NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Standards Drafting Team Update

Michael Assante, VP & Chief Security Officer
North American Electric Reliability Corp.

February 3, 2008

to ensure the reliability of the bulk power system

Overview

- About NERC
- Project Background
- Proposed Modifications to Existing Standards
- New Asset Implementation Plan
- Technical Feasibility Exception Proposal
- Questions and Answers

About NERC: Mission

To ensure the reliability of the North American bulk power system

- Develop & enforce reliability standards
- Assess current and future reliability
- Analyze system events & recommend improved practices
- Encourage active participation by all stakeholders
- Pursue mandatory standards in all areas of the interconnection
- Operate the ES-ISAC

About NERC: ES-ISAC

- Monitors the bulk power system
- Provides:
  - Leadership
  - Coordination
  - Technical Expertise
  - Assistance


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Recommendation to Industry
CIP: Microsoft Out-of-Band Security Bulletin MS08-067

Initial Distribution: October 24, 2008
Additional Information Distributed: November 20, 2008

Limited Exploitation of Vulnerability Has Occurred. Final Reporting Requirements Below.

Status: Acknowledgment of Receipt & Reporting Required By December 2, 2008.
Instructions for acknowledging receipt have been sent to the primary compliance contact.

PUBLIC: NO HANDLING RESTRICTIONS
More on handling >>

Instructions: This NERC Recommendation is not the same as a reliability standard, and your organization will not be subject to penalties for a failure to implement this Recommendation. However, pursuant to Rule 810 of NERC's Rules of Procedure, you are required to report to NERC on the status of your activities in relation to this recommendation. For U.S. entities, NERC will compile the responses and report them to the Federal Energy Regulatory Commission.

Issuance of this Recommendation does not lower or otherwise alter the requirements of any approved Reliability Standard, or excuse the prior failure to follow the practices discussed in the Recommendation if such failure constitutes a violation of a Reliability Standard.

Distribution: As posted on www.nerc.com
All Registered Entities

Who else will get this alert? >>
What are my responsibilities? >>

Primary Interest Groups: Generation, Transmission, Control Centers, SCADA, EMS; Users of Microsoft Windows Platforms

Recommended Action: All recipients of this Recommendation should review the materials provided by Microsoft and determine appropriate mitigating steps to address this vulnerability. Recipients should note that not all mitigations and workarounds (specifically blocking ports or disabling services) from the MS08-067 bulletin are appropriate for control systems. All recipients of this Recommendation should contact their control system (EMS, SCADA, Substation Automation, Plant Control, etc.) vendors to determine what actions are recommended or appropriate for their particular environments.

Appendix A: Report on Recommendation to Industry
R-2008-10-24-F: CIP: Microsoft Out-of-Band Security Bulletin

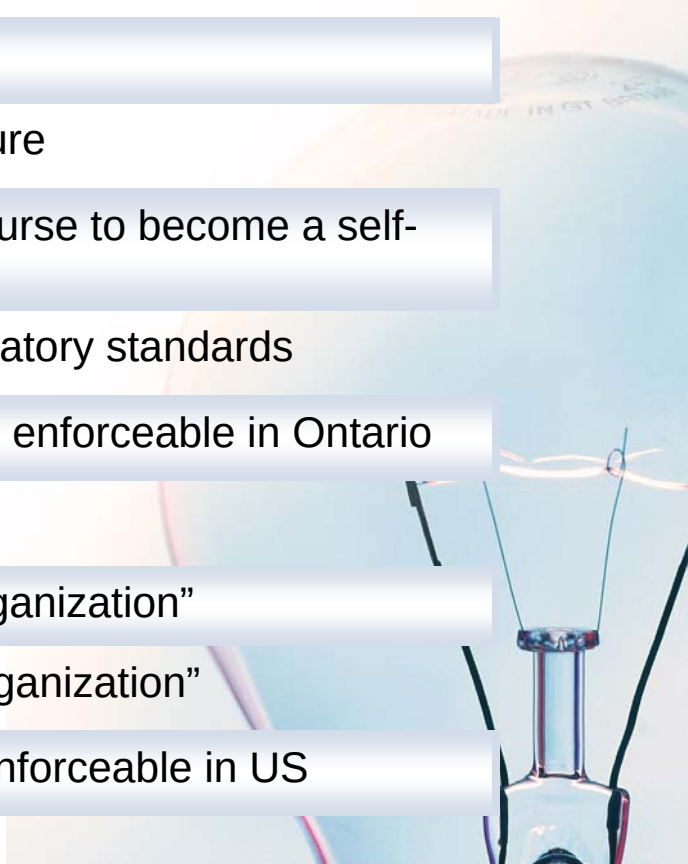
9

- Issues advisories, recommendations, & essential action notifications

About NERC: Reliability History

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

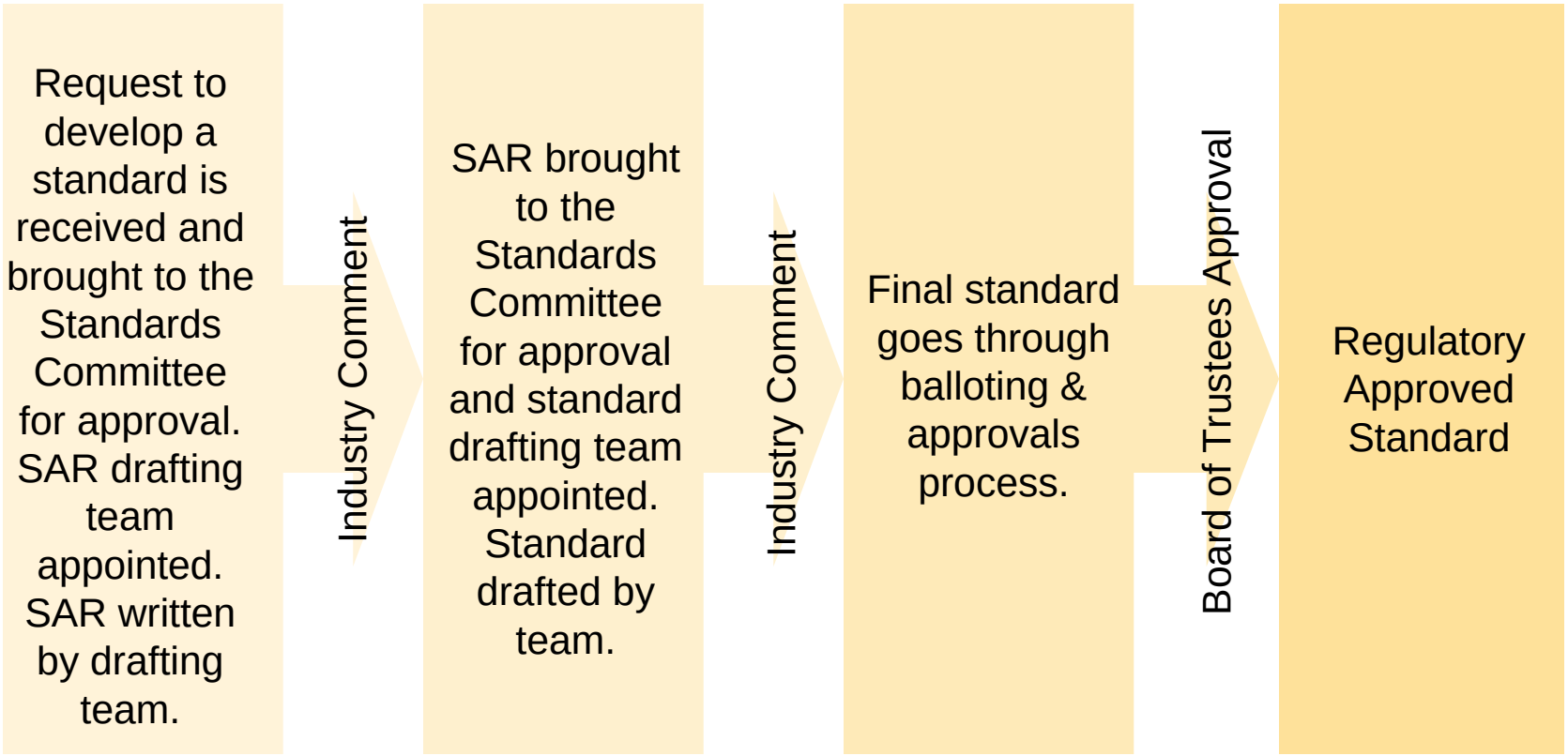
1965	Northeast Blackout I
1968	NERC formed
1978	National Energy Act – NERC Expands
1980	NERC Merges with NAPSIC
1987	National Electric Security Committee
1992	Energy Policy Act - NERC action plan for the future
1996	FERC orders on open access put NERC on a course to become a self-regulatory reliability organization
1997	NERC/DOE “Blue Ribbon” Panel suggests mandatory standards
2002	First reliability standards become mandatory and enforceable in Ontario
2003	Northeast Blackout II
2005	Energy Policy Act creates “Electric Reliability Organization”
2006	NERC applies & becomes “Electric Reliability Organization”
2007	First reliability standards become mandatory & enforceable in US



About Reliability Standards

- Focus on bulk power system reliability
  - No market practices
  - Minimum distribution system requirements
- Results-oriented
  - Avoid prescribing practices – allow entities to determine their own “best way” to meet a standard given their individual circumstances
  - Encourage innovation in compliance
  - Specific & measurable requirements
- Starting point for industry implementation

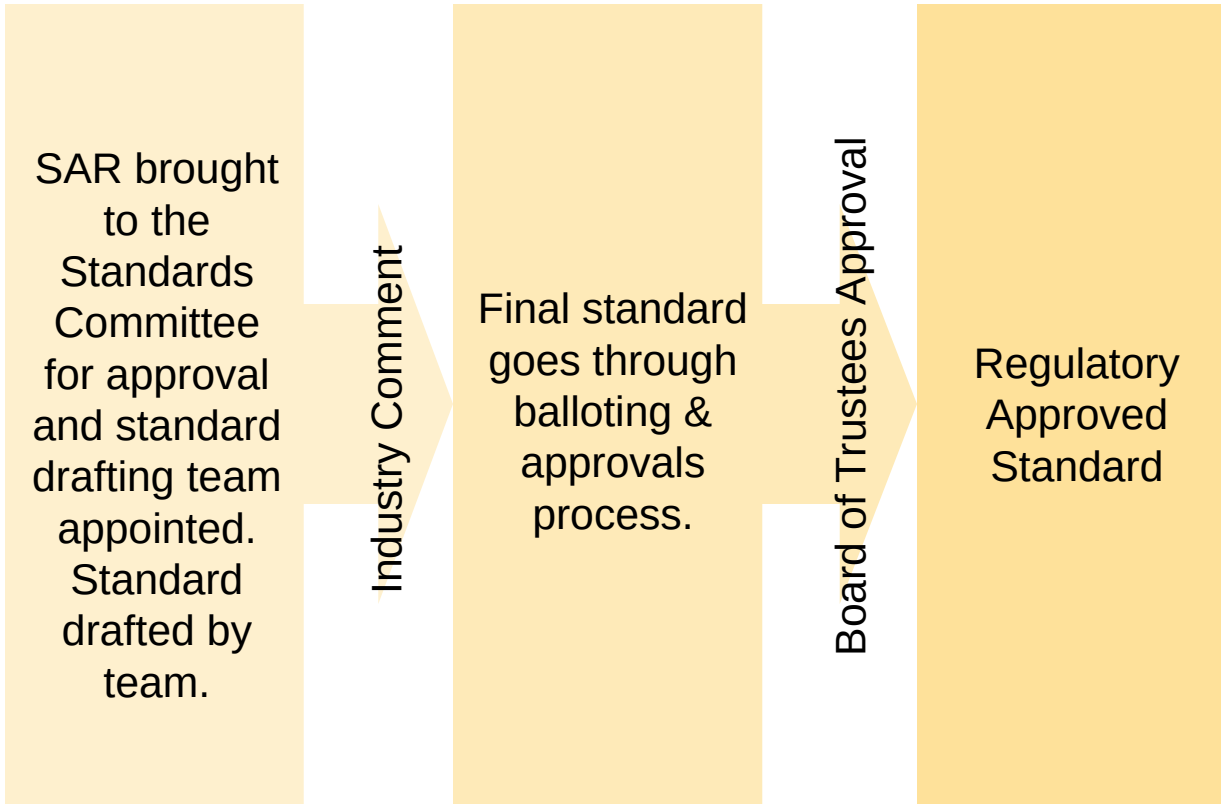
Standards Development Process



Standards Development Process

Open & Transparent Process

- ANSI Accredited Standards Process
- Standards Committee is nominated and elected by the industry.
- Every comment received during the commenting phase is considered and responded to.
- NERC guides and facilitates the process



Development Process: Approval

- Initial ballot and recirculation ballot
  - Recirculation required if one or more negative votes with comments is submitted on first ballot
- **Quorum is 75% of ballot pool**
- Stakeholder approval **requires ≥ 2/3** affirmative vote using weighted segment voting
- Board adoption
- Regulatory approval

CIP Standards Background

Background

- January 17, 2008 – FERC Order 706
  - Final rule approves NERC CIP Cyber Security standards
  - Directs ERO to develop modifications concerning a number of oversight and technical issues related to cyber protections
  - Directs NERC to monitor NIST cyber security standards to “determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards”

Background

- July 10, 2008 – Approval of SAR for developing revisions to CIP Cyber Security Standards:
  - CIP-002-1 Critical Cyber Asset Identification
  - CIP-003-1 Security Management Controls
  - CIP-004-1 Personnel and Training
  - CIP-005-1 Electronic Security Perimeter(s)
  - CIP-006-1 Physical Security
  - CIP-007-1 Systems Security Management
  - CIP-008-1 Incident Reporting and Response Planning
  - CIP-009-1 Recovery Plans for Critical Cyber Assets

Background

- August 7, 2008 – Standards Drafting Team appointed to review CIP Cyber Security Standards
  - Address directed modifications identified in FERC Order 706
  - Conform to current ERO Rules of Procedure
  - Consider other cyber security standards and guidelines (e.g., NIST, ISO, ISA, IEC, DOE, CIPC)
  - Consider stakeholder issues identified in the SAR comment process

Background

- October 2008 – Standards Drafting Team (SDT) adopts a multi-phase approach for revising the CIP Cyber Security standards
  - Phase I addresses date-driven directives included in FERC Order 706, clarifications, and conformance edits approved by 75% of the SDT
  - Later phase(s) will address more controversial cyber security issues

Schedule – Phase I

- Phase I dates (tentative):
  - Post for Industry Comment: Nov 21, 2008 – Jan 5, 2009
  - Respond to Comments: Jan 7 – Feb 5, 2009
  - Pre-ballot posting: Feb 5 – March 9, 2009
  - Initial Ballot: March 9 – March 19, 2009
  - Respond to Comments: March 20 – April 2, 2009
  - Recirculation Ballot: April 3 – April 13, 2009
  - BoT Review: April 20 – May 20, 2009
  - BoT Approval: around May 21, 2009
  - Submit to Regulators: June 10, 2009

Schedule – Phase II

- Phase II Schedule (tentative and estimate):
  - Develop Modifications 1Q09
  - Post Draft 1 & Respond to Comments: 2Q09
  - Post Draft 2 & Respond to Comments: 3Q09
  - Post Draft 3 & Respond to Comments: 4Q09
  - Post Draft 4 & Respond to Comments: 1Q10
  - Post Draft 5 & Respond to Comments: 2Q10
  - Post and Ballot: 3Q10
  - Finalize, approve & Submit to Regulators: 4Q10

Proposed Modifications to Standards

Phase I Posting Details

- As directed in Order 706:
  - Purpose Section: Removed the term “reasonable business judgment”
  - Where applicable, removed the phrase “acceptance of risk”
- To comply with ERO Rules of Procedure:
  - Applicability: Added Regional Entity, in place of Regional Reliability Organization

Phase I Posting Details

- Effective Date section updated to integrate implementation timeframe for CIP 002-2 through CIP 009-2
- Versioning
  - Phase I changes to existing version will be reflected as CIP 002-2 through CIP 009–2
- Administrative edits to reflect changes in numbering references

Phase I Posting Details

- Requirements
  - Modifications to remove extraneous information, improve readability, and bring the compliance elements into conformance with the latest guidelines
  - Where sub-requirements were numbered, but not all required, numbers were replaced with “bullets”
- Measures
  - Format of measures modified to conform to format used in other standards

Phase I Posting Details

- Compliance Elements
  - Compliance elements of standard updated to reflect language used in the ERO Rules of Procedure
  - Term, “Compliance Monitor” was replaced with “Compliance Enforcement Authority”
  - Term, “Regional Reliability Organization” was replaced with “Regional Entity”
  - Compliance Monitoring and Enforcement Processes were added
  - Monitoring Time Period and Reset Periods were marked as “not applicable”
  - Data Retention section was updated

Phase I Posting Details

- CIP 002 Critical Cyber Asset Identification
  - As directed in Order 706:
    - R4 Annual Approvals: Adds that senior manager shall annually review and approve the risk-based assessment methodology

Phase I Posting Details

- CIP 003 Security Management Controls
  - Simplification:
    - R2.1 Leader Identification: Removes business phone and business address designation.
  - As directed in Order 706:
    - Applicability 4.2.3: Requires Responsible Entities having no Critical Cyber Assets to comply with CIP 003-2 R2.
    - R2 Leadership: Require the designation of a single manager, with overall responsibility and authority for leading and managing the entity's implementation of CIP.
    - R2.3: Where the assigned senior manager delegates authority, the delegation must be in writing.

Phase I Posting Details

- CIP 004 Personnel and Training
  - Clarification to assure that requirement must be implemented:
    - R1. Awareness: Explicitly require implementation of Awareness Program.
    - R2. Training: Explicitly require implementation of the Training Program.

Phase I Posting Details

- CIP 004 Personnel and Training
  - As directed in Order 706:
    - R2.1 Training: Personnel having access to Critical Cyber Assets must be trained prior to their being granted such access, except in specified circumstances, such as an emergency. (Was 90 days, adds provision for emergency situations.)
    - R3 Personnel Risk Assessment: Personnel risk assessment shall be conducted prior to granting personnel access to Critical Cyber Assets except in specified circumstances such as an emergency. (Was 30 days, adds provision for emergency situation.)

Phase I Posting Details

- CIP 005 Electronic Security Perimeter(s)
  - Clarification:
    - Clarifies the scope of this requirement to include Cyber Assets used in either access control and/or monitoring to the Electronic Security Perimeter.
  - Clarification to assure that requirement must be implemented:
    - R2.3 Electronic Access Controls: Explicitly requires the implementation of the procedure to secure dial up access to the Electronic Security Perimeter.

Phase I Posting Details

- CIP 006 Physical Security Perimeter(s)
  - Restructuring of Requirements:
    - Former requirement R1.8 moved and incorporated into new Requirement R2 (Protection of Physical Access Control Systems) as Requirement R2.2.
    - Other modifications to Requirements R1.1 through R1.8 for readability.
    - Requirement referencing changed to reflect moved requirements
  - Clarifications to assure that requirement must be implemented:
    - R1. – R1.8 Physical Security Plan: All requirements of the Physical Security Plan must be implemented.

Phase I Posting Details

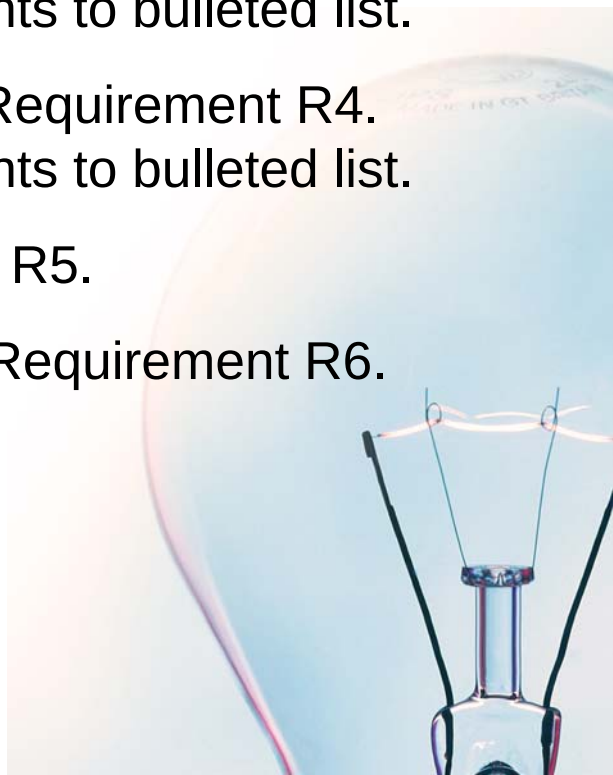
- CIP 006 Physical Security Perimeter(s)
  - As directed in Order 706:
    - R1.7 Updates to the Physical Security Plan: Shortens the time for updates to the Physical Security Plan to thirty calendar days (was 90 days), and adds the word “completion” to the requirement.
    - R1 Physical security Plan: Changes the term “a senior manager” to “the senior manager.”

Phase I Posting Details

- CIP 006 Physical Security Perimeter(s)
  - Additional Clarifications:
    - R1.6 Escorted Access: Clarified that the escort within a Physical Security Perimeter should continually remain with the escorted person.
    - R1.8 Annual Review: Formerly Requirement R1.9.
    - R2.2: Formerly R1.8. Changed references to requirement numbers as appropriate.
    - R4 Physical Access Controls: Formerly Requirement R2. Changes enumeration of sub requirements to bulleted list.

Phase I Posting Details

- CIP 006 Physical Security Perimeter(s)
  - Additional Clarifications:
    - R5 Monitoring Physical Access: Formerly Requirement R3. Changes enumeration of sub requirements to bulleted list.
    - R6 Logging Physical Access: Formerly Requirement R4. Changes enumeration of sub requirements to bulleted list.
    - Requirement R7: Formerly Requirement R5.
    - R8 Maintenance and Testing: Formerly Requirement R6.



Phase I Posting Details

- CIP 006 Physical Security Perimeter(s)
  - Requirements Added:
    - R2 Protection of Physical Access Control Systems: Moves requirement to protect Physical Access Control Systems out of Requirement R1 into its own requirement and excludes hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers from the requirement.
    - R2.1 Protection of Physical Access Control Systems: Adds requirement that Physical Access Control Systems be protected from unauthorized access.
    - R3 Protection of Electronic Access Control Systems: Adds that cyber assets used in access control and/or monitoring of the Electronic Security Perimeter shall reside within an identified Physical Security Perimeter.

Phase I Posting Details

- CIP 007 Systems Security Management
  - As directed in Order 706:
    - R2.3 Ports and Services: Removal of the term “or an acceptance of risk.”
    - R3.2 Security Patch Management: Removal of the term “or an acceptance of risk.”
    - R4.1 Malicious Software Prevention: Removal of the term “or an acceptance of risk.”
    - R9 Documentation Review and Maintenance: Shortens the time frame to update documentation in response to a system or control change to thirty calendar days (was 90 days) and further clarifies this timeframe to begin after such change is complete.

Phase I Posting Details

- CIP 007 Systems Security Management
  - Clarifications to assure that requirements must be implemented:
    - R2 Ports and Services: Explicitly requires the implementation of process to ensure only required ports and services are enabled.
    - R3 Security Patch Management: Explicitly requires the implementation of Security Patch Management program.
    - R7 Disposal and Redeployment: Explicitly requires the implementation of Cyber Asset disposal and redeployment procedures.

Phase I Posting Details

- CIP 008 Incident Response & Reporting
  - As directed in Order 706:
    - R1.4 Updating the Cyber Security Incident Response Plan: Shortens the timeframe to update the Incident Response Plan to thirty calendar days (was 90 days).
    - R1.6 Testing of the Incident Response Plan: Adds language to clarify that testing need not require a responsible entity to remove any systems from service.
  - Clarifications to assure that requirements must be implemented
    - R1 Incident Response Plan**:** Explicitly requires implementation.

Phase I Posting Details

- CIP 009 Recovery Plans
  - As directed in Order 706:
    - R3 Change Control: Shortens the timeframe for communicating updates to Critical Cyber Asset recovery plans to thirty calendar days (was 90 days) of the change being completed.

New Asset Implementation Plan

Newly Identified Critical Cyber Assets

- Current gap in the CIP standards is compliance of newly identified Critical Cyber Assets.
  - Once “compliant” date reached in Version 1 implementation plan, newly identified Critical Cyber Asset is expected to be immediately fully compliant.
  - The SAR recognizes that the industry may need some time to apply certain CIP standards requirements to newly identified Critical Cyber Asset.
- New plan addresses the issue and allows time to come into compliance.

Newly Identified Critical Cyber Assets

- Three classification categories identified:
  1. Previously registered Responsible Entity identifies its first Critical Cyber Asset under CIP standards. To this point, the entity does not have a compliance program in place and needs time to build the program.
  2. A compliance program is in place and an existing Cyber Asset becomes subject to the CIP standards, *not as a result of a planned change to the Cyber Asset or network environment*.
  3. A compliance program is in place and an existing Cyber Asset becomes subject to the CIP standards *as a result of a planned change*.

Newly Identified Critical Cyber Assets

- First Critical Cyber Asset (Category 1).
  - Responsible Entity currently required to comply with all requirements of CIP-002.
    - Version 1 implementation plan may still be in effect
      - Table 3 requires full compliance by December 31, 2009).
      - May be coincident with Responsible Entity registration, invoking Table 4 of the Version 1 implementation plan.
  - Identification starts the 24 month clock to build a compliance program for CIP-003 through CIP-009.
    - Compliance date is later of Version 1 implementation plan or 24 months from identification of first Critical Cyber Asset.

Newly Identified Critical Cyber Assets

- New Critical Cyber Asset, *not as a result of a planned change* (Category 2).
  - Examples of unplanned change include existing asset, such as generation or transmission, identified as Critical Asset due to change in system conditions or risk assessment methodology.
- Responsible Entity already subject to requirements of CIP-003 through CIP-009.
  - Later of in-effect initial implementation plan or zero to 12 months to comply with identified standards requirements following identification of Critical Cyber Asset or other Cyber Asset within the ESP.

Newly Identified Critical Cyber Assets

- New Critical Cyber Asset, *as a result of a planned change* (Category 3).
  - Examples of planned change include deployment of new Cyber Asset, reconfiguration of existing Cyber Asset, hardware or software upgrade, or network reconfiguration.
- Responsible Entity already subject to requirements of CIP-003 through CIP-009.
  - Later of in-effect initial implementation plan or immediate compliance with all standards requirements upon deployment of the Critical Cyber Asset or other Cyber Asset within the ESP.

Other Considerations

- Construction of *new* Critical Asset or upgrade/replacement of existing Critical Asset.
  - Identification of asset as Critical Asset is part of the planning process. This is normally considered a *planned* change once a CIP standards compliance program is in place.
    - A change of system conditions or risk assessment methodology could cause an asset to be determined to be a Critical Asset after construction has commenced.
  - Identification of Critical Asset invokes appropriate schedule for CIP standards compliance as previously described.

Other Considerations

- Mergers and Acquisitions
  - First Critical Cyber Asset category is applicable if neither party already has Critical Cyber Assets identified.
  - Otherwise, entities have:
    - One year from closing to evaluate merging of programs.
    - Followed by invocation of Category 2 (zero to 12 months to comply with identified Standards requirements).
- Restoration as part of a disaster recovery situation shall follow the emergency provisions of the Responsible Entity's CIP standards compliance policy (CIP-003, Requirement R1).

Key Expectation

Documentation is critical to this process. The Responsible Entity must be able to demonstrate which implementation schedule and corresponding compliance set of dates is applicable on a per-Cyber Asset basis.

Seeking Input

- Should the New Critical Cyber Asset implementation pan be incorporated into the CIP standards or retained as a separate document?
- To incorporate into the CIP standards:
  - New requirement in CIP-002 to classify newly identified Critical Cyber Assets and other Cyber Assets within the ESP.
  - Milestone timeframes for each standard requirement incorporated into the Compliance section of each standard.
  - Table 4 of the Version 1 Implementation Plan would also be incorporated into the standards.

Technical Feasibility Exception Proposal

Technical Feasibility Exceptions

- Technical Feasibility Exceptions (TFE) introduced in CIP Standards
  - An “Exception” not an “Exemption”
  - Compliance is still required, through the use of the TFE
- Used where compliance is not possible or feasible due to *technical* reasons
  - Includes operational and safety concerns (FERC Order 706 ¶186)
  - “Funding Availability” as a reason for extending compliance date being discussed

Technical Feasibility Exception Process

- Broad requirements for TFE described in FERC Order 706 (¶222)
  - NERC Staff developing whitepaper to fill in details and describe process and expectations
- Process modeled after existing Self-Report and Mitigation Plan processes in the Compliance Monitoring and Enforcement Program (CMEP)
  - Documented in NERC Rules of Procedure Section 400 and Appendix 4C

FERC Order 706 Requirements

- Identification of specific conditions for invoking a technical feasibility exception (¶106, ¶178).
  - Preferable alternative to acceptance of risk (¶151).
  - Provides for documentation, reporting and approval of how responsible entities have elected to comply with the CIP Reliability Standards (¶152).
  - Would permit the ERO and Regional Entities to assess the significance of any possible vulnerability (¶152).
  - Should not be limited simply to whether something is technically possible but also whether it is technically safe and operationally reasonable (¶152, ¶182).

FERC Order 706 Requirements

- Specific documentation components (¶192).
  - The responsible entity must develop, document and implement a mitigation plan that achieves a comparable level of security to the Requirement.
  - Use of the technical feasibility exception by a responsible entity must be accompanied by a remediation plan and timeline for elimination the use of the technical feasibility exception.
  - An entity must provide an explanation when it believes that it is not possible for a remediation plan to provide a reasonable completion date.

FERC Order 706 Requirements

- Regular review and approval.
  - Approval of the mitigation and remediation steps by the senior manager (identified pursuant to CIP-003-1) (¶211).
  - An approval process requiring the ERO or a Regional Entity to approve any technical feasibility exception, taking into account whether the technical feasibility exception is needed and whether the mitigation and remediation steps are adequate to the circumstance (¶218).
  - Submission of an annual report by the ERO to the Commission that provides a wide-area analysis regarding use of the technical feasibility exception and the effect on Bulk-Power System reliability (¶220).

Technical Feasibility Exception process

- Many elements the same as existing CMEP process
  - In-take process
  - Accept / Approval process
  - Appeals
- Some significant changes
  - Long-term remediation plans allowed
  - Requirement for ERO analysis of combined TFE requests

Technical Feasibility Exception Requests

- Identification of NERC Standard Requirement that cannot be met
- Justification for TFE
- Description of compensating or mitigating controls implemented to remediate risk associated with the exception
- Remediation plan describing how the entity will become compliant with the requirement
  - Plans may be multi-year, indeterminate, or open-ended
- Approval by Entity Senior Manager

Technical Feasibility Exception Process

- TFE request and remediation plan is analyzed and accepted by Regional Entity
- TFE request and remediation plan is analyzed and approved by ERO
- TFEs must be re-submitted annually
- The ERO is required to develop an annual report analyzing the wide-area effect of all approved TFEs on the reliability of the BPS (¶220)

Technical Feasibility Exception Process

- Implementation of compensations and remediation plan may be subject to audit
- Information contained in TFE requests may be sensitive, and will be protected following NERC's Rules of Procedure section 1500 (Confidential Information)
- All requests for Hearing and Appeal of decisions made during an approval process will follow the existing Rules of Procedure as described in Appendix 4C

Cautions

- Entities filing TFEs may face expedited audits (¶215)
- Entities not following the process may face findings of potential non-compliance
- Entities not following self-imposed milestones in mitigation plans may face finding of potential non-compliance
  - Updates to plans allowed when requested with acceptable justifications
- Entities not providing sufficient access to information pertaining to the TFE may face finding of potential non-compliance

Next Steps

- Whitepaper describing process proposal is being developed by NERC staff with input from the Standards Drafting Team
- Whitepaper will likely be posted for industry comment prior to subsequent actions
  - Posting intended for 1Q09
  - Process is outside Standards Development posting and response process

Next Steps

- After further refinement, the whitepaper will be turned into a Rules of Procedure Proposed Amendment
  - NERC Board of Trustees (BoT) approval following stakeholder comments and consideration of the NERC Member Representatives Committee
  - Following BoT approval, filed with appropriate government regulators for their approval
  - Process becomes effective following government regulator approval

Next Steps

- ERO expects TFE submission prior to Compliant date
  - Need to determine timing for entities that reached Compliant stage prior to TFE process approval

Question & Answer

Contacts:

Michael Assante
michael.assante@nerc.net
609.524.7049