



USAID
FROM THE AMERICAN PEOPLE



Cybersecurity Handbook Overview

September 14, 2021





Cybersecurity Handbook Overview

- Broad introduction to cybersecurity
- Targeted to novice readers
- Summarizes the webinar series and panel sessions
- Distills recommendations from cybersecurity experts into a checklist
- Provides links to resources in one place
- Shows examples of threats utilities have faced and actions utilities have taken

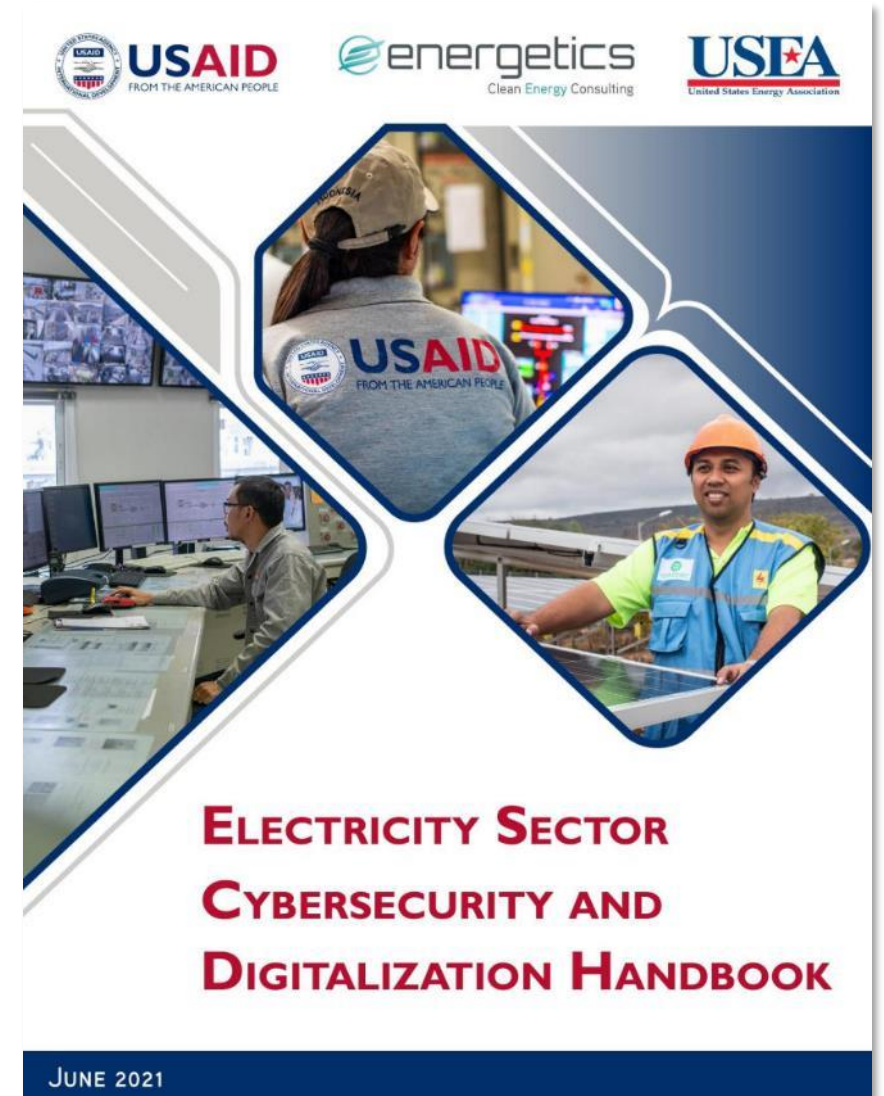




Table of Contents

- **Executive Summary** makes the case for caring about cybersecurity
- **Chapter 1: Introduction** provides overview of the handbook
- **Chapters 2-6:** Five main content chapters summarize webinars
- **Appendix A: Checklist** distills the lessons from the experts into action items
- **Appendix B: Resources** has links to all the resources mentioned throughout

Electricity Sector Cybersecurity and Digitalization Handbook

FOREWORD BY USAID	I
LETTER FROM THE ACTING EXECUTIVE DIRECTOR, USEA	II
ACKNOWLEDGEMENTS	III
LIST OF ACRONYMS	IV
EXECUTIVE SUMMARY	VI
CHAPTER 1: INTRODUCTION	1
Organization of This Handbook	2
Getting Started	2
CHAPTER 2: INTEGRATING CYBERSECURITY INTO THE UTILITY BUSINESS MODEL	1
Strategies for Intelligence Integration: Connections Between Digitalization and Cybersecurity	2
Building Blocks to Support Cybersecurity in the Power Sector	6
The Corporate Culture and the Importance of Cyber Hygiene	10
Utility Digitalization Progress and Digitalization Strategies and Roadmaps	14
Cybersecurity and Distributed Energy Resources	19
CHAPTER 3: ASSESSING CYBERSECURITY AND DEVELOPING PLANS	23
Introduction to the Cybersecurity Assessment Methodologies	24
Forging a Cybersecurity Defense for Utilities	31
Cyber Risk Management Through Measurement	38
Energy Sector Cyber Threats, Intrusion Detection, & Testing	46
CHAPTER 4: IMPLEMENTING CYBERSECURITY CONTROLS	51
Utility Data Protection Policies and Practices	52
Industrial Control System (ICS) and SCADA: Risks and Solutions	57
The Importance of Supply Chain Security	62
CHAPTER 5: REGULATIONS, STANDARDS, AND BEST PRACTICES	67
Cybersecurity Standards and Best Practices: Utilities and ISO 27001	68
Cybersecurity Standards and Best Practices: U.S. Standards	73
The Relationship Between Regulators and Power Utilities	82
CHAPTER 6: INFORMATION SHARING AND COMMUNICATION	86
Communication Strategies for Regulators Before, During, and After Cyber Attacks	87
Key Elements of Trusted Collaboration and Information Sharing	90
CONCLUSION	95
APPENDIX A. CHECKLIST TO BEGIN TO ADDRESS CYBERSECURITY VULNERABILITIES	96
APPENDIX B. ADDITIONAL RESOURCES	99
APPENDIX C. GLOSSARY OF KEY TERMS	103



Main Content and Intended Audiences

Chapter & Topics	Primary Audience
Chapter 2: Integrating Cybersecurity into the Utility Business Model <ul style="list-style-type: none">Benefits and risks of digitalization; cybersecurity governance and culture	Utility leadership/executives Management at all levels
Chapter 3: Assessing Cybersecurity and Developing Plans <ul style="list-style-type: none">Summary of assessment frameworks; recommendation for defense	Cybersecurity leads Utility leadership/executives
Chapter 4: Implementing Cybersecurity Controls <ul style="list-style-type: none">Details on data protection, industrial control systems, and supply chain	Cybersecurity leads Utility leadership/executives
Chapter 5: Regulations, Standards, and Best Practices <ul style="list-style-type: none">ISO27001, NERC CIP, and the relationship between regulators and utilities	Regulators Utility personnel
Chapter 6: Information Sharing and Communication <ul style="list-style-type: none">Strategies for communication and information sharing	All stakeholders in the electric power sector
Appendix A: Checklist <ul style="list-style-type: none">Distillation of recommended actions from across the webinar series	Utility personnel

