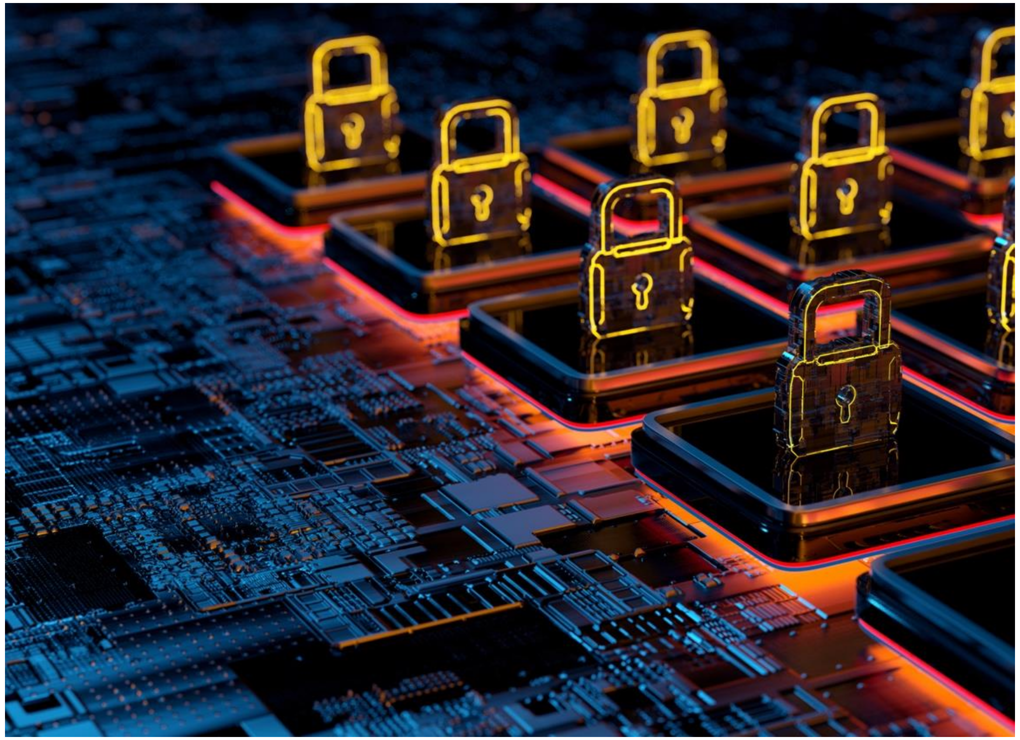
Annual Cybersecurity Awareness Campaign

- Marketing campaign throughout entire organization
  - Hang posters
  - Create fun games – treasurer hunts, crossword puzzles, word searches, trivia
- Mandatory training videos with knowledge tests
  - Must score 80% or higher, retake test until achieved
- Accountability structure in place
  - Needs manager sign off
- Incentives
  - Prizes for not “getting caught in the trap”
    - Free coffee with the CISO or CIO
    - Free lunch party for the team with the best scores or has the training completed by the designated date



Frequency

- How often should Executives get training?
- How often should IT & OT staff get updated training?
- How often should all other staff get training?
- Is there an accountability structure set up to make sure everyone is completing their training?



FROM ISTOCK 1192070289

How much does Cybersecurity Awareness Training Cost?

Resources

- Time
- Staff
- Money

Costs range based on size of organization

- Dependent on level and type of training (e.g. IT, OT, HR, Finance)
- Several free online resources

FROM ISTOCK 1249306214

Metrics: How do you measure successes and failures?

- How many compromised emails reached the users (junk email)
- How many employees clicked on the malicious email
- Did you reduce the amount of resources needed to respond to the event
- Helps determine improvements that need to be made

FROM ISTOCK 1220099714

Essential Data

- For each category of sensitive information, who has access to it?
- How do we track who has access to sensitive information?
- High-level information on risk, threats, and vulnerabilities affecting the utility
- Is there a process for revoking access to sensitive information when the employee no longer needs it or when the employee leaves the organization? Removing all access when someone leaves the organization.

- When terminating someone revoke access immediately
- How sensitive is this information? (What negative impact would arise if it were lost, stolen, or altered by an attacker?)
- What do staff need to know about security for each type of sensitive information and the system that stores it?

Resources

- USAID/-NREL Partnership can help with planning or execution of your cybersecurity awareness training
    - Visit the website at: https://resilient-energy.org/cybersecurity-resilience
    - Read the guidance document: Power Sector Cybersecurity Building Blocks https://www.nrel.gov/docs/fy21osti/79396.pdf
- Free NIST training- https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content
- – Center for Development of Security Excellence Cybersecurity eLearning - *free*
- – Chief Information Security Officer Workshop Training – *free*
- – Critical Knowledge Explorer – *free*
- – CyberTraining 365 Online Academy – *free*

Closing Thoughts

How else can USAID & NREL help?

Presentations for utility:

- Board of directors
- Executives
- Technical staff
- Non-technical staff
- Regulators

New documents

New tools for

- Expanded assessments
- Cybersecurity investment ROI
- Other topics?

One-on-one technical assistance

How else can USAID & NREL help?

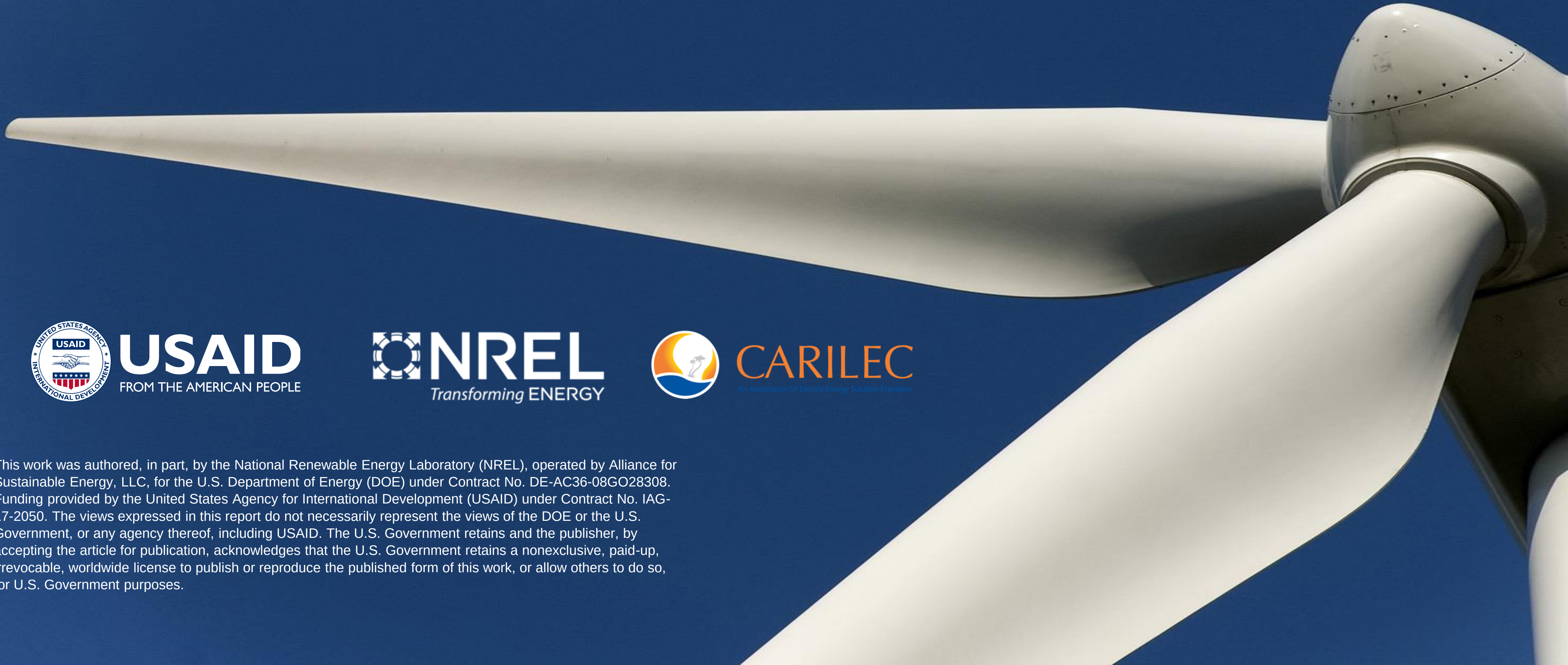
Read the guidance document: *Power Sector Cybersecurity Building Blocks* report available at: https://resilient-energy.org/cyber

Contact Us:
Maurice.Martin@nrel.gov,
Tami.Reynolds@nrel.gov

Upcoming Webinars in this Series:

- July 2021: Incident Response
- September 2021: Technical Controls (focus on SCADA network security)
- November 2021: Regulatory Compliance
- January 2022: Risk Management
- March 2022: IT Network Security

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.