RELIABILITY & SECURITY

Workshop - Salt Lake City, UT

March 26–27, 2024

WECC

Holistic Physical Security Principles and Applications

March 27, 2024

Brady Phelps, CPP, PCI, PSP
Physical Security Lead

What You Will Learn and Why it Matters

- Understand the framework of physical security standards.
- Gain insights into the NERC CIP standards, what to expect during audits and how best to prepare.
- Adopting a holistic security strategy and learning from the experiences of others can elevate an entity's security measures to not only meet but exceed regulatory expectations, thereby safeguarding critical infrastructure and contributing to the overall stability and reliability of the power grid.

Welcome and Agenda

WELCOME

Welcome and Agenda

Introduction to Physical Security Standards

- Overview of NERC CIP Physical Security Requirements
- Transition to WECC's Audit Approach

Welcome and Agenda

WECC's Audit Approach Explained

- Methodologies and Criteria for Assessing Compliance
- Preparing for an Audit: Expectations vs. Reality

Welcome and Agenda

Holistic Security Principles

- Integrating NERC CIP Standards with Industry Best Practices
- Developing Comprehensive Security Plans
- The Importance of a Proactive and Adaptive Security Strategy

Welcome and Agenda

Real-world Findings and Lessons Learned

- Common Audit Findings: Challenges and Gaps
- Best Practices Derived from Audit Experiences

Welcome and Agenda

Conclusion and Q&A

- Recap of Key Takeaways
- Open Floor for Questions and Discussion

Overview of NERC CIP Physical Security Requirements

NERC CIP-003-8 R2 Attachment 1, Section 2:

Establishes the requirement for a documented cybersecurity policy that addresses the security of the Bulk Electric System's cyber assets critical to its reliability.

NERC CIP-006-6:

Mandates the implementation of physical security measures to protect critical cyber assets within identified Physical Security Perimeters.

NERC CIP-014-3:

Requires the identification and protection of transmission stations, substations, and their primary control centers critical to the reliability of the Bulk Electric System against physical attacks.

WECC’s Audit Approach

NERC CIP-003-8 R2 Attachment 1, Section 2

Documented Plan

- Based on need
- As determined by you

To:

The Cyber Asset(s), as specified by the Responsible Entity, or

To:

The locations of the BES Cyber Systems within the asset.

WECC's Audit Approach

NERC CIP-003-8 R2 Attachment 1, Section 2

Verify Implementation

WECC’s Audit Approach

NERC CIP-003-8 R2 Attachment 1, Section 2

Security Objective

- Verify Security Objective has been achieved;

To:

The Cyber Asset(s), as specified by the Responsible Entity, or

To:

The locations of the BES Cyber Systems within the asset.

WECC’s Audit Approach

NERC CIP-006-6 R1.1

Documented Plan

- Verification of one or more documented plans

Implementation

- Verify the plan has been implemented

WECC’s Audit Approach

NERC CIP-006-6 R1.2

Plan Documentation

- Verify written plan for this part

Verify

- Each PSP has at least one method of physical access control

Verify

- Ensure only authorized individuals have unescorted access to each relevant Physical Security Perimeter.

WECC’s Audit Approach

NERC CIP-006-6 R1.3

Plan Documentation

- Verify written plan for this part

Verify

- Each PSP has at least two methods of physical access control

Verify

- Ensure only authorized individuals have unescorted access to each relevant Physical Security Perimeter

WECC's Audit Approach

NERC CIP-006-6 R1.4

Documented Plan

- Verify written plan for this part

Implementation

- Ensure monitoring for unauthorized entry through PSP access points

WECC’s Audit Approach

NERC CIP-006-6 R1.5

Documented Plan

- Verify written plan for this part

Implementation

- Confirm alarms for unauthorized PSP entry, alert relevant personnel within 15 minutes

WECC's Audit Approach

NERC CIP-006-6 R1.5

Alarm or Alert Issue

Full Language: ***Verify that an alarm or alert is issued in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.***

WECC’s Audit Approach

NERC CIP-006-6 R1.6

Documented Plan

- Verify written plan for this part

Implementation

- Ensure PACS monitors and reports any unauthorized access attempts

WECC’s Audit Approach

NERC CIP-006-6 R1.7

Documented Plan

- Verify written plan for this part

Implementation

- Ensure alerts for unauthorized PACS access are issued to identified personnel within 15 minutes of detection

WECC's Audit Approach

NERC CIP-006-6 R1.6/1.7

G&TB

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6, and 1.7 beyond what is already required for the PSP.

WECC’s Audit Approach

NERC CIP-006-6 R1.8

Documented Plan

- Verify written plan for this part

Implementation

- Ensure logs for each authorized individual’s PSP entry include identity, date, and time details

WECC's Audit Approach

NERC CIP-006-6 R1.9

Documented Plan

- Verify written plan for this part

Implementation

- Ensure retention of PSP entry logs for authorized individuals for at least 90 days

WECC's Audit Approach

NERC CIP-006-6 R1.10

Documented Plan

- Verify written plan for this part

Implementation

- Ensure physical or logical protection for external ESP cabling and components, with implementation of logical protections, for non-physical safeguards

WECC’s Audit Approach

NERC CIP-006-6 R2.1

Documented Plan

- Verify written plan for this part

Implementation

- Ensure continuous escort for unauthorized individuals within PSPs, except under exceptional circumstances

WECC’s Audit Approach

NERC CIP-006-6 R2.2

Documented Plan

- Verify written plan for this part

Implementation

- Log visitor entry/exit at PSPs: include dates, times, names, and contact, except during CIP Exceptional Circumstances

WECC's Audit Approach

NERC CIP-006-6 R2.3

Documented Plan

- Verify written plan for this part

Implementation

- Verify that visitor logs are retained for at least 90 calendar days

WECC's Audit Approach

NERC CIP-006-6 R3.1

Documented Plan

- Verify written plan for this part

Implementation

- Ensure PACS and PSP hardware and devices are maintained and tested biennially for proper functionality

WECC's Audit Approach

NERC CIP-014-3 R4

Review & Verify

- Review evidence of evaluation and verify it considers…

TVA

- Potential Threats and vulnerabilities as described in Requirement R4

WECC’s Audit Approach

NERC CIP-014-3 R4.1

Review & Verify

- Review evidence of evaluation and verify it considers…

Unique Characteristics

- Potential Threats and vulnerabilities as described in Requirement R4

WECC’s Audit Approach

NERC CIP-014-3 R4.2

Review & Verify

- Review evidence of evaluation and verify it considers…

Prior History of Attack

- Consider attack history on similar facilities by frequency, proximity, and severity

WECC's Audit Approach

NERC CIP-014-3 R4.3

Review & Verify

- Review evidence of evaluation and verify it considers…

Intelligence

- Consider intelligence or threat warnings from law enforcement, ERO, E-ISAC, and governmental agencies

WECC's Audit Approach

NERC CIP-014-3 R4

R4 Key Takeaway

Ensure comprehensive threat and vulnerability assessments by incorporating prompts from sections 4.1 to 4.3 in the development process.

WECC’s Audit Approach

NERC CIP-014-3 R5

Verify physical security plans cover identified facilities per R1/R2, developed within 120 days post-R2, include R5.1 – 5.4 attributes, and are properly implemented.

WECC's Audit Approach

NERC CIP-014-3 R5.1

Evaluate the collective design of resiliency and security measures to their effectiveness in deterring, detecting, delaying, assessing, communicating, and responding (DDDACR) to potential threats and vulnerabilities identified in the R4 evaluation.

WECC's Audit Approach

NERC CIP-014-3 R5.2

Evaluate the documented and implemented coordination with law enforcement, emphasizing the importance of establishing clear, actionable contact and coordination information as a critical component of the entity's capability for response and resiliency. This includes verifying the integration of such protections within the broader security measures design to DDDACR to potential physical threats.

WECC's Audit Approach

NERC CIP-014-3 R5.3

Assess the clarity, realism, and adherence to the specified timeline for executing physical security enhancements and modifications within the security plan, highlighting the timeline's importance as a best practice indicator for effective project management and security improvement execution.

WECC’s Audit Approach

NERC CIP-014-3 R5.4

Evaluate the process and provisions in place for continuously assessing evolving physical threats and updating corresponding security measures as per R5 Part 5.4, emphasizing the critical importance of adaptability and the implementation of responsive security measures as indicators of maintaining robust physical security.

WECC's Audit Approach

NERC CIP-014-3 R6

Review and assessment of evidence for dated documentation of unaffiliated third-party review of entity's R4 and R5 security plan(s).

WECC's Audit Approach

NERC CIP-014-3 R6.1

Assess the qualifications of reviewing entity staff against the criteria specified in Part 6.1, focusing on the adequacy and relevance of their expertise as an indicator for ensuring competent and effective reviews.

WECC's Audit Approach

NERC CIP-014-3 R6.2

Verify the timeliness of the unaffiliated third-party review, ensuring it was conducted within 90 calendar days after the completion of security plans as outlined in R5, as an indicator of compliance in maintaining a proactive security posture.

WECC's Audit Approach

NERC CIP-014-3 R6.3

Assess whether, upon receiving recommendations from an unaffiliated third-party reviewer regarding changes to the evaluations or security plan(s), the entity responds within 60 calendar days by either implementing the suggested modifications or documenting the rationale for not doing so. This process is a critical indicator of an entity's commitment to iterative improvement and adherence to best practices in security planning and response.

WECC’s Audit Approach

NERC CIP-014-3 R6.4

Evaluate the entity's implementation of procedures, such as non-disclosure agreements, to safeguard sensitive or confidential information shared with or developed for the unaffiliated third-party reviewer, ensuring compliance with this Reliability Standard. This assessment will focus on the entity's practices for protecting critical information from public disclosure, serving as a key indicator of their adherence to confidentiality and security best practices.

Preparing for an Audit: Expectations vs. Reality

Expectation: Adversarial Audit

Entities often anticipate a confrontational audit process

Reality: Collaborative and Educational

Audits are professional, organized, and purpose-driven, focusing on sharing best practices, education, and outreach

Preparing for an Audit: Expectations vs. Reality

Expectation: Strictly Formal Procedures

There's an assumption audits strictly follow formal procedures without flexibility

Reality: Dynamic Interaction

In addition to off-site reviews, on-site audits include impromptu interviews or "walk-and-talks," and real-time testing of security measures, offering a more comprehensive and engaging evaluation

Preparing for an Audit: Expectations vs. Reality

Expectation: Sole Focus on Compliance

Entities might expect auditors to solely focus on compliance checklists

Reality: Holistic Approach

While compliance is key, auditors also assess the effectiveness of implemented security measures, ensuring entities are not just compliant but also effectively secured against threats

Holistic Security Principles

Observation:

Holistic Physical Security Principles, in the context of compliance with NERC CIP physical security Standards, encompass a broad and integrated approach to ensuring the physical security of the BES. These principles are designed to not only meet specific regulatory requirements but also to promote a comprehensive, adaptive, and resilient security posture that protects against physical threats and vulnerabilities.

Holistic Security Principles

Integrated Security Framework

Low Impact

Emphasizes the importance of managing security as an integral part of the org's broader security framework. This includes identifying and documenting physical risks to BES Cyber Systems and applying appropriate security controls.

Holistic Principle

Ensures that physical security measures are not siloed but integrated into the overall security and risk management framework of the org, promoting a unified approach to protecting critical infrastructure.

Holistic Security Principles

Layered Defense Strategies (Defense-in-Depth)

CIP-006-6

Focuses on the implementation of physical security measures to protect BES Cyber Systems by creating a PSP and employing controls to manage access and protect against unauthorized physical access.

Holistic Principle

Advocates for a multi-layered, or defense-in-depth, approach to physical security, ensuring that multiple controls and barriers are in place to protect critical assets, thereby reducing the risk of a single point of failure.

Holistic Security Principles

Risk-Based Priority Setting

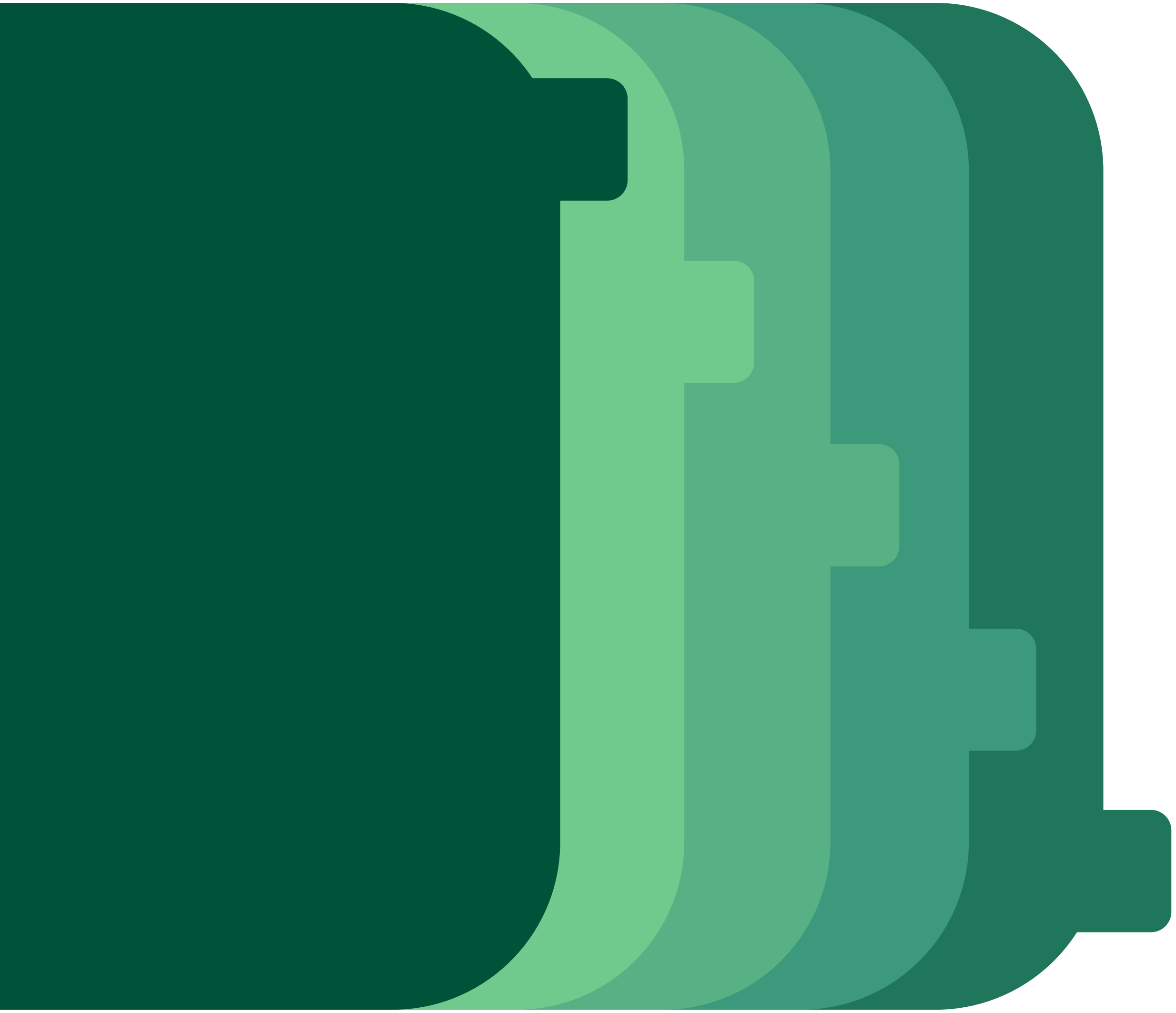
CIP-014-3

Requires entities to identify and protect assets that are critical to the reliability of the BES through a risk-based assessment.

Holistic Principle

Emphasizes the importance of assessing risks, employing layered defenses, adapting to evolving threats, prioritizing based on risk, fostering collaboration, and ensuring continuous improvement to safeguard the reliability of the electric grid.

Developing Comprehensive Security Plans



Developing Comprehensive Security Plans

Policy & Documentation

Craft detailed cybersecurity policies that comply with NERC CIP-003-8 R2 Attachment 1 Section 2, focusing on the protection of low impact BES Cyber Systems. Ensure these policies are well-documented, accessible, and communicated across the organization.

Developing Comprehensive Security Plans

Access Control Measures

Implement stringent access control measures to manage physical access to BES Cyber Systems. This includes defining roles and responsibilities for personnel granting access and ensuring that access is based on need.

Developing Comprehensive Security Plans

Training & Awareness

Develop and maintain comprehensive training and awareness programs for all personnel with access to BES Cyber Systems, emphasizing the importance of cybersecurity and the specific requirements of NERC CIP-003-8.

Developing Comprehensive Security Plans

Risk Assessment & Mitigation

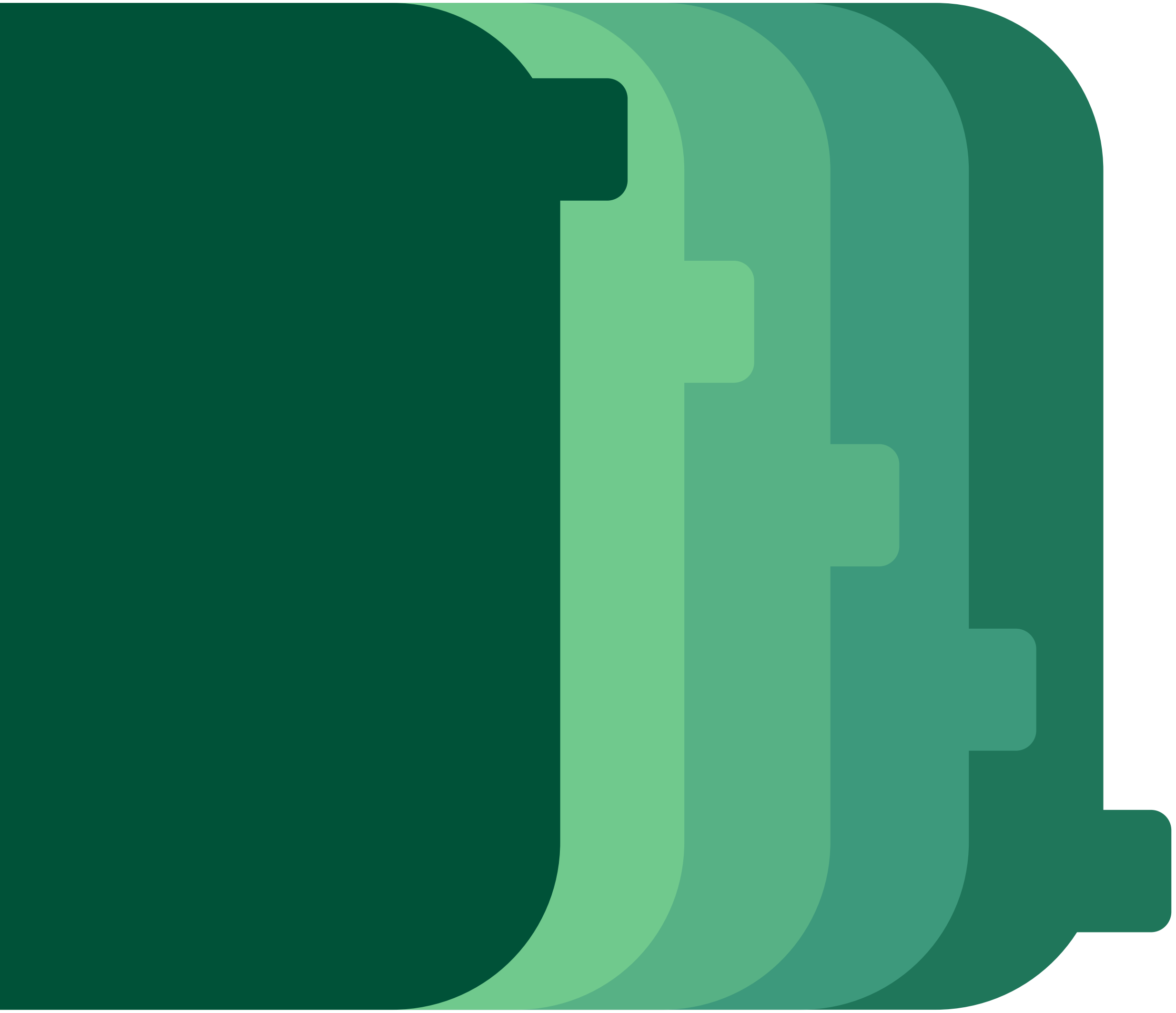
Conduct regular risk assessments to identify potential physical threats to cyber assets and vulnerabilities in existing security controls. Based on the assessment results, update and enhance security measures to mitigate identified risks, ensuring a dynamic and responsive security posture.

Developing Comprehensive Security Plans

Risk Assessment & Mitigation

Implement continuous monitoring processes to detect unauthorized access or anomalies within your physical perimeters. Regularly review and update the policies and practices to adapt to evolving threats and changes in the regulatory environment.

Developing Comprehensive Security Plans



Developing Comprehensive Security Plans

Defining & Securing PSPs

Clearly define the boundaries of each PSP to include all critical cyber assets. Implement physical barriers (e.g., cabinets, walls) and access controls (e.g., card readers, biometric scanners) to secure these perimeters against unauthorized access.

Developing Comprehensive Security Plans

Surveillance & Monitoring Systems

Install surveillance cameras and monitoring systems around and within PSPs to detect and record unauthorized access attempts or suspicious activities. Ensure these systems are actively monitored to enable immediate response to security incidents.

Developing Comprehensive Security Plans

Visitor Management Protocols

Establish strict protocols for managing visitors within PSPs, including logging visitor entry and exit, requiring escorts at all times, and verifying visitor identities. This ensures that visitors do not compromise the physical security of critical cyber assets.

Developing Comprehensive Security Plans

Testing & Maintenance

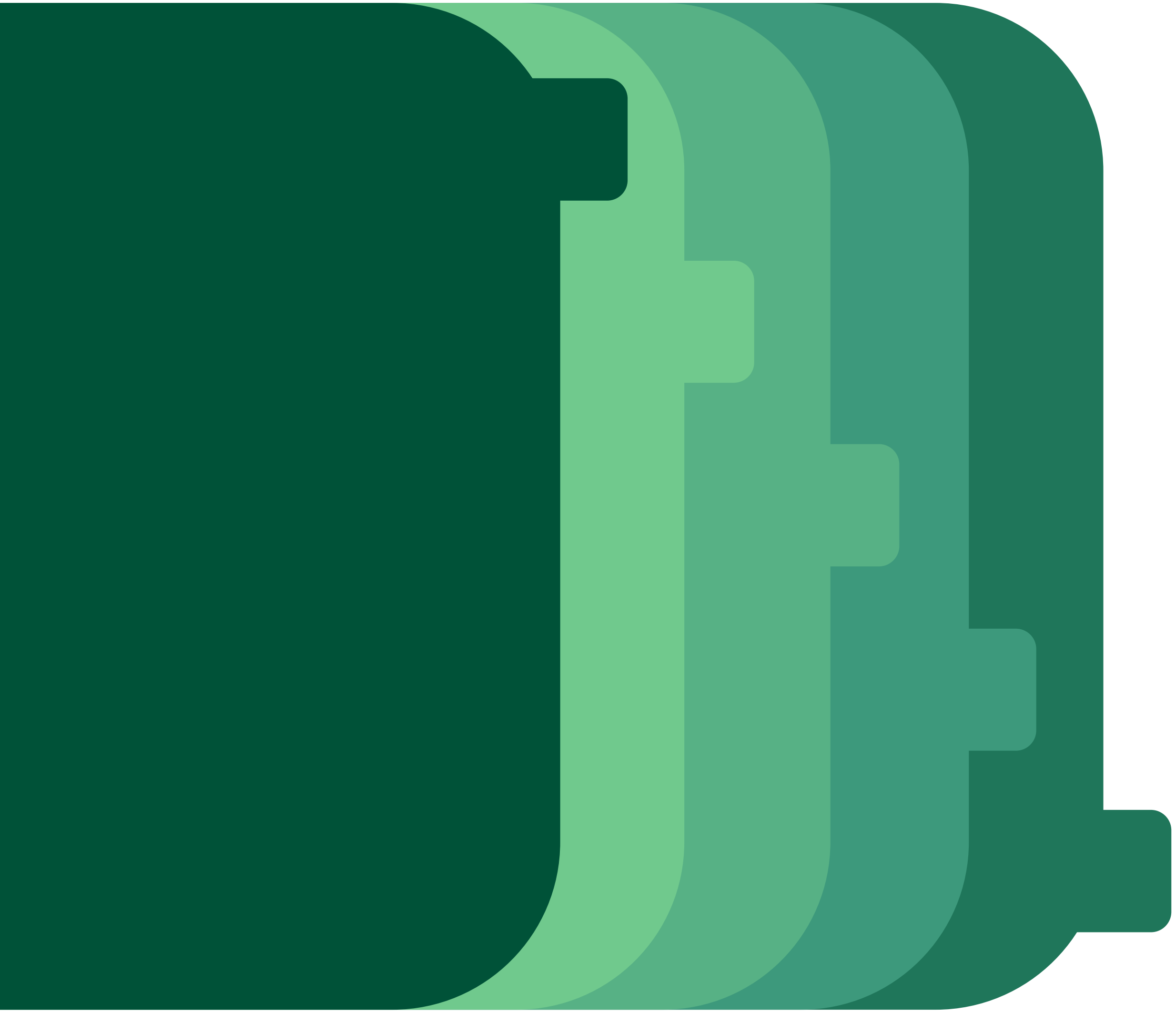
Conduct biennial testing and maintenance of PACS and associated hardware, like card readers, alarms, and barriers, to verify their proper function, and perform regular security drills to evaluate the efficacy of the physical security measures and protocols in place.

Developing Comprehensive Security Plans

Integrate with Cybersecurity

Ensure that physical security measures are integrated with cybersecurity policies and procedures. This includes coordinating incident response efforts and sharing information between cyber- and physical security teams to address multi-faceted threats effectively.

Developing Comprehensive Security Plans



Developing Comprehensive Security Plans

Detailed Threat Analysis

Incorporate findings from the R4 threat and vulnerability evaluation to identify specific risks to transmission stations, substations, and control centers. Use this analysis to tailor the security plan to address the unique characteristics and potential attack vectors of each facility.

Developing Comprehensive Security Plans

Response Strategies

Design security measures that collectively deter, detect, delay, assess, communicate, and respond to physical attacks. This should include physical barriers, surveillance systems, access controls, and incident response protocols, each chosen based on the R4 analysis outcomes.

Developing Comprehensive Security Plans

Law Enforcement Coordination

Develop formal relationships and communication/response plans with local law enforcement and other relevant agencies. Ensure these plans are reflected in the security strategy, facilitating quick response and coordination in the event of a security incident.

Developing Comprehensive Security Plans

Execution and Timeline Management

Create a clear timeline for implementing security enhancements, based on the priority of risks identified in the R4 evaluation. This timeline should be realistic and allow for the sequential rollout of security measures, with critical vulnerabilities addressed first.

Developing Comprehensive Security Plans

Dynamic Evaluation and Revisions

Establish a process for continuous review and adaptation of the security plan to account for evolving threats, new intelligence, and feedback from exercises and actual incidents. This ensures that the security strategy remains relevant and effective over time.

Proactive & Adaptive Strategies

Anticipate Emerging Threats

Proactively adapting security strategies under LI standards ensures that entities can anticipate and prepare for emerging threats, rather than react to incidents after they occur.

Enhance Security Posture

A proactive and adaptive approach allows continuous improvement in posture, using the latest technologies and best practices to protect cyber assets from threats, ensuring that security measures are current.

Compliance & Resilience

Adapting to shifts in regulatory requirements and threat landscapes is essential not only for compliance but also for building resilience against disruptions to the BES.

Proactive & Adaptive Strategies

Alarm Management & Response

Implementing a proactive strategy for alarms ensures that potential breaches are not only detected swiftly but are followed by quick, well-coordinated responses, minimizing the impact of incidents within the PSP.

Adaptive Visitor Management

Using advanced visitor management techniques, such as electronic logging, allows for more efficient handling of visitor access, ensuring that security protocols can adapt quickly to varying threat levels and visitor volumes.

Proactive PACS M&T

Regular assessments of PACS and their hardware ensures that any vulnerabilities are identified and addressed promptly, keeping the security infrastructure reliable and up-to-date with the latest security standards and technological advancements.

Proactive & Adaptive Strategies

Continuous Threat Intel

By staying informed on industry trends in attack methods, entities can proactively update their threat models and adjust measures to address evolving tactics, ensuring that current vulnerabilities are identified and mitigated in line with the latest threat intelligence.

Adaptive Physical Security Plan

Physical security plans that are adaptable to emerging threats ensures that security measures for critical facilities can evolve in response to changing threat landscapes.

Proactive UTPR

Engaging unaffiliated (and independent) third-party reviewers with a proactive approach to evaluating plans allows for the early identification of improvements, ensuring that feedback is incorporated to enhance security measures effectively.

Real-World Findings and Lessons Learned

Common Audit Findings: Challenges & Gaps

Real-World Findings and Lessons Learned

Challenges in Low Impact

Entities often provide vague policies, such as stating they “will grant access based on need” without detailing the underlying process.

Real-World Findings and Lessons Learned

Identified Gaps

Lack of detail fails to specify the procedural steps an individual must undertake to be granted necessary access, leaving the process open to interpretation and inconsistency.

Real-World Findings and Lessons Learned

Best Practices Derived from Audits

Document the full access request process within the security plan, clearly outlining:

- The initiation of the access request,
- The roles responsible for processing the request,
- The criteria for determining access necessity,
- The method of granting access, and
- Regular reviews of granted access to validate its continued necessity and appropriateness.

Real-World Findings and Lessons Learned

By incorporating these best practices, entities can close documentation gaps, clarify access protocols, and enhance their compliance with NERC CIP-003-8 R2 Attachment 1 Section 2.

Real-World Findings and Lessons Learned

Common Audit Findings: Challenges & Gaps

Real-World Findings and Lessons Learned

Challenges in Physical Security

Entities often lack comprehensive access management plans, specifically in the management of physical keys.

Real-World Findings and Lessons Learned

Identified Gaps

Reliance on traditional hard keys and padlocks without a detailed key management plan leaves low impact assets vulnerable and security measures unenforceable.

Real-World Findings and Lessons Learned

Best Practices Derived from Audits

- Key assignment tracking
- Access level definitions
- Key duplication control
- Regular key audits
- Lost key protocols

Real-World Findings and Lessons Learned

Incorporating these best practices into a key management plan can significantly strengthen physical security and regulatory compliance by providing a clear and auditable method of managing physical access to protected areas and assets.

Real-World Findings and Lessons Learned

Common Audit Findings: Challenges & Gaps

Real-World Findings and Lessons Learned

Challenges in Physical Security

Entities often fail to test site protections adequately before audit team visits.

Real-World Findings and Lessons Learned

Identified Gaps

Oversights in alarms, perimeter security, or procedural adherence are frequently uncovered during effectiveness testing by the audit team, which could have been preemptively identified and rectified.

Real-World Findings and Lessons Learned

Best Practices Derived from Audits

- Scheduled pre-visit testing
- Routine effectiveness checks
- Audit preparation drills
- Immediate remediation procedures
- Documentation and review

Real-World Findings and Lessons Learned

By implementing these best practices, entities can proactively ensure the effectiveness of their security controls and demonstrate their commitment to regulatory compliance and the physical security of their assets.

Real-World Findings and Lessons Learned

Common Audit Findings: Challenges & Gaps

Real-World Findings and Lessons Learned

Challenges in Physical Security

Failing to conduct comprehensive unique characteristic evaluations

Real-World Findings and Lessons Learned

Identified Gaps

Security assessments often overlook the unique aspects of each facility, such as its functions, location, contents, construction, regular visitors, entry and exit methods, access roads, and surrounding terrain, missing threats unique to that facility.

Real-World Findings and Lessons Learned

Best Practices Derived from Audits

- Detailed facility profiling
- Contextual threat analysis
- Stakeholder consultation
- Regular review and update

Real-World Findings and Lessons Learned

By integrating these best practices, entities can ensure their security assessments account for each facility's unique characteristics, leading to more effective and targeted security plans that address specific vulnerabilities and threats. This approach not only enhances compliance with NERC CIP-014-3 R4, but significantly improves the overall security posture of critical infrastructure.

Real-World Findings and Lessons Learned

Common Audit Findings: Challenges & Gaps

Real-World Findings and Lessons Learned

Challenges in Physical Security

Relying solely on generalized threat information

Real-World Findings and Lessons Learned

Identified Gaps

Entities may replicate attack methodologies directly from general information sources like E-ISAC without considering the unique attributes and vulnerabilities of their specific site. This can lead to misallocated resources on unlikely threats, such as vehicle borne improvised explosive devices (VBIED) at facilities with no history or contextual likelihood of such attacks.

Real-World Findings and Lessons Learned

Best Practices Derived from Audits

- Customized threat analysis
- Rational threat prioritization
- Dynamic threat assessment process
- Continuous learning and adaptation

Real-World Findings and Lessons Learned

By integrating these best practices, entities can ensure their security assessments fully account for each facility's unique characteristics, leading to more effective and targeted security plans that address specific vulnerabilities and threats. This approach not only enhances compliance with NERC CIP-014-3 R4, but also significantly improves the overall security posture of critical infrastructure.

Real-World Findings and Lessons Learned

Common Audit Findings: Challenges & Gaps

Real-World Findings and Lessons Learned

Challenges in Physical Security

Inadequate response timeline development

Real-World Findings and Lessons Learned

Identified Gaps

Entities often implement security measures without properly analyzing or testing their effectiveness in real-time scenarios, leaving uncertainties in their capacity to mitigate threats within actionable timelines.

Real-World Findings and Lessons Learned

Best Practices Derived from Audits

- Realistic threat simulation
- Detailed response timing analysis
- Adaptive security adjustments
- Continuous testing and documentation
- Compliance through preparedness

Real-World Findings and Lessons Learned

By adhering to these best practices, entities can ensure they develop a clear, realistic, and effective timeline for responding to threats, closing the gap between theoretical security measures and their practical application in safeguarding critical infrastructure.

Real-World Findings and Lessons Learned

Common Audit Findings: Challenges & Gaps

Real-World Findings and Lessons Learned

Challenges in Physical Security

Inappropriate selection of third-party reviewers

Real-World Findings and Lessons Learned

Identified Gaps

Not all professionals holding CPP or PSP certifications may possess the specific expertise required for CIP-014 reviews. Additionally, independence issues arise when entities hire the same UTPR to both write and review R4/R5, leading to potential conflicts of interest and biased assessments in R6.

Real-World Findings and Lessons Learned

Best Practices Derived from Audits

- Industry peer consultation
- Review historical performance
- Understand noncompliance consequences
- Build a networking community
- Assess reviewer’s independence

Real-World Findings and Lessons Learned

By following these best practices, entities can more effectively select third-party reviewers who are not only qualified but unbiased and capable of providing insightful, constructive feedback that contributes to the security and reliability of the BES.

In Closing…

Recap of Key Takeaways

Document, Test, and Adapt

Ensuring compliance across NERC CIP-003-8, CIP-006-6, and CIP-014 requires rigorous documentation, regular testing of security measures, and adaptation based on findings. This approach secures not just compliance, but the resilience of physical security systems against evolving threats.

Customize Security to Asset Specifics

Tailor security strategies to the unique aspects of each facility covered by the different standards. Understanding the specific vulnerabilities and threats to low impact assets, PSPs, and critical transmission facilities enables more effective and targeted protective measures.

Continuous Improvement and Collaboration

Emphasize a culture of continuous improvement and sector-wide collaboration, sharing insights and learning from incidents to enhance physical security measures. This collective wisdom approach helps entities stay ahead of threats and aligns practices with the dynamic nature of security challenges.

Questions and Discussion

We encourage your questions and participation in discussions.

WECC

Electric Reliability and Security for the West

www.wecc.org