

NARUC

Cybersecurity Program Review

Lynn P. Costantini, DSc., CISSP
Center for Partnerships & Innovation
February 6, 2019

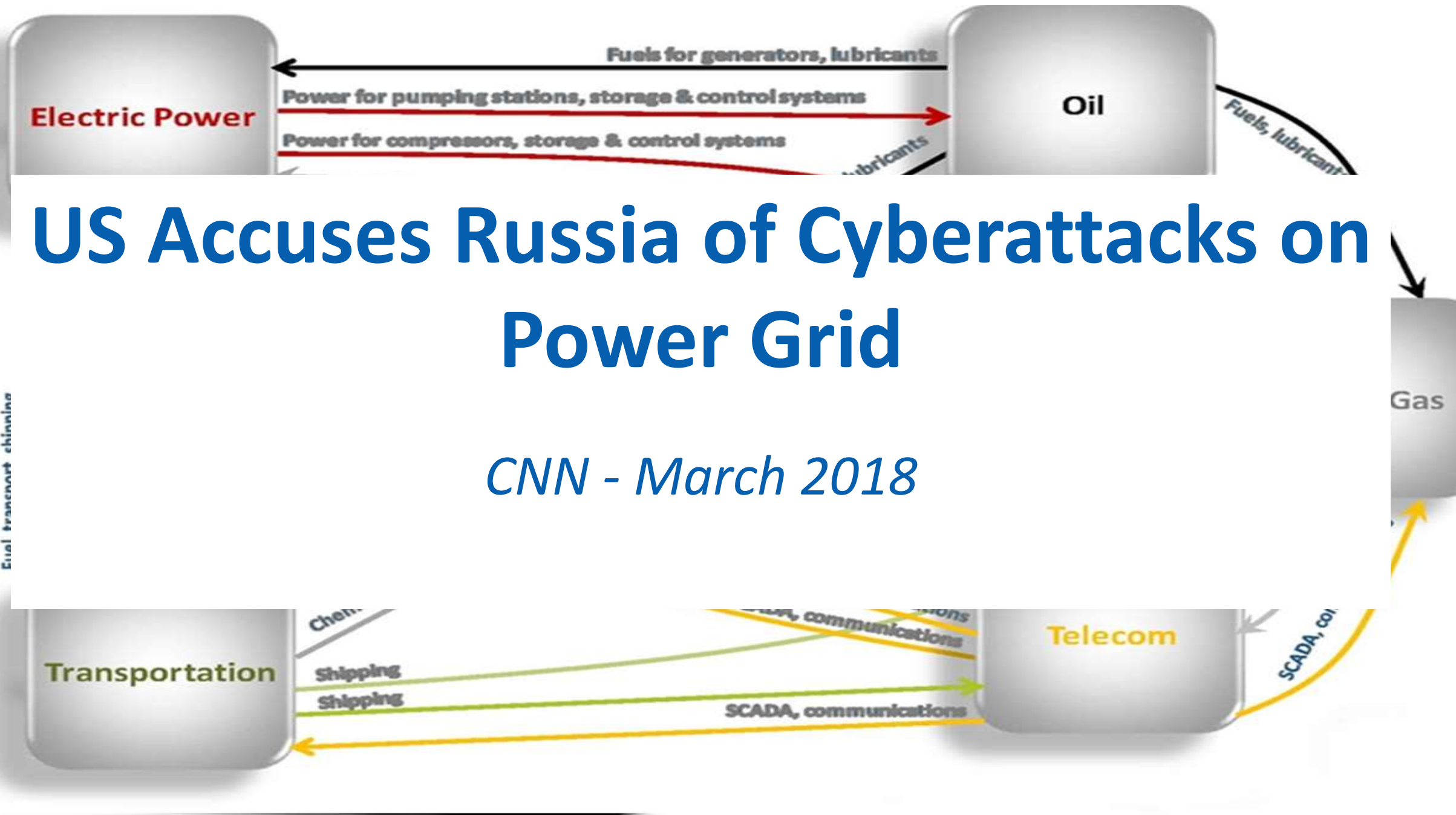


Center for Partnerships & Innovation (CPI)

- Identify emerging utility policy challenges and connect state commissions with expertise and strategies to navigate complex decision-making
- Build relationships, develop resources, and deliver training
 - Energy infrastructure modernization
 - Electricity system transformation
 - Critical infrastructure/cybersecurity/resilience
 - Innovation hot topics



Equal Transport China



US Accuses Russia of Cyberattacks on Power Grid

CNN - March 2018

Starting Point

- Risk Management for Critical Infrastructure Protection: An Introduction for State Utility Regulators
- Cybersecurity Primer for State Utility Regulators Version 3.0
- Critical Infrastructure Resource Repository

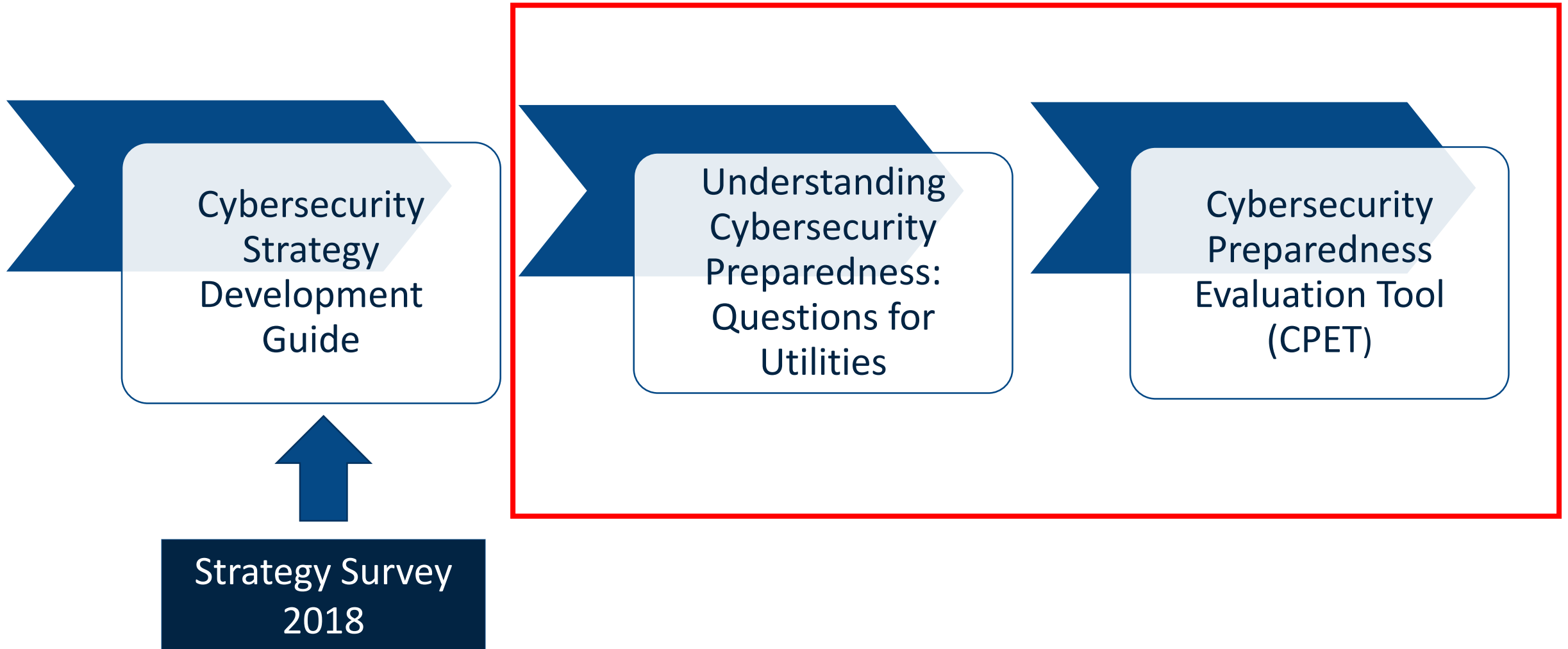


Cyber Manual Project

- Turns foundational cybersecurity concepts into useful tools to drive action
- Set of individual tools tailored to public utility commissions
- Tools purposefully fit together to optimize value

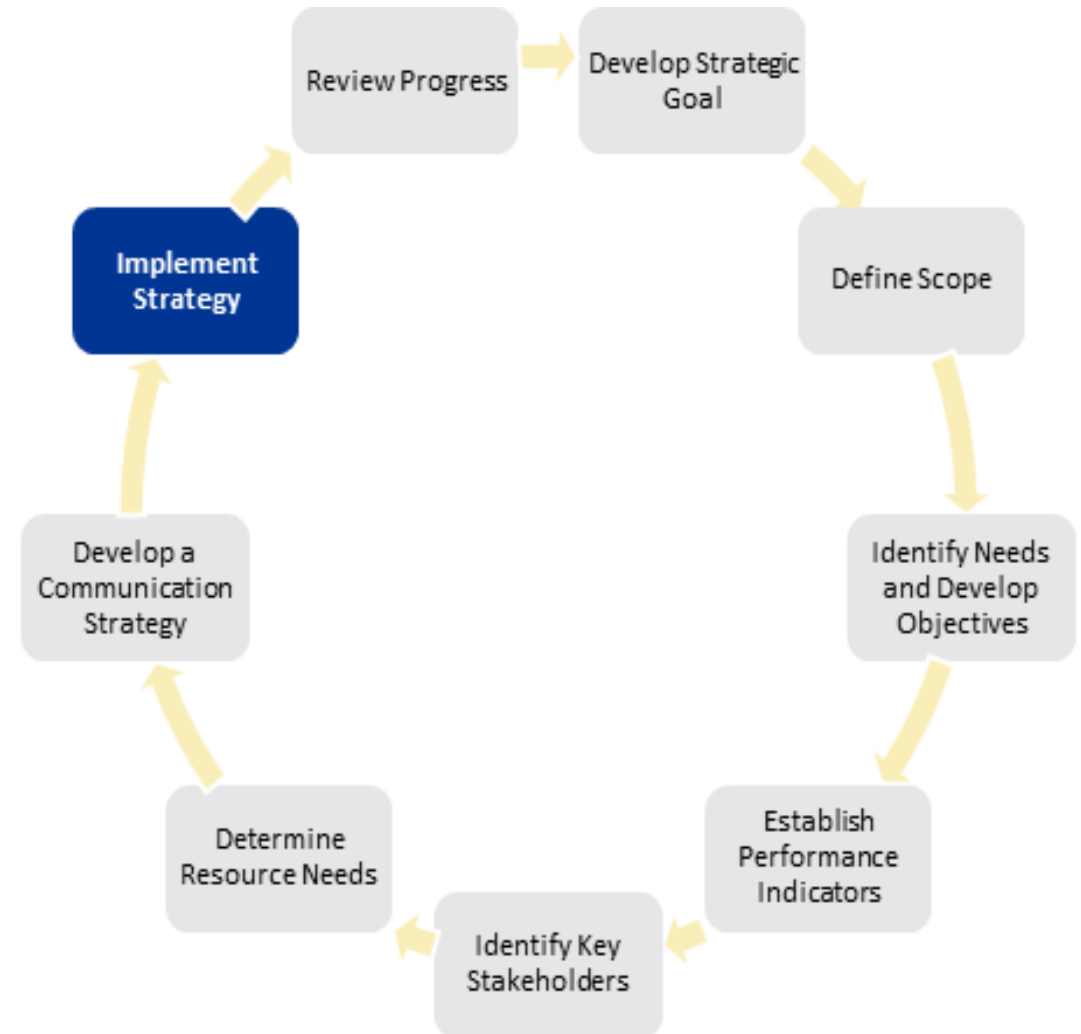


Cyber Manual Components - 2018



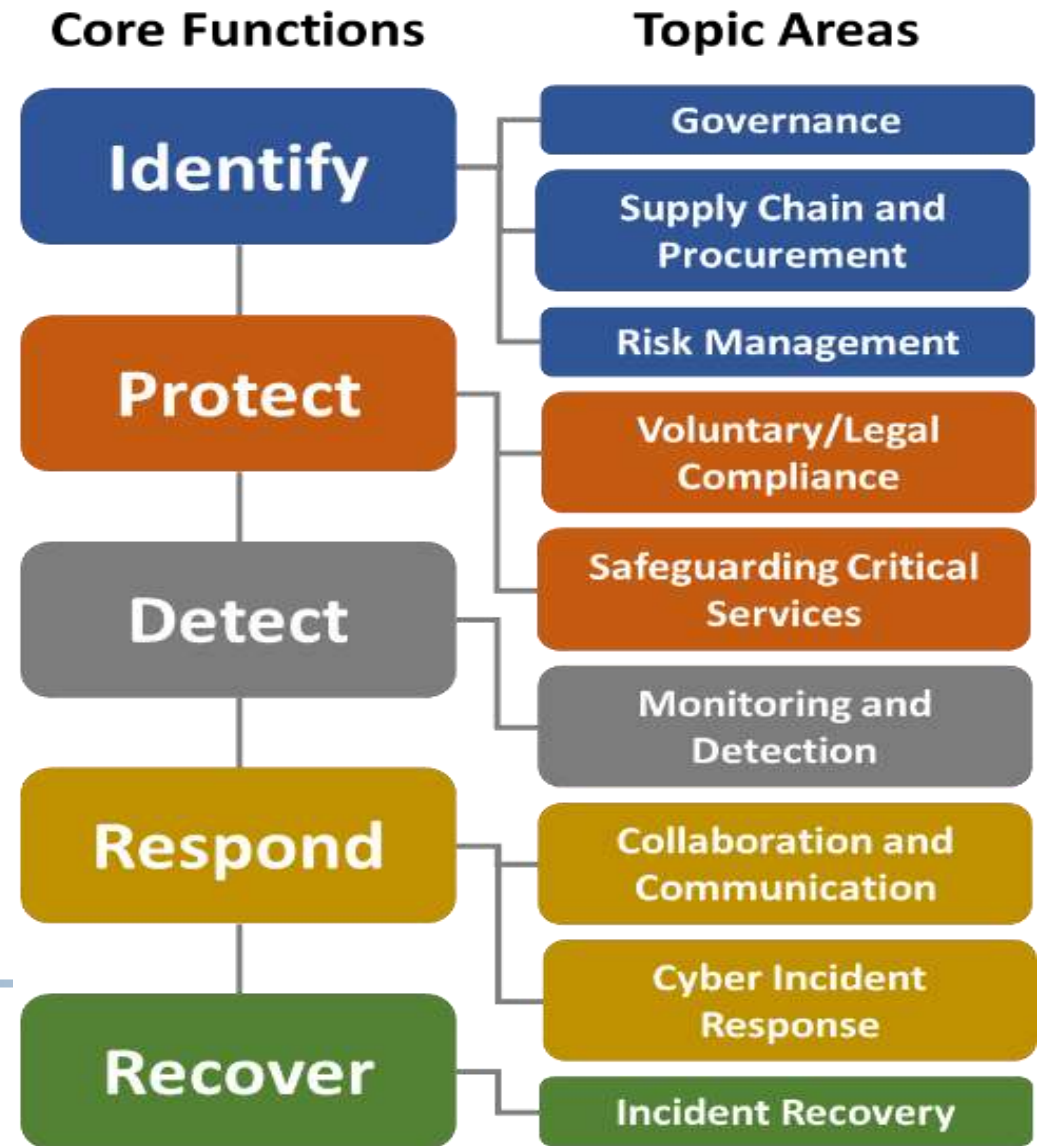
Cybersecurity Strategy Development Guide

- Focuses on how PUCs engage with utilities on cybersecurity preparedness topics
- Provides step by step guidance for developing PUC-specific objectives, goals, and communications plans to ensure meaningful, engagement and actionable outcomes
- Developed in partnership with Cadmus Group LLC



Understanding Cybersecurity Preparedness: Questions for Utilities

- Modeled on NIST Cybersecurity Framework
- Builds on NARUC's Cybersecurity Primer
- Frames the assessment categories used in CPET



Cybersecurity Preparedness Evaluation Tool (CPET)

- Provides indicators of a utility's cybersecurity program maturity
 - for non-technical audiences
 - based on DOE C2M2
- Supports PUCs' awareness of utilities' current level of cybersecurity preparedness
- Provides means of evaluating improvements year over year
- Relies on data inputs from Questions for Utilities tool



CPET Maturity Ratings

No Criteria

No Information

Level 1: Initial

Level 2: Established

Level 3: Mature

Level 4: Optimized

**Planning
and Policy**

**Implementation
and Operation**

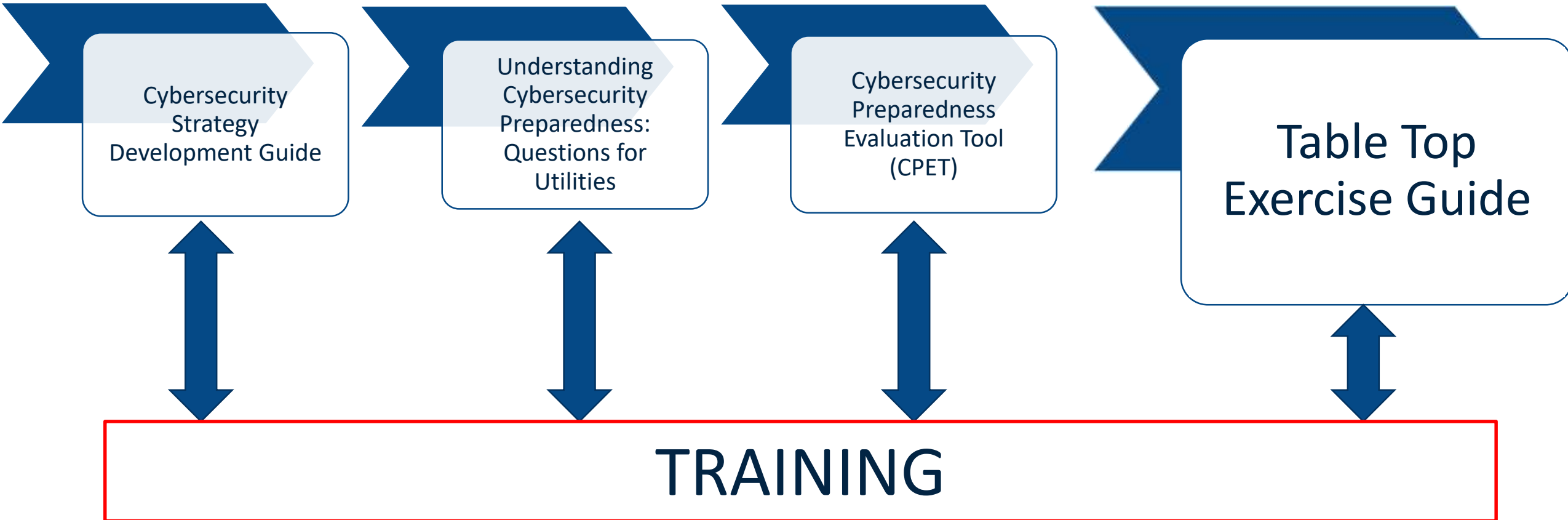
Glossary of Cybersecurity Terms

Cybersecurity Incident

An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

^[1] <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.

Cyber Manual Components - 2019



Also in 2019...

- Report on State Cybersecurity Collaboration Models (with NASEO)
- Assessment of Cybersecurity Workforce Impacts on PUCs
- Guide to Cybersecurity Information Protection



Contact Info

Lynn Costantini

Deputy Director, Center for Partnerships & Innovation

lcostantini@naruc.org

Matthew Acho

Program Officer, Center for Partnerships & Innovation

macho@naruc.org

