Building Blocks to Support Cybersecurity in the Power Sector

June 25, 2020

Housekeeping Items

- Listen through your computer.
  - Please select the “microphone and speakers” button on the right-hand audio pane display.
- Listen by telephone.
  - Please select the “telephone” option in the right-hand display, and a phone number and pin will display.
- Technical difficulties:
  - Contact the GoToWebinar Help Desk: 1-888-259-8414

www.nrel.gov/usaid-partnership

Housekeeping Items

- To ask a question
  - Select the ‘Questions’ pane on your screen and type in your question.
- Share with others or watch it again
  - A video/audio recording of this webinar and the slide decks will be emailed to all attendees shortly after the webinar has concluded.
- Recordings are also available on the USAID-NREL Partnership Learning Channel playlist on YouTube
  - https://www.youtube.com/playlist?list=PLmIn8Hncs7bEWpXMKTzTf3lzlx6kBp2a0

www.nrel.gov/usaid-partnership

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.
- 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

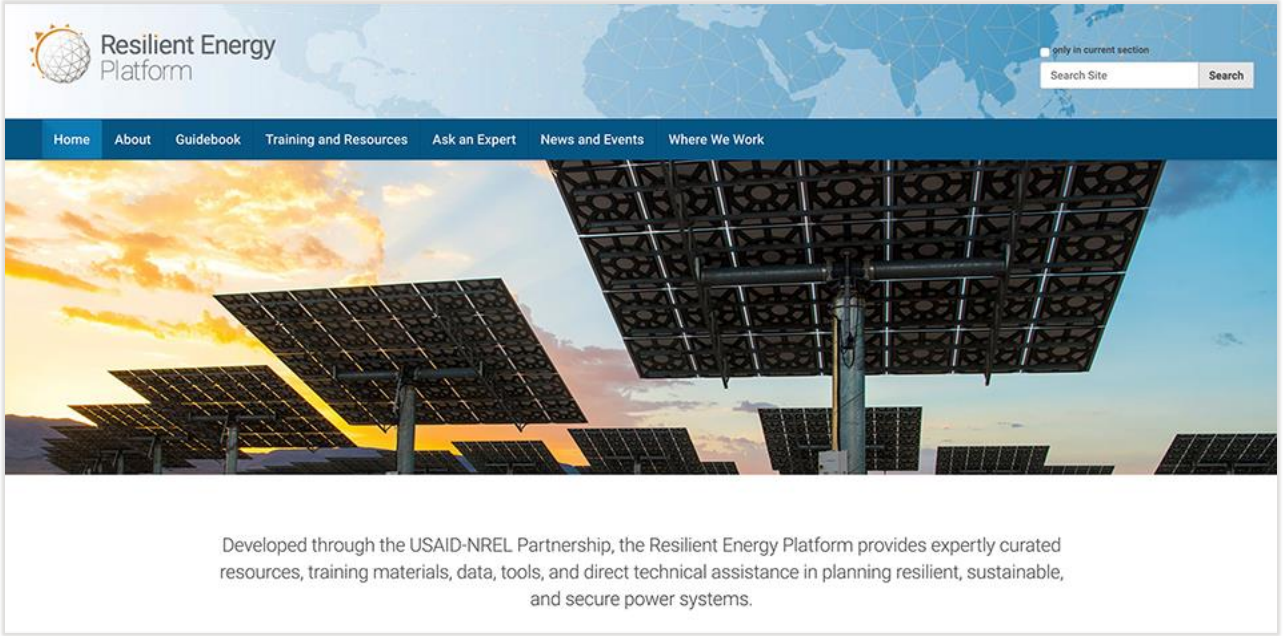
USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

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



www.resilient-energy.org

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Agenda

Opening
Jeremy Foster

Senior Energy Advisor,

USAID

Webinar Series Introduction
Jamila Amodeo

Senior Energy Advisor,

USAID

Building Blocks
Maurice Martin

Senior Cybersecurity Research Leader,

National Renewable Energy Laboratory

Q&A
James Elsworth

Research Engineer,

National Renewable Energy Laboratory

USAID Support Approach for Cyber Security

Jamila Amodeo
Senior Energy Advisor,
USAID

Resilient Energy Platform

Building Blocks to Support Cybersecurity in the Power Sector

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

About Maurice Martin

- National Renewable Energy Laboratory
- 12 years technology research for the electric utility industry
- Focus on security architectures for complex systems
- Previous work focused on small and under-resourced utilities and their cybersecurity challenges

Impacts of cyber attack

Resilient Energy Platform

For all types of business…

- Deleted data -- cost to restore
- Ransomware -- cost to restore…or pay the ransom!
- 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

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

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

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Elements necessary to ensure cybersecurity for the power sector

Resilient Energy Platform

Objectives for cyber "building blocks":

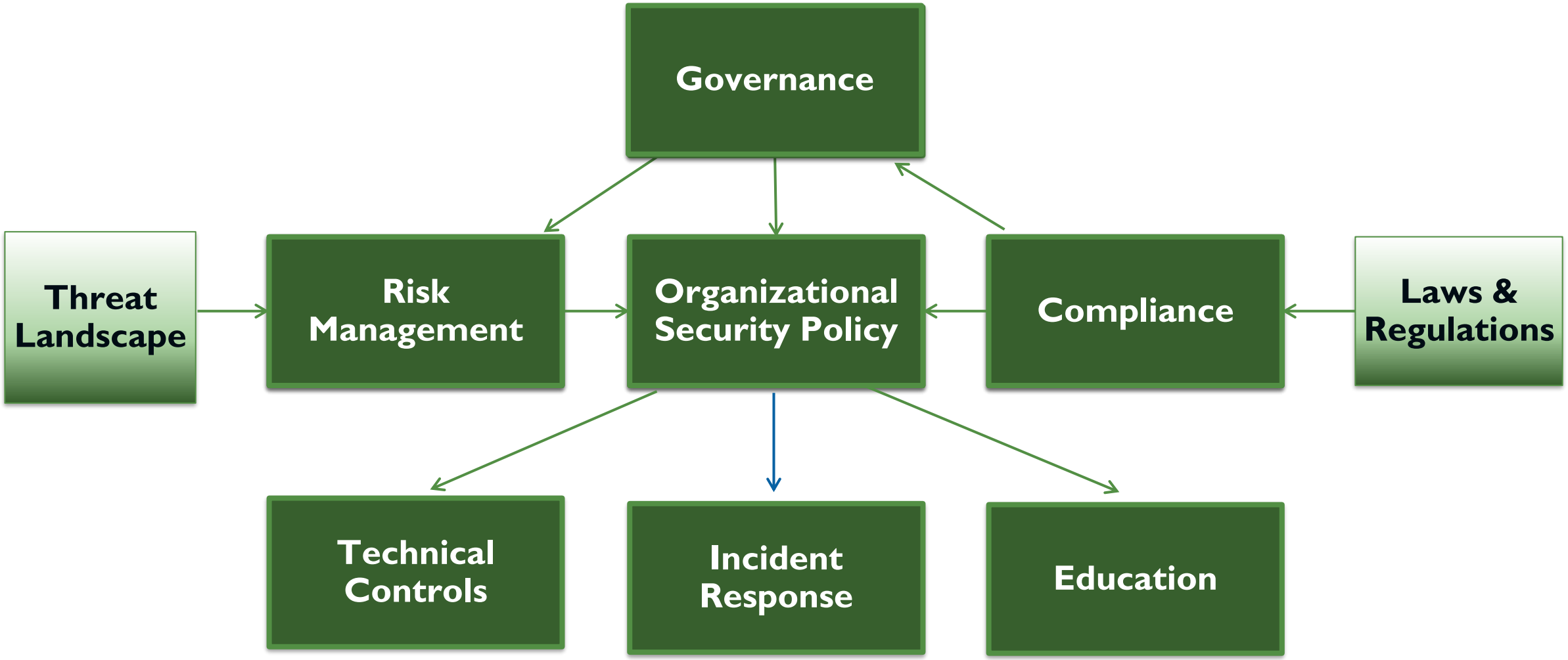
- Serve as an introduction
- Span multiple stakeholders
- Interconnected & mutually supporting
- Not the last word!

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

The Building Blocks

Resilient Energy Platform

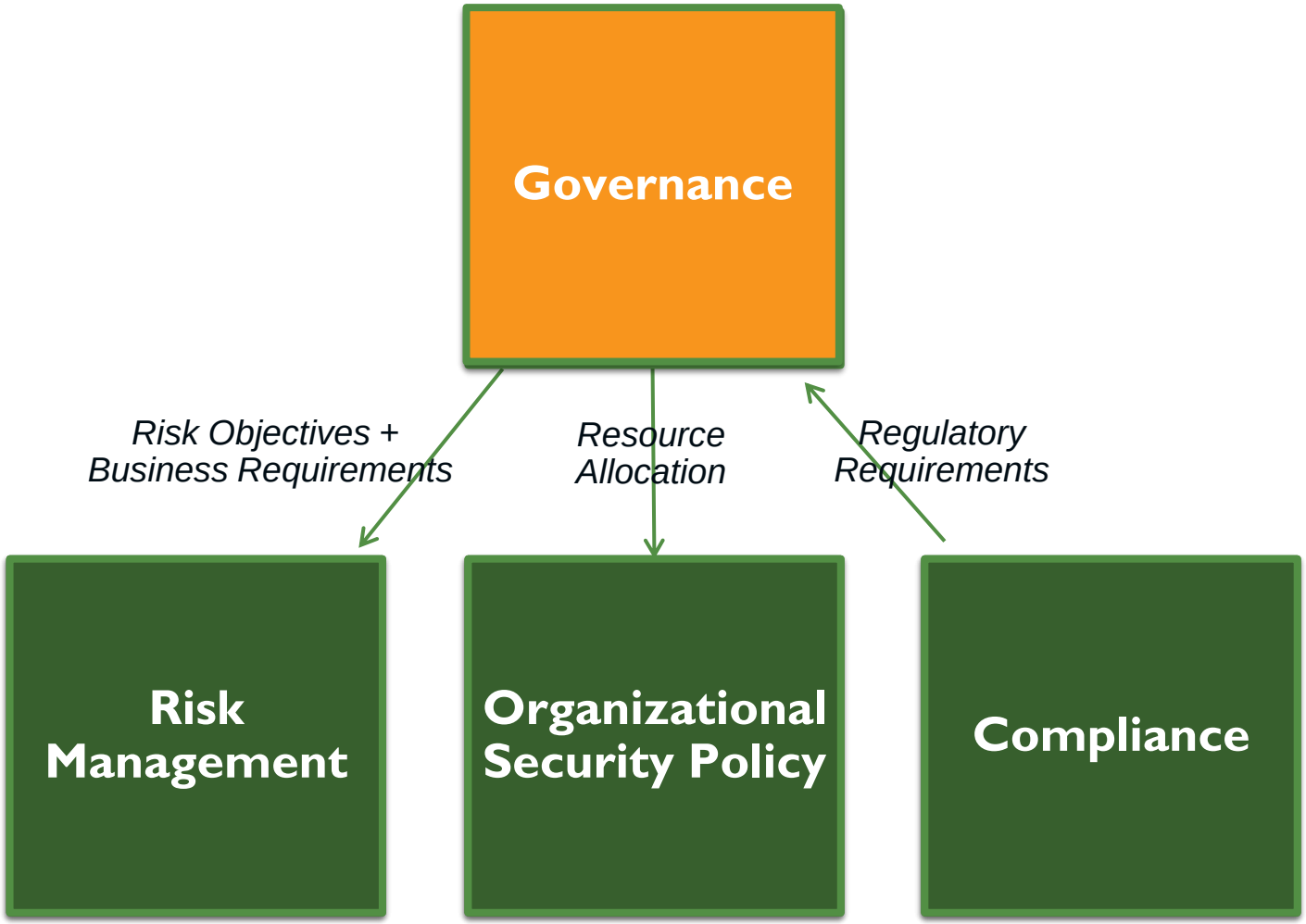


USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Governance

- **Importance:**
  Leadership buy-in
- **Touchpoints:**
  Objectives, Requirements, & Resources
- **Processes and actions:**
  - Establish and communicate policy
  - Assign roles and responsibilities
  - Review legal and regulatory requirements



Organizational Security Policy

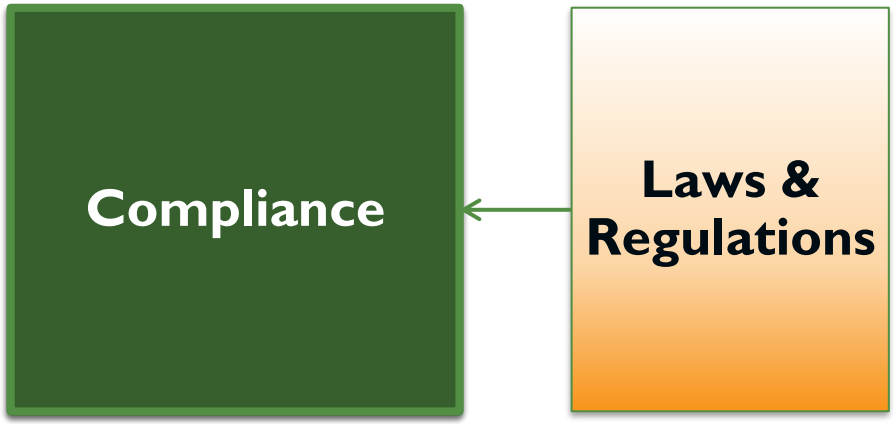
- **Importance:**
  Captures the utility's approach to cyber
- **Touchpoints:**
  Resources & Objectives
- **Processes and actions:**
  - Create the policy
  - Vet the policy
  - Review and update periodically

Laws & Regulations

- **Importance:**
  Defines a cybersecurity strategy for the power system on a national level

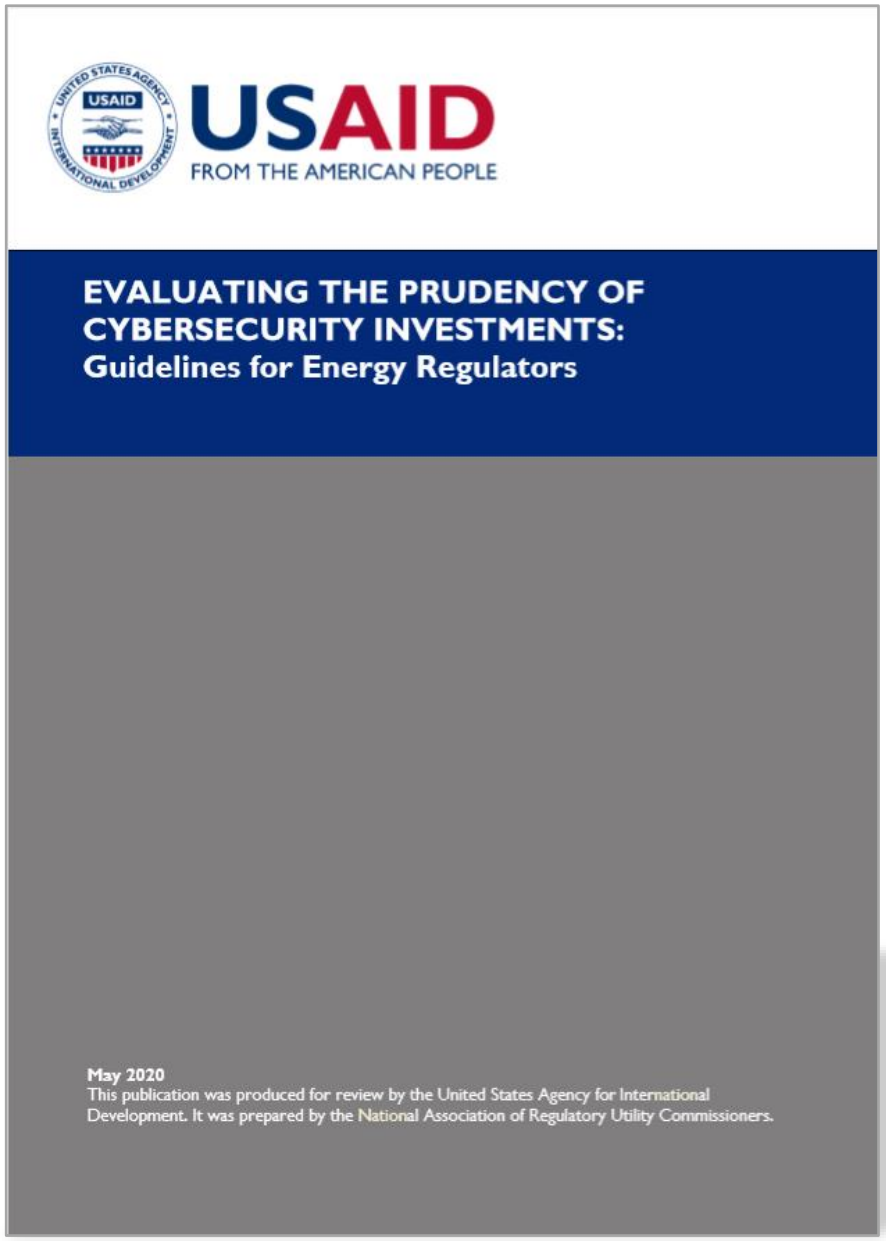
- **Touchpoints:**
  Objectives for the electricity sector in line with the overall national strategy

- **Processes and actions:**
  - Pass laws that reflect national priorities
  - Define regulatory objectives that support the intent of the relevant laws
  - Define indicators & procedures to calculate the indicators
  - Perform controls and inspections
  - Schedule updates



Resource

- Approaches to creating a regulatory framework for cybersecurity
- Cost identification and benchmarking
- Effectiveness metrics
- Regulatory principles and tools



USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Unexpected Quote*:

Utility Cybersecurity Manager:

"Without regulations, I wouldn't have a cybersecurity budget."

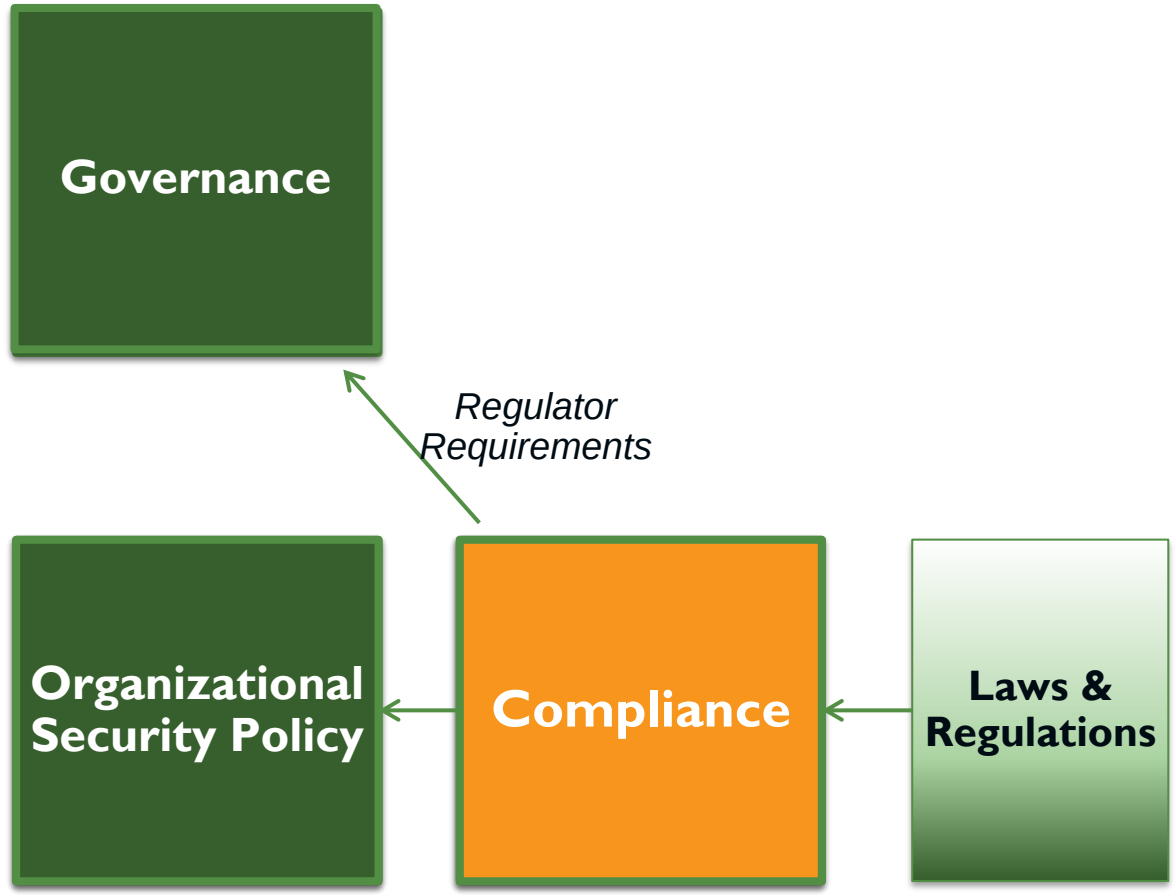
*paraphrased

Compliance

- **Importance:**
  The utility's effort to meet regulatory expectation

- **Touchpoints:**
  Regulatory requirements in the context of the specific utility (for Governance, high-level)

- **Processes and actions:**
  - Identify all laws and regulations that apply
  - Select a security framework
  - Select risk methodology
  - Determine control objectives
  - Document compliance



Compliance vs. Security

Compliance means you've reduced SOME risk.

Residual risk remains.

What is your organization's risk tolerance?

Remember these?

- Deleted data
- Ransomware
- Theft of sensitive information
- Reputational damage
- Loss of productivity
- Safety concerns
- Interrupted service
- Damaged/destroyed physical assets

They can still happen even if you comply with all applicable regulations.

USAID FROM THE AMERICAN PEOPLE

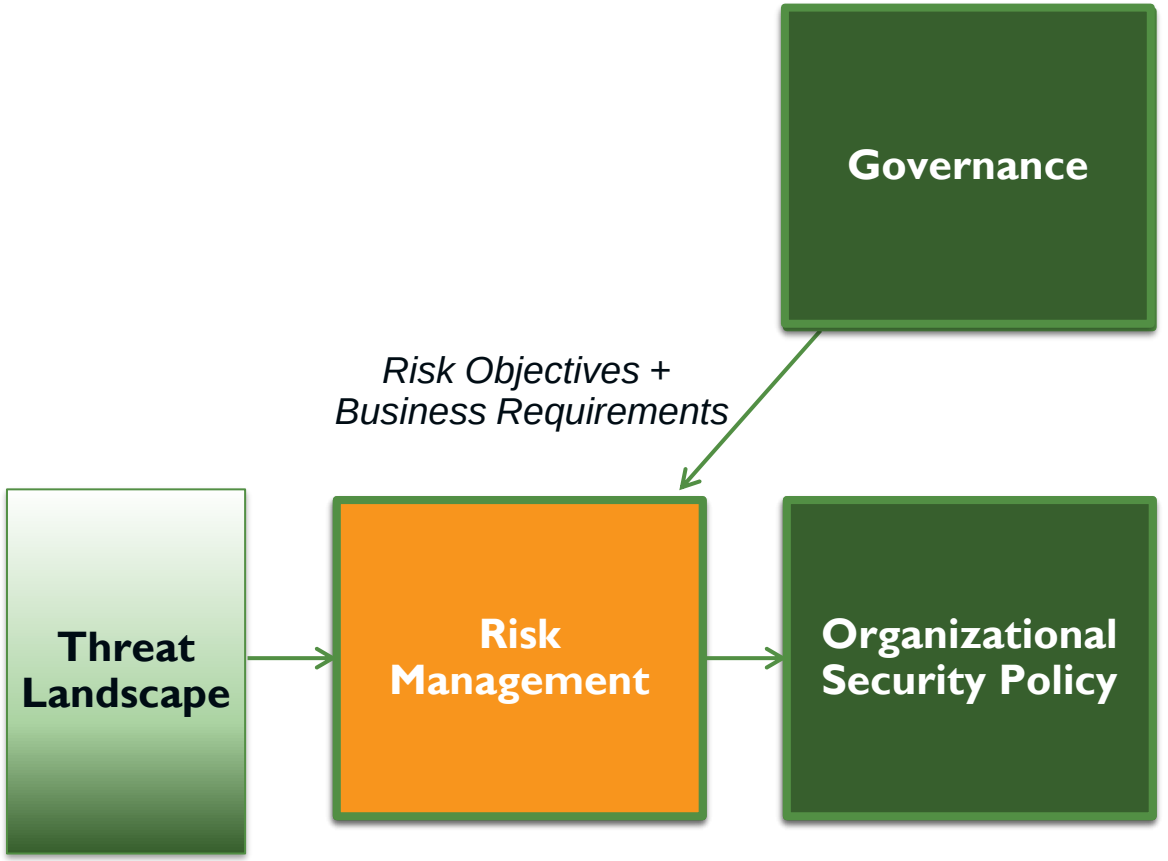
NREL Transforming ENERGY

Risk Management

- **Importance:**
  Balances business objectives against potential threats to define acceptable risk

- **Touchpoints:**
  Factors in resources of attackers, your assets, impact of attacks, and risk objectives

- **Processes and actions:**
  Frame risk, assess risk, respond to risk, monitor risk



Business Impact Analysis (BIA)

Part of the “assess risk” process

How much damage could a cyber attack do?

Classify criticality of business functions, assign value to assets, etc.

BIA Steps*:

1. Select individuals for data gathering
2. Create data-gathering tools
3. Identify the company’s critical business functions
4. Identify the resources these functions depend upon
5. Calculate how long these functions can survive without these resources
6. Identify vulnerabilities and threats to these functions
7. Calculate risk for each different business functions
8. Document findings and report to management

* Adapted from *All-in-One CISSP (7th edition)* by Shon Harris and Fernando Maymi

USAID FROM THE AMERICAN PEOPLE

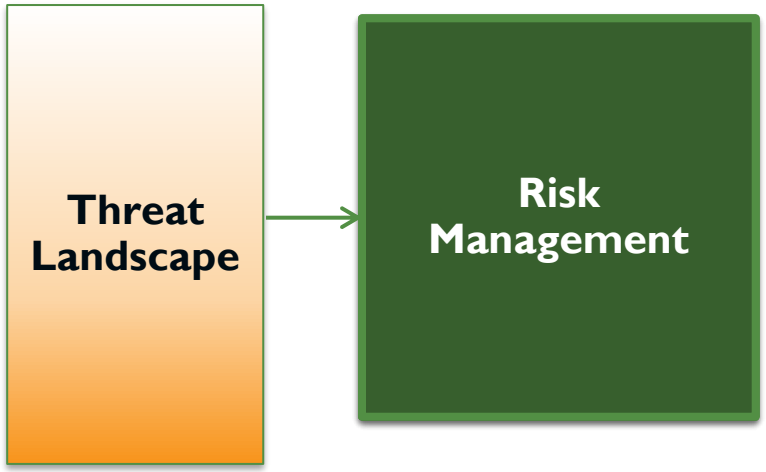
NREL Transforming ENERGY

Threat Landscape

- **Importance:**
  Need to understand who might attack you and what tools and resources they might use

- **Touchpoints:**
  Provides information for informed decisions on risk investments

- **Processes and actions:**
  - Gather information on hostile groups who may be interested in disrupting the electrical grid and their cyber capabilities
  - Identify sources of cyber threat intelligence (CTI) relevant to your organization
  - Establish relationships with government agencies and law enforcement that may have in interest in sharing information.
  - Assign responsibility for monitoring CTI and formulating appropriate responses



Sources of Cyber Threat Intelligence (CTI)

Free vs.
paid subscription?

Non-profit vs.
government agency vs.
private company?

General vs.
specific to electric sector
(or ICS)?

Examples (not endorsements…)

1. **Spamhaus Project** (www.spamhaus.org)
   - International non-profit, Switzerland-based
   - General CTI
   - Free public service (with some restrictions)
2. **SANS Internet Storm Center** (isc.sans.edu)
   - Private company (SANS Institute)
   - General CTI
   - Free public service
3. **ICS-CERT** (www.us-cert.gov/ics)
   - U.S. government program
   - CTI specific to industrial control systems
   - Free public service
4. **RSA** (www.rsa.com)
   - Private company
   - Sector specific with automated segmentation
   - Paid subscription
5. **National Council of ISACS** (www.nationalisacs.org)
   - Coordinator for 20 individual ISACS (Information Sharing and Analysis Centers)
   - Each ISAC is sector-specific (e.g., Electricity ISAC)
   - Some ISACS free, other membership based

USAID FROM THE AMERICAN PEOPLE

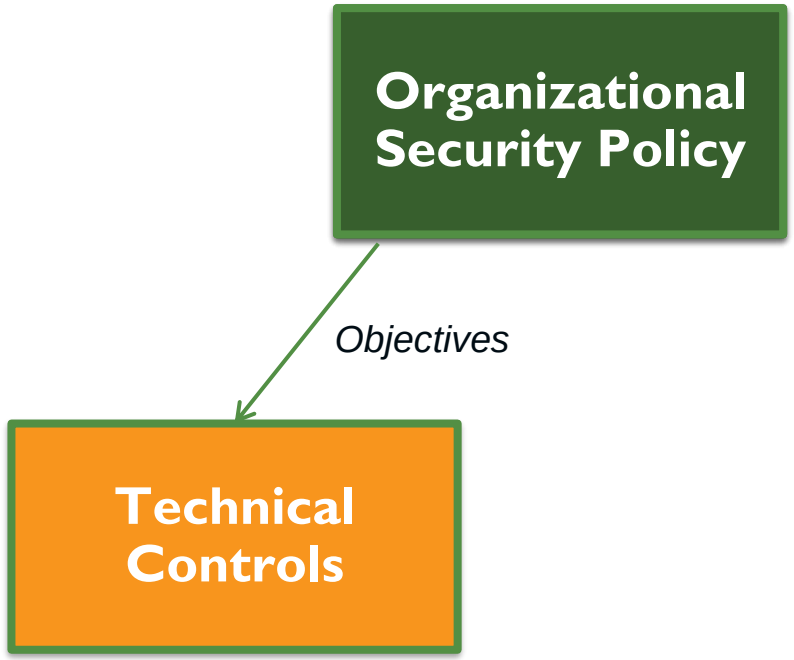
NREL Transforming ENERGY

Technical Controls

- **Importance:**
  These technologies form the front line of cyber defense (e.g., firewalls, access control, intrusion detection, etc.)

- **Touchpoints:**
  Objectives from the organizational security policy

- **Processes and actions:**
  - Decide on a security architecture (including standards)
  - Select categories of controls
  - Select vendors
  - Secure procurement
  - Installation, operation, and updating



Incident Response

- **Importance:**
  Must prepare in advance for a cyber attack

- **Touchpoints:**
  Objectives from the organizational security policy

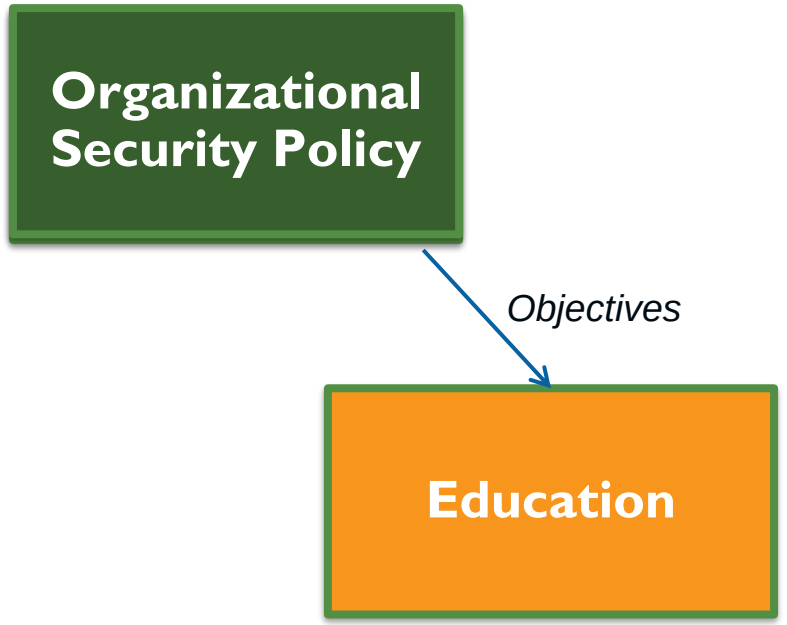
- **Processes and actions:**
  - Develop plans (restoration/recovery, communication, reporting)
  - Identify law enforcement agencies
  - Rehearse plans

Education

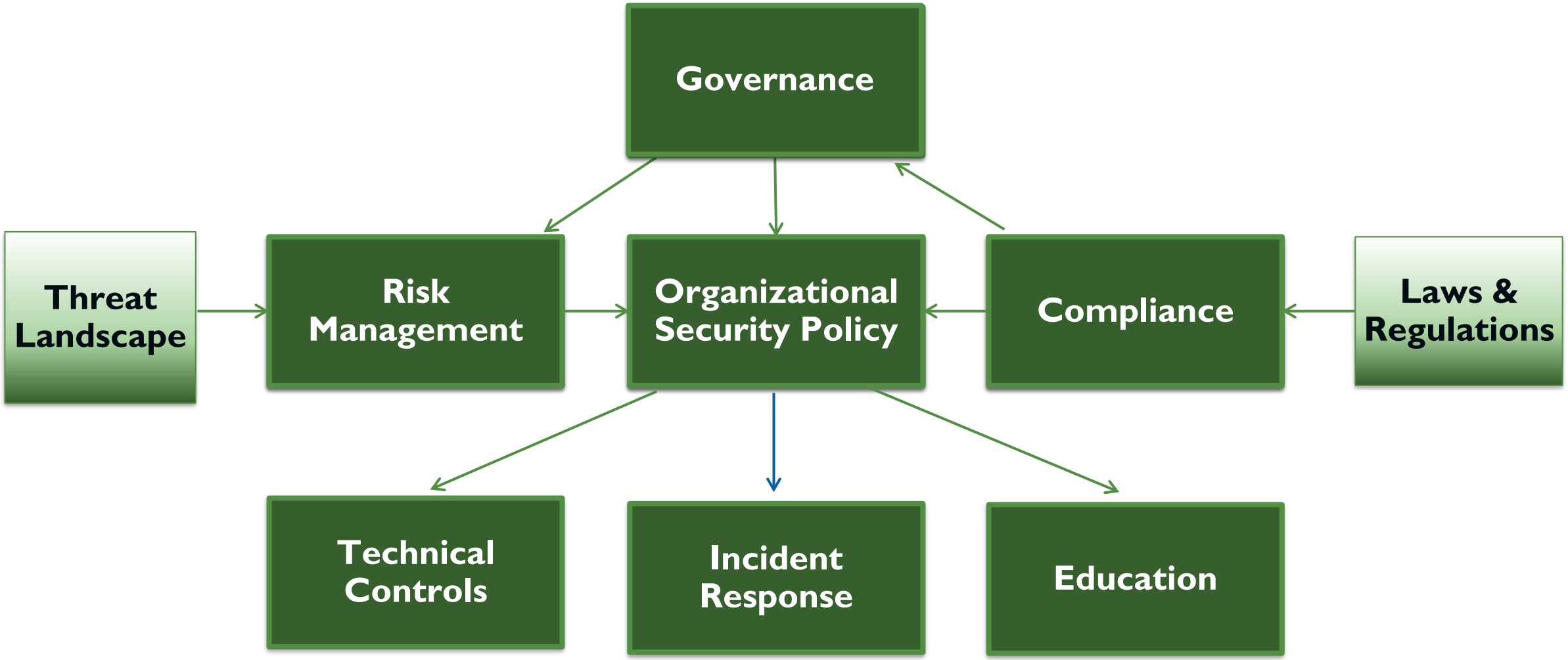
- **Importance:**
  Raise awareness of ALL employees
  - non-technical staff,
  - executives,
  - technical staff (specialized)

- **Touchpoints:**
  Objectives from the organizational security policy

- **Processes and actions:**
  - Prioritize training objectives
  - Identify sources of training
  - Scheduling



The Building Blocks



Next Steps

Resilient Energy Platform

- The **cyber building blocks** presented are within a **“living” framework** – We welcome **your feedback, input and experience** to improve the framework and building blocks! Email Maurice.Martin@nrel.gov to provide input.

- NREL, with input from USAID and other partners, will develop the **building blocks** into a **practitioners’ guide** and **cyber pillar** within the **Resilient Energy Platform website** with elaborated information on each building block, key knowledge resources, etc.

- The **broader webinar series**, and discussions during the webinars, will also inform further development of the building blocks and guide.

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Key Knowledge Resources to Support Work on the Building Blocks (1)

Resilient Energy Platform

Information Security Management

- ISO/IEC 27001
- https://www.iso.org/isoiec-27001-information-security.html

Cyber Governance

- Control Objectives for Information and Related Technology (COBIT)
- https://www.isaca.org/resources/cobit

Framework for setting organizational priorities

- NIST Cybersecurity Framework
- https://www.nist.gov/cyberframework

Security Controls

- CIS Critical Security Controls for Effective Cyber Defense
- https://www.cisecurity.org

COBIT 5
AN ISACA® FRAMEWORK

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Key Knowledge Resources to Support Work on the Building Blocks (2)

Resilient Energy Platform

Guidelines for Energy Regulators

- Evaluating the Prudency of Cybersecurity Investments
- Link

Industrial Security

- ANSI/ISA 62443-2-1
- Link

System Security

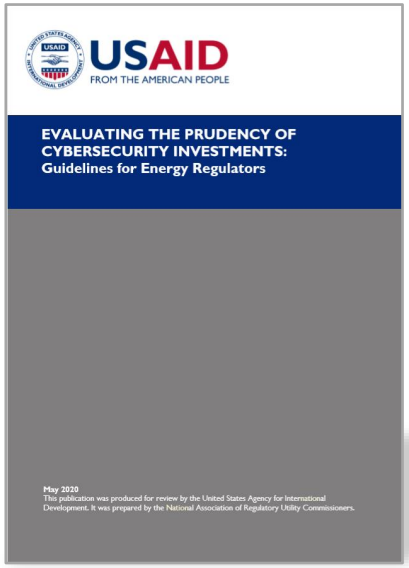
- ANSI/ISA 62443-3-3
- Link

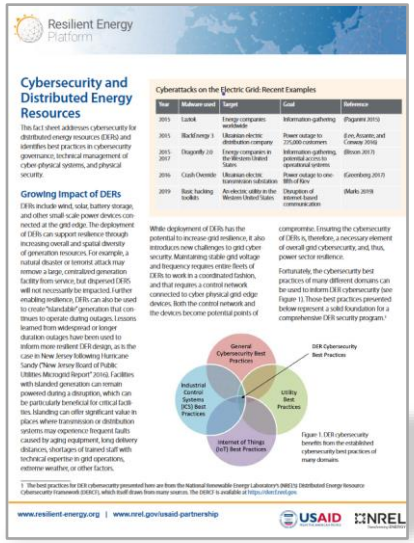
Cybersecurity and Distributed Energy Systems

- Link

Cybersecurity Procurement Language for Energy Delivery Systems

- Link





USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Key Knowledge Resources to Support Work on the Building Blocks (3)

Example (not endorsement) sources of Cyber Threat Intelligence (CTI)

Spamhaus Project (www.spamhaus.org)

SANS Internet Storm Center (isc.sans.edu)

ICS-CERT (www.us-cert.gov/ics)

RSA (www.rsa.com)

National Council of ISACS (www.nationalisacs.org)

“Best of Lists” (opinions of the writers)

- **Vendors, Public Sources, and Private Sources**
- https://www.tylercybersecurity.com/blog/guide-to-cyber-threat-intelligence-sources

- **Paid Subscriptions**
- https://www.esecurityplanet.com/products/top-threat-intelligence-companies.html

Resilient Energy Platform

Building Blocks to Support Cybersecurity in the Power Sector

Questions & Answers

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

Next Webinars in this Series

July 2 @ 9 a.m. U.S. EDT (1300 GMT)

- **Tracking Utility Digitalization Progress, Strategies, and Roadmap**

July 9 @ 9 a.m. U.S. EDT (1300 GMT)

- **Cybersecurity and Distributed Energy Resources**

July 16 @ 11 a.m. U.S. EDT (1500 GMT)

- **The Corporate Culture and Importance of Cyber Hygiene**

More to be announced!

Register and check for updates at
https://usea.org/events

How to Stay In Touch

- Follow NREL on:
  - LinkedIn - National Renewable Energy Laboratory
  - Twitter - @NREL

- Join the USAID-NREL Partnership mailing list at:
  - https://www.nrel.gov/usaid-partnership/newsletter.html

www.nrel.gov/usaid-partnership

Thank you!

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.