Resilient Energy Platform

Fact Sheet: Power Sector Cybersecurity Building Blocks

Background

The Power Sector Cybersecurity Building Blocks, developed through the U.S. Agency for International Development (USAID)-National Renewable Energy Laboratory (NREL) Partnership and the Partnership's Resilient Energy Platform, are designed to help a variety of stakeholders improve security for the electrical grid. This effort grows out of USAID and NREL's discussions with utilities around the world, as well as past cybersecurity assessments performed by NREL on dozens of utilities and government agencies, with a focus on the cybersecurity challenges faced by small and under-resourced utilities.

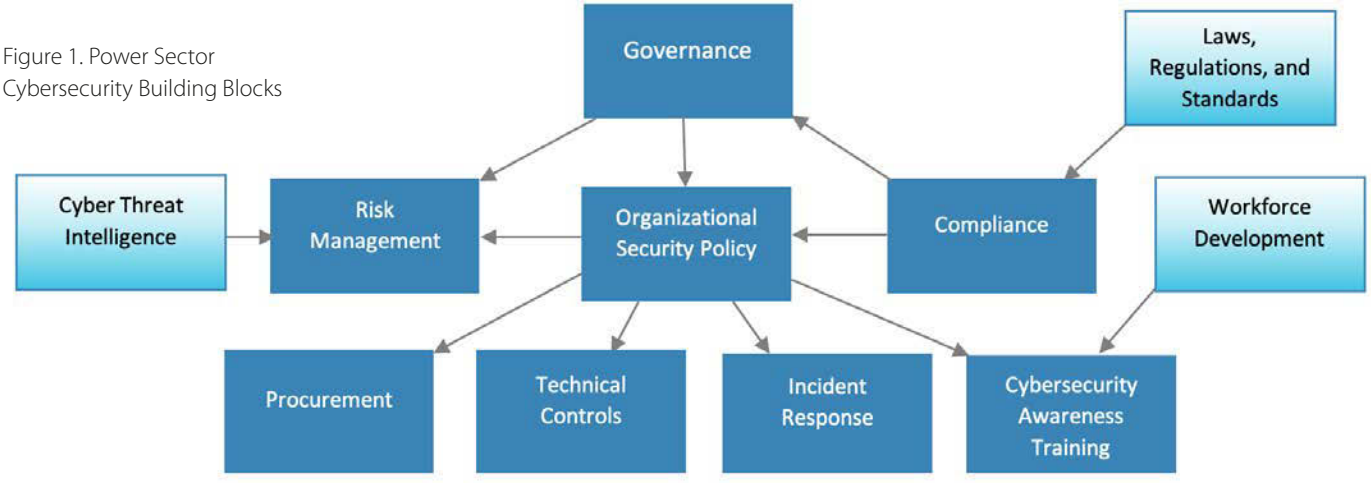
The Building Blocks

The document (available at www.resilient-energy.org/cyber) outlines 11 building blocks for power sector cybersecurity (Figure 1). It functions as a guide to help organizations develop a robust cybersecurity defense program. Individually, each building block represents a cluster of related activities within cybersecurity on which an organization should focus. Using the building blocks, organizations can effectively prioritize their cybersecurity efforts to best thwart a wide range of potential cyberattacks.

The 11 Cybersecurity Building Blocks each discuss a particular element of a well-rounded cybersecurity framework:

- **Governance:** The processes that direct a utility-wide cybersecurity effort and provide accountability for that effort. Cybersecurity governance requires the understanding and action of those at the very top level of the utility, such as the executive director, chief executive officer, board of directors, and others.
- **Organizational Security Policy:** This building block focuses on the high-level document that captures the essential elements of a utility's efforts in cybersecurity and includes the effort to create, update, and implement that document.
- **Risk Management:** Activities that identify and evaluate cybersecurity risk, with the goal of reducing that risk to a level appropriate to the utility's business objectives.
- **Cyber Threat Intelligence:** Cyberattack tools and adversaries that might constitute a threat and the vulnerabilities they could exploit. Utilities need cyber threat intelligence to understand the threat landscape and take action to mitigate cyber risks.
- **Laws, Regulations, and Standards:** Laws and regulations are the compulsory host country directives that a utility must comply with regarding cybersecurity. Regulations sometimes enforce standards created by nongovernmental entities that capture best practices.
- **Compliance:** The effort within a utility to remain in compliance with laws, regulations, and standards.
- **Procurement:** The processes used to monitor and improve the cybersecurity of devices, applications, and services as they are acquired and integrated into utility operations, as well as efforts to manage supply chain risk.
- **Technical Controls:** The hardware and software components that protect a system against cyberattack.

Figure 1. Power Sector Cybersecurity Building Blocks



Firewalls, intrusion detection systems, encryption, and identification and authentication mechanisms are examples of technical controls.

- **Incident Response:** The actions taken by a utility to prepare for cyberattacks. This includes creating plans for response, rehearsing the response prior to an attack, continuous monitoring to identify attacks, and the actual response.
- **Cybersecurity Awareness Training:** Steps taken by utilities to educate all employees (including nontechnical staff) about potential cyber threats and their roles in preventing them.
- **Workforce Development:** The efforts by multiple organizations, such as government, industry, or academia, to ensure an adequate supply of workers with specialized cybersecurity knowledge and skills.

The Need

There are already many excellent guides, standards, and frameworks for organizations seeking to improve cybersecurity. Some are produced by standards bodies, such as the International Organization for Standardization. Others are produced by government agencies, such as the United States National Institute of Standards and Technology (NIST). Equipment vendors, consultants, and nonprofits have also created useful resources.

However, many organizations still struggle to create a cybersecurity program that is balanced across all areas required to protect their assets from attack. They may have heavy investments in one area, with little investment in another. For these organizations, the "building block" approach will hopefully prove useful. The building blocks define clusters of related activities within a balanced cybersecurity program and provide references and resources for each area. Since the building blocks correspond to activities, staff time and resources need to be allocated to them in the same way that staff time and resources are allocated to noncyber activities (such as accounting).

The clusters of related activities defined by the Power Sector Cybersecurity Building Blocks span multiple stakeholders. In Figure 1, the dark blue rectangles correspond to building blocks within a utility, while the light blue rectangles are external to a utility. The arrows show major categories of information passing between building blocks.

Organizations in the early stages of cybersecurity maturity will likely get the most benefit from these building blocks because they are likely to struggle with the question of what a complete cyber program looks like. More "cyber mature" organizations can also use the building blocks to gain a fresh perspective on their efforts and fill in gaps in their existing cyber programs.

The Power Sector Cybersecurity Building Blocks are not meant to be the final word on cybersecurity for the power sector, as this field is evolving rapidly with the introduction of new power grid technology and an ever-changing threat landscape. USAID and NREL welcome discussion regarding updates to future iterations of these building blocks. For more information, please read the full report available at: https://resilient-energy.org/cyber.

Resilient Energy Platform

The Resilient Energy Platform helps countries and localities address power system vulnerabilities by providing strategic resources and direct country support to enable planning and deployment of resilient energy solutions. This includes expertly curated reference material, training materials, data, tools, and direct technical assistance in planning resilient, sustainable, and secure power systems. Ultimately, these resources enable decision makers to assess power sector vulnerabilities, identify resilience solutions, and make informed decisions to enhance energy sector resilience at all scales, including local, regional, and national scales. To learn more about the technical solutions highlighted in this fact sheet, visit the Resilient Energy Platform website at: https://resilient-energy.org.

https://resilient-energy.org/cyber | www.nrel.gov/usaid-partnership

Jeremy Foster
U.S. Agency for International Development
Email: jfoster@usaid.gov

Sarah Lawson
U.S. Agency for International Development
Email: slawson@usaid.gov

Sadie Cox
National Renewable Energy Laboratory
Email: sadie.cox@nrel.gov

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.

NREL/FS-5R00-79542 I April 2021
NREL prints on paper that contains recycled content.

The Resilient Energy Platform provides expertly curated resources, training, tools, and technical assistance to enhance power sector resilience. The Resilient Energy Platform is supported by the U.S. Agency for International Development.

The USAID-NREL Partnership addresses critical challenges to scaling up advanced energy systems through global tools and technical assistance, including the Renewable Energy Data Explorer, Greening the Grid, the International Jobs and Economic Development Impacts tool, and the Resilient Energy Platform. More information can be found at: **www.nrel.gov/usaid-partnership**.

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

REexplorer MAPPING OUR ENERGY FUTURE

Greening the Grid

I-JEDI

Resilient Energy Platform