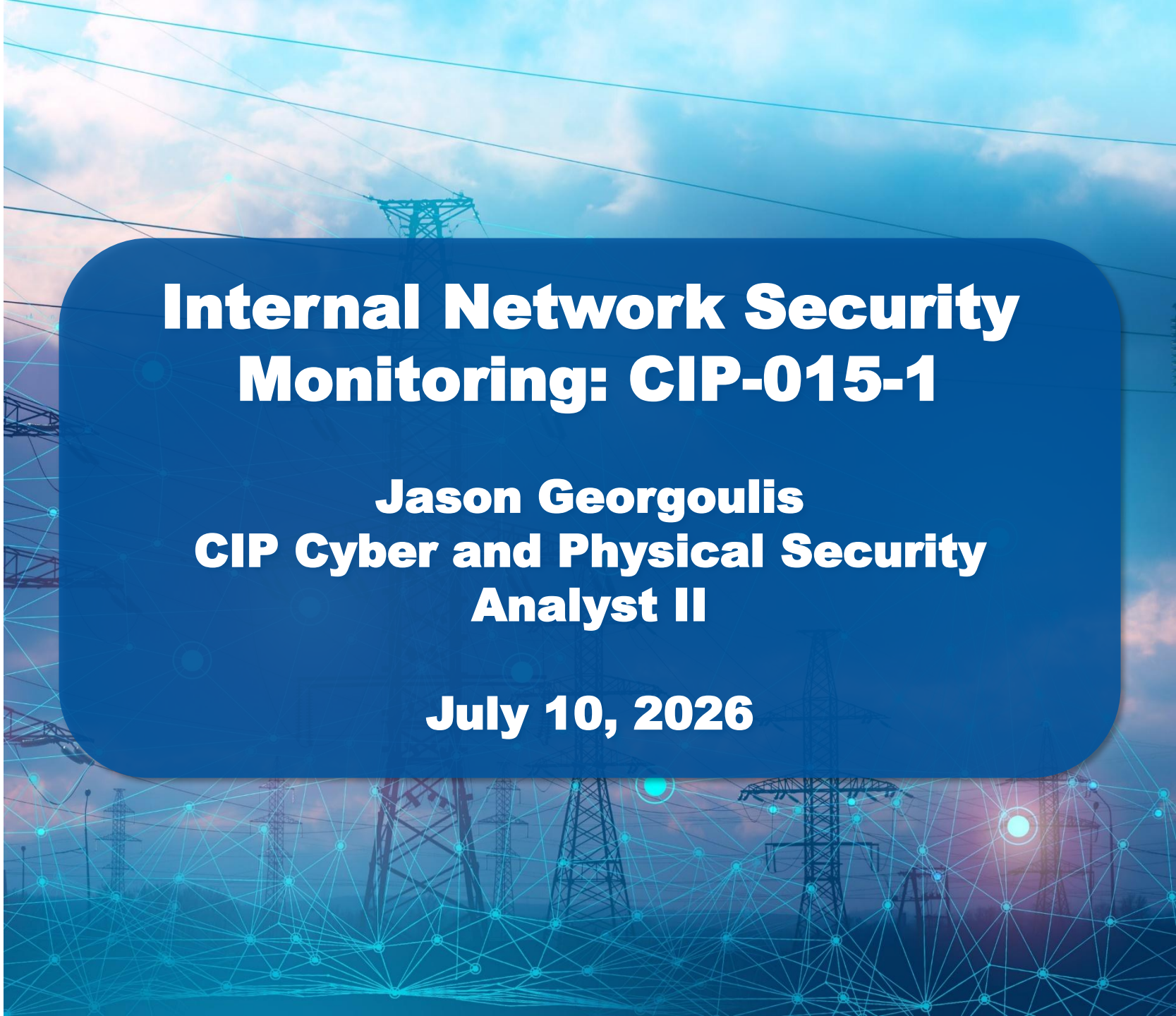


TEXAS RE

Internal Network Security Monitoring: CIP-015-1

Jason Georgoulis
CIP Cyber and Physical Security Analyst II

July 10, 2026

CIP-015-1

Purpose

- To improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack.

R1

- Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity.

CIP-015-1 R1 Parts

Part 1.1

1.1: Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications

Part 1.2

1.2: Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1

Part 1.3

1.3: Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s)

Considerations

- Location of network data feeds
- Methods of data collection
- How you define “anomalous”

Best Practices and Internal Controls

- Start broad and narrow the collected data that contains the most relevant data
- Complimentary monitoring systems
- Ongoing tuning of internal network security monitoring systems (INSM) systems
- Workflows for evaluation with potential actions

CIP-015-1 R2

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity at a minimum until the action is complete in support of Requirement R1, Part 1.3.

Considerations

- Data retention process

Best Practices and Internal Controls

- Secure repository for storing network activity data
- Workflows for defining anomalous data and what criteria is used

CIP-015-1 R3

R3. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification.

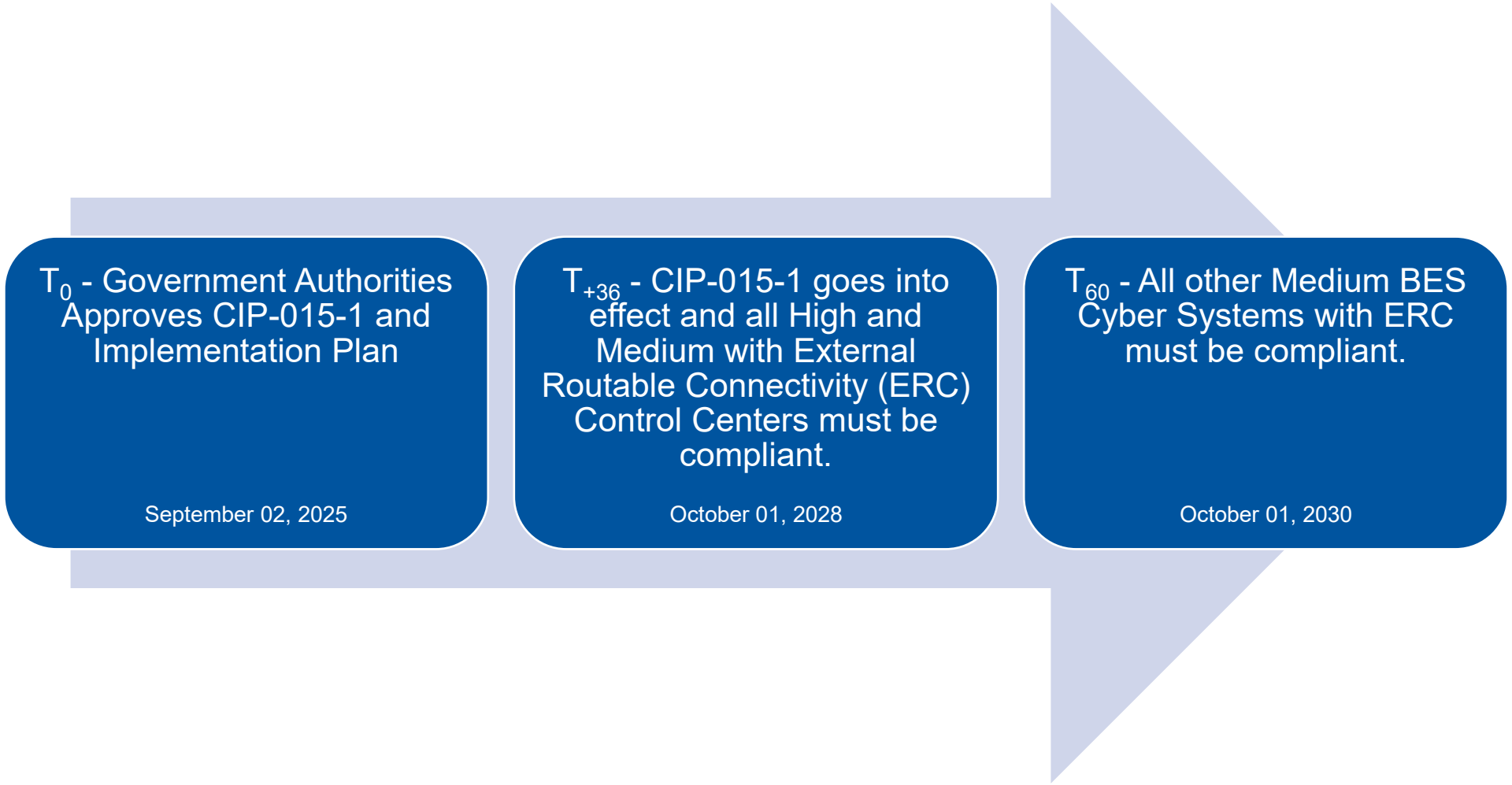
Considerations

- Who has access rights to the data?

Best Practices and Internal Controls

- Secure backups
- Data integrity

Phased-in Implementation

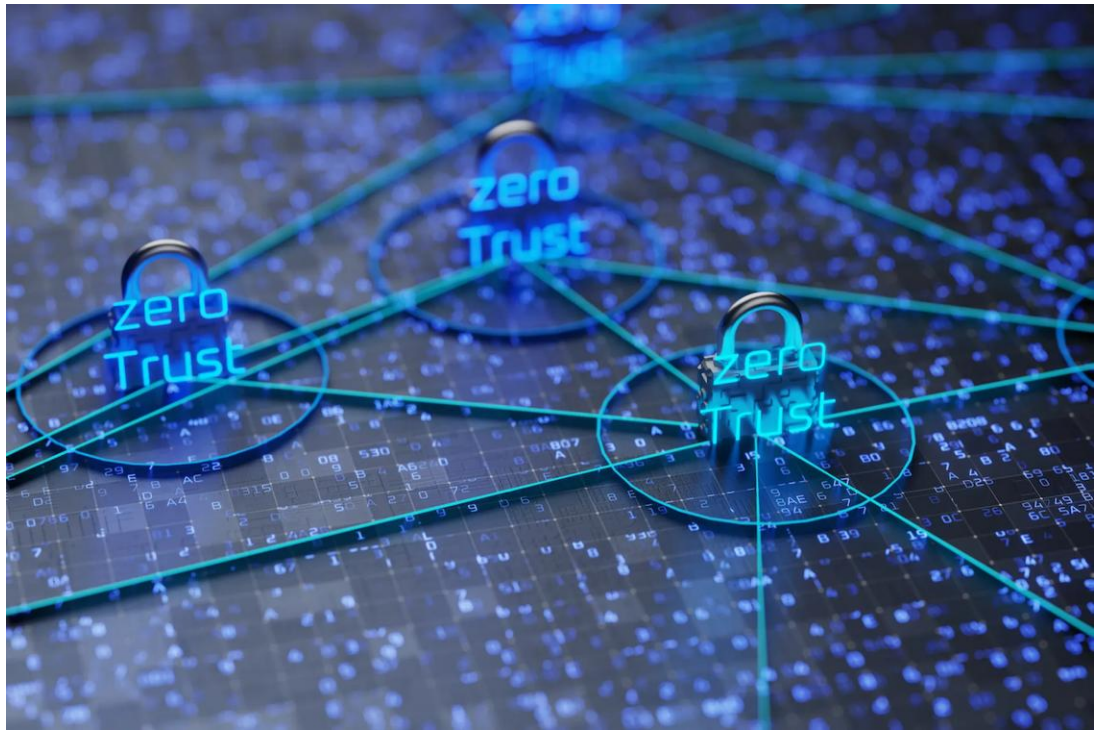


Resources

MITRE ATT&CK®

SP 800-207, Zero Trust Architecture | CSRC

CMEP practice guide-network-monitoring-sensors



Questions?

TEXAS RE
Ensuring electric reliability for Texans