NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Standards: Development Proposal

Scott Mix, CISSP

Manager of Situation Awareness and Infrastructure Security

SDT Kickoff Meeting

NIST Headquarters

October 6, 2008

to ensure the reliability of the bulk power system

VSL Development

- VSLs now required for each requirement of a standard (currently also for sub-requirements)
- Project Team to complete VSLs for approved (existing) standards has formed
- Announcement at September 22-23, 2008 Standards Committee meeting
- Note: VSL (and VRF) development for revised standards will be developed by SDT as part of the normal standard development process (this process)

CIP Auditor Training

- NERC is developing training for NERC and Regional compliance auditor staff
  - Restricted to NERC and Regional Compliance Audit staff
- Multiple training sessions have been scheduled for the remainder of this year, and early next year

Future Plans

- All very tentative pending discussions with SDT
  - Meet Face-to-Face every other week ~2 – 3 days
  - Teleconference / WebEx capability at meetings
  - Proposing 3 (3+) phases
    1. "Low Hanging Fruit", high priority items
    2. Majority of issues
    3. Large, challenging issues

       3+ Extremely large and challenging issues
- Guidelines will need to be addressed

Development Schedule

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Three development phases
  1. Low Hanging Fruit and High Priority Items
     - “Easy” and “Need-to-do” issues
     - Complete to Commission in 6 months (March, 2009)
  2. Majority of Issues
     - Not hard, but lots of them
     - Complete and to Commission 18 months following #1 (October 2010)
  3. Challenging Issues
     - Expect difficulty in reaching consensus
     - Following #2 (exact time depends on how many and how hard)

Guidelines

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- FERC Order 706 provides for the development of reference documents (guidelines) to assist with compliance
  - Guidelines are not Standards nor Requirements
  - Compliance with a guideline is optional
- About 25 guideline topics have been identified in the order
- The SDT will need to determine whether a topic should be addressed through a guideline, modifications to the requirements of a standard, or both
  - Choice must be made on a topic by topic basis
  - Guideline development will be controlled by the SDT's decision on these options

Process

- Develop modifications to Standards Language
  - Requirements, Measures, etc
- Develop VRF / VSL for requirements
  - Effort for existing standards as a starting point
- Develop implementation timeline and effective date
  - Less complicated than existing implementation plan
  - Tie to FERC approval date?
  - Tie to existing implementation plan timeline?
- Industry review and comment
- Industry Ballot
- BoT Approval
- Submit to Commission

Low-Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Mostly non-contentious issues
- Initial edits “easy”
  - But final language may not be
- NERC Staff proposal for consideration by the SDT
- Other areas may be added so long as they do not adversely effect the schedule

Phase 1 schedule

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Working backwards:
  - Submit to Commission (end of) March 2009
  - BoT approval March 23
  - BoT notice Feb 20 (30 days)
  - Second Ballot Feb 5 (includes responses to comments)
  - First Ballot Jan 15
  - Ballot posting Dec 15 (30 days) (includes responses to comments)
  - Draft to industry for comments on October 30 (45 days)
- May be able to cut back on some posting timeframes (but not all)

Need-to-do issues

- Reasonable Business Judgment
  - NERC Staff edit to remove sentence in all standards
- Critical Asset Identification
  - Needs work
  - See Critical Asset Identification Guideline for ideas
- Risk Acceptance / Technical Feasibility
  - Needs Work
  - NIST Framework for ideas
  - NERC Filings to FERC for ideas

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Proposed edits done by NERC Staff
  - Minor formatting (version numbers, etc)
  - Removal of “Reasonable Business Judgment” language from all standards
  - Change “Regional Reliability Organization” to “Regional Entity”
    - Question: do we need to keep both?
  - No work preformed on Measures or Compliance sections

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-002
  - Newly identified Critical Assets
  - Newly identified Critical Cyber Assets
  - Senior Manager approval of Risk-based Asset Identification Methodology
  - Reliability Coordinator approval of lists

Low Hanging Fruit

- CIP-003
  - Clarification of who the Senior manager is
  - Senior Manager Delegation process
  - Escorting clarification

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-004
  - “Implement” awareness and training programs
  - Clarification for training program
  - Train prior to access
  - Additional mandatory elements of training program
  - PRA prior to access
  - PRA clarifications for new hires and emergencies

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-005
  - Implement secure dial-up procedure
  - Update documentation in 30 days (from 90)

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-006
  - Implement Physical Security plan and physical security procedures
  - Update procedures in 30 days (from 90)

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-007
  - Implement procedures
  - Update documentation in 30 days (from 90)

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-008
  - Implement procedures
  - Update procedures in 30 days (from 90)
  - Procedures for when documented procedures are not followed
  - Update of response plans for new situations
  - Clarification on testing – not required to remove equipment from service to test

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-009
  - Update procedures in 30 days (from 90)
  - Procedures for when documented procedures are not followed
  - Update of response plans for new situations

Need-do-do Issues

- Edits *not* performed by NERC staff:
  - Critical Cyber Asset identification updates (CIP-002)
  - Technical Feasibility and Risk Management (CIP-003)
- Work teams and schedules need to be developed at this meeting

Majority of Issues

- Lots of issues
  - List available
  - Everything that is neither a “Low Hanging Fruit” issues nor a “challenging” issue
- May include sub-phases
- Items may move into phase 3 if consensus cannot be reached in allocated timeframe
- Can start tackling some now if resources available

Challenging Issues

- May have 2 sub-phases
  - Will be based on SDT resource and industry comment
- Will include issues that we can't come to consensus with in phase 2
- Will take time to reach consensus in SDT
  - Will take longer to reach industry consensus
- Can start at any time (pending resources)
  - Should not hold up our ability to submit at the 18-month development milestone for phase 2

Challenging Issues

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Proposed list of Phase 3 issues:
  - Design Basis Threat (258) **
  - Misuse of control centers (282)
  - Non-routable protocols (285)
  - “immediate” revocation of access privileges (460, 461)
  - Two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter (496, etc)

** -- may be a Phase “3+”

Challenging Issues

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Exception process and demonstration of untolerable delays for defense in depth electronic security perimeter (498)
- Fail-safe defensive measures (500)
- Specific verification technologies, authentication technology in general (511)
- Use of encryption (511)
- Log review processes, response to log review alerts, log sampling (525 - 528)

Challenging Issues

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Vulnerability Assessments (541, 543, 544, 547)
- "Full live vulnerability Assessments" (542) **
- "Two or more different security procedures when establishing a physical security perimeter" (572 - 575)
- Test environment requirements (609 - 611)
- Safeguards against introduction of malware (621, 622)
- Log review procedures (628, 629)

** -- may be a Phase "3+"

Challenging Issues

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Vulnerability Assessments (643)
- Incident reporting (661)
- Mandatory government reporting (673, 675)
- Report time requirements (674, 676)
- Relationship between CIP-001 and CIP-008 (677)
- Forensic data practices (706 – 710)
- Recovery exercises (725)
- Backup, storage, testing of media (739 – 740, 748)

Questions

Scott Mix, CISSP
Manager of Situation Awareness
and Infrastructure Security
Scott.Mix@NERC.net
215-853-8204