RELIABILITY & SECURITY

Workshop - Portland, Oregon

October 29–30, 2024

WECC

Current and Emerging Cybersecurity Risks: CIP Themes Report

October 29, 2024

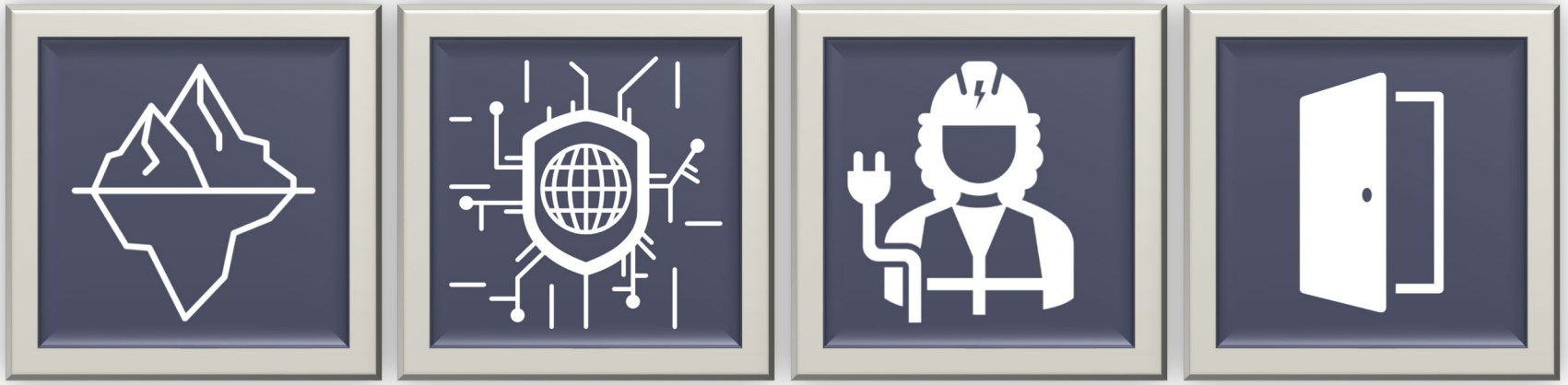
Kevin Spontak, Senior Attorney, Enforcement, WECC

Joe Tromba, Legal Counsel, SERC

Mike Hattery, Senior Counsel, Legal & Enforcement, RF

Critical Infrastructure Protection (CIP) Themes

- Four themes
  - Latent Vulnerabilities
  - Insufficient Commitment to Low Impact Programs
  - Shortages of Labor and Skillsets
  - Performance Drift



Latent Vulnerabilities

The Importance of Internal Detective Controls

- Long-standing, higher risk issues that evade detection and persist within entities' environments
- Examples in physical security, electronic access, and patching

Latent Vulnerabilities

The Importance of Internal Detective Controls

- Suggestions
  - Promote strong detective controls
    - Dedicate resources
    - Conduct testing
    - Scrutinize design
  - Conduct and act on internal assessments

Insufficient Commitment to Low Impact Programs

Increasing complacency on shared security objectives

- Low impact entities are susceptible to:
  - Misinterpreting CIP objectives
  - Misunderstanding cyber environments
- Potential vulnerabilities include:
  - Electronic access management
  - Cyber asset implementation

Increasing Insufficient Commitment to Low Impact Programs

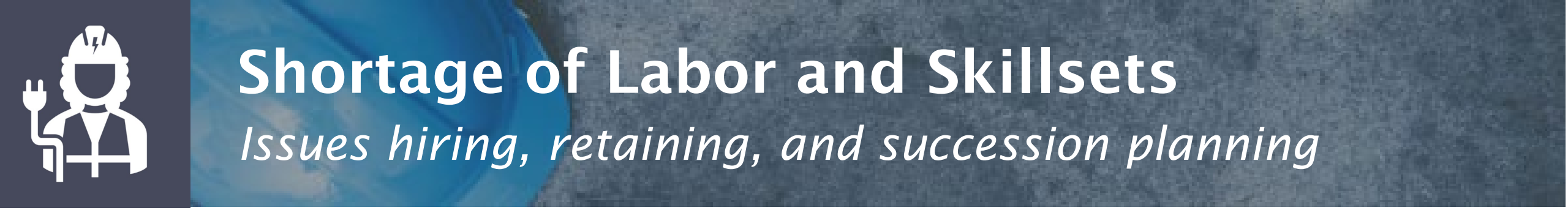
Increasing complacency on shared security objectives

- Suggestions
  - Understand technology configurations and impacts on facilities
  - Clarify and document processes: consistent training, delineated roles and responsibilities, and open channels of communication
  - Identify and verify program execution and implementation

Shortages of Labor and Skillsets

Issues hiring, retaining, and succession planning

- Challenging threat landscape coupled with reported labor shortage
- Issues transitioning work or managing organizational complexities



Shortage of Labor and Skillsets

Issues hiring, retaining, and succession planning

- Suggestions
  - Hire new staff and use experienced staff to train successors
  - Reassess HR approach to induce joining/staying
  - Ensure adequate resource availability to execute new processes/controls, including responsible personnel participation in vendor demonstrations
  - Implement succession plans
  - Create process commonalities between business units
  - Use different ERO tools and resources

Performance Drift

Physical security issues as markers of performance drift and apathy

- Increasing failure in physical security programs when disciplined execution becomes inconvenient or uncomfortable
- Bypassing security controls, relying on assumptions, propping doors, leaving doors and gates open, and sharing badges and PINs

Performance Drift

Physical security issues as markers of performance drift and apathy

- Suggestions
  - Test for potential performance drift for physical security
  - Reinforce why process adherence matters
  - Construct incentive programs to promote process adherence

WECC

Electric Reliability and Security for the West

www.wecc.org