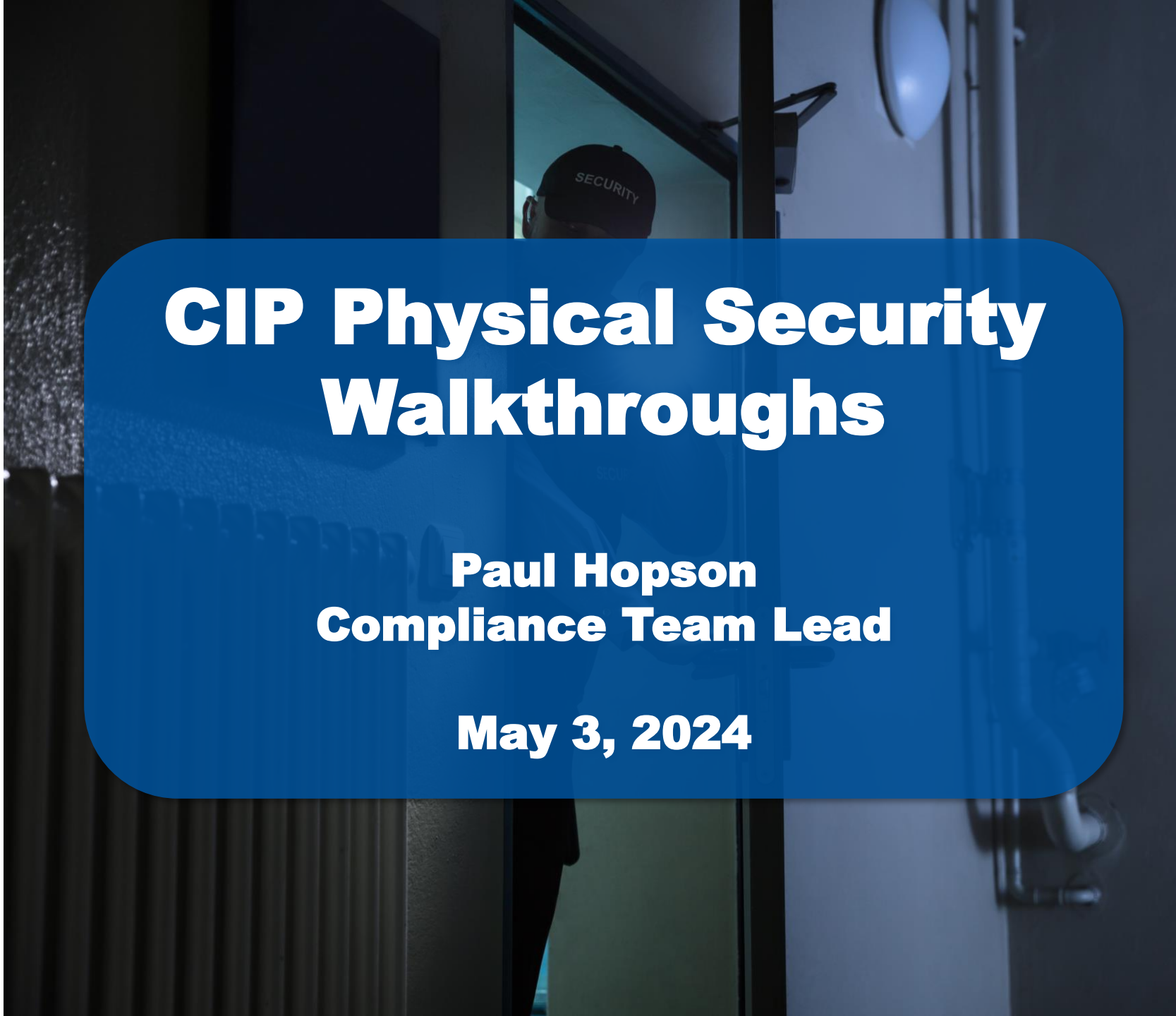
TEXAS RE



CIP Physical Security Walkthroughs

Paul Hopson
Compliance Team Lead

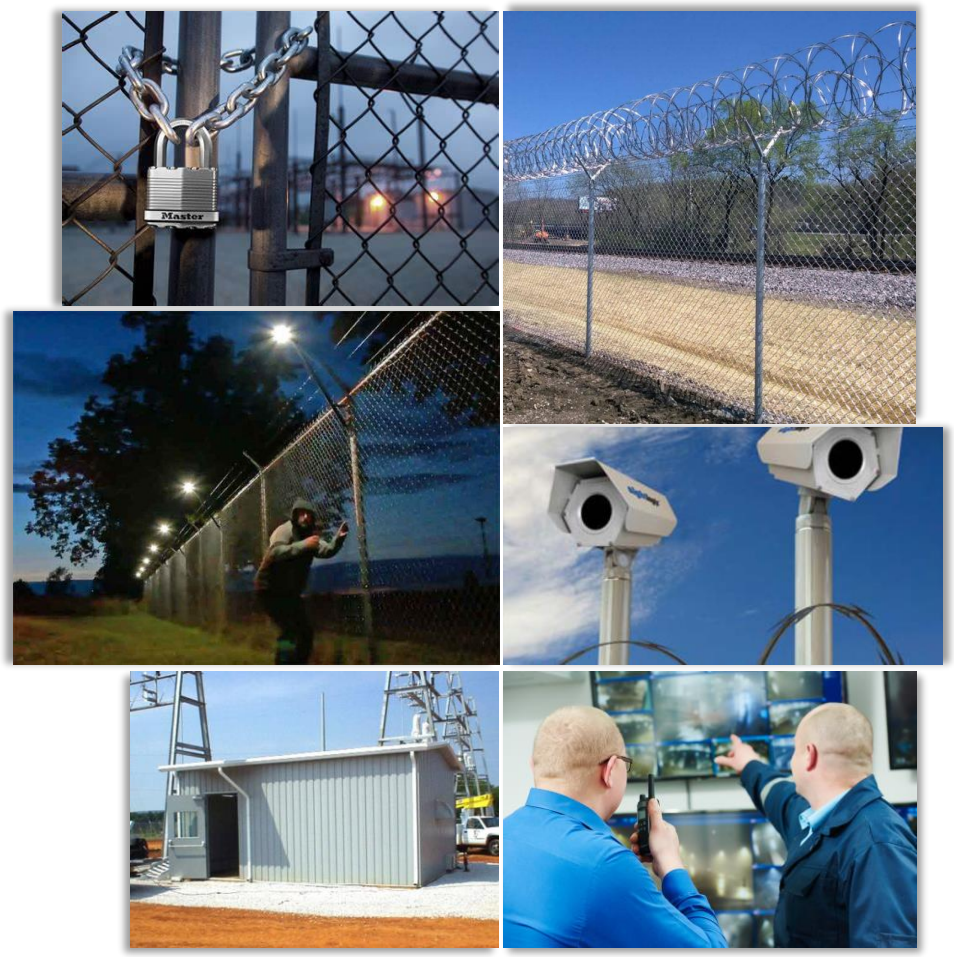
May 3, 2024

Understanding CIP Physical Security Walkthroughs

Physical security walkthroughs involve reviewing the physical security of BES Cyber Systems (BCS) to assess the effectiveness of physical security plans, visitor control programs, Physical Access Control Systems (PACS), and to ensure compliance with NERC CIP standards

These walkthroughs seek to identify any vulnerabilities or deficiencies and ensure they are addressed to mitigate the risk of unauthorized access or other security threats to critical infrastructure

Some Key Components of a CIP Physical Security Walkthrough



- Access Controls
- Perimeter Security
- Intrusion Detection
- Surveillance
- Security Personnel
- Access Logs

CIP Standards Used During Walkthroughs

CIP-003-8 (Low Impact BCS)

Section 2, Physical Security Controls – at the asset or the locations of the low impact BES Cyber Systems within the asset, and the Cyber Assets that provide electronic access controls

CIP Standards Used During Walkthroughs

CIP-006-6 (High and Medium Impact BCS with External Routable Connectivity)

Part 1.2 Utilize at least one physical access control to allow only individuals who have authorized unescorted physical access into the Physical Security Perimeter (PSP)

Part 1.3 Utilize at least two or more different physical access controls

Part 1.4 Monitor for unauthorized access into a PSP

Part 1.5 Issue an alarm or alert in response to detected unauthorized access through a physical access point to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection

Part 1.6 Monitor each Physical Access Control System (PACS) for unauthorized physical access

Part 1.7 Issue an alarm or alert of detected unauthorized physical access to a PACS to personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection

Part 1.8 Log entry of everyone with authorized unescorted physical access into each PSP

Part 1.9 Retain physical access logs for at least 90 days

Part 1.10 Restrict physical access to cabling and nonprogrammable communication components outside of the PSP, or encrypt/monitor the status of the link and issue alarm/alert within 15 minutes of detection, or equal logical protection

Part 2.2 Require manual or automated visitor logging

Part 2.3 Retain visitor logs for at least 90 days

CIP Standards Used During Walkthroughs

CIP-007-6

- High Impact BCS and Medium Impact BCS at Control Centers and associated PCA and nonprogrammable communication components located inside both physical and electronic security perimeters
- Part 1.2 Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media

Additional Information

- CIP-014-3 – Physical Security – Reviewing evidence (applicability lists, models, and technical analyses) of the risk assessments
- Electronic Access Points identified and associated PSPs
- Electronic Access Controls & Monitoring Systems (EACMS)
- Physical Access Control Systems
- Cyber Assets identified – sampled
- TOP-001-6 R20 – Verify that there is redundant and diversely routed infrastructure (switches, routers, servers, power supplies, network cabling, etc.) at the primary Control Center, including its associated data center

CIP Physical Walkthroughs during Your Engagement

- Inspect perimeter fencing, gates, and barriers to ensure they are adequate to deter unauthorized access
- Check surveillance systems, including cameras and sensors, to verify their functionality and coverage
- Test access control measures, such as card readers, alarms/alerts, and security personnel to ensure only authorized individuals can enter secure areas
- Review access logs, and visitor logs to ensure continuous escorted access of visitors within the PSP
- Review environmental controls for Control Centers and associated datacenters, redundancy and diverse routing - avoiding single points of failure

TEXAS RE
Ensuring electric reliability for Texans