NPCC Workshop
September 22 2010
Boston, MA
Standards CIP
For
New facility
Disclaimer

This NPCC TFIST workshop provides a forum for the presentation and discussion of member experience in the implementation of compliance programs for the NERC CIP Cyber Security Standards. Materials presented or discussed are the presenters’ own interpretation and recommendations and do not necessarily represent those of their organizations or NPCC.
Agenda

- **Critical asset or not ? CCA ?**
  - CIP-002

- **Classification and Information Protection**
  - CIP-003-3 R4 and R5 -Information Protection

- **Access during project**
  - CIP-005-3 Electronic and CIP-006-3 Physical

- **Requirements of the project**
  - CIP-004, CIP-005, CIP-006, CIP-007, CIP-008 and CIP-009

- **Update documentation (after project)**
  - CIP-004, CIP-005, CIP-006, CIP-007, CIP-008 and CIP-009
Agenda

- **Critical asset or not? CCA?**
  - CIP-002

- **Classification and Information Protection**
  - CIP-003-3 R4 and R5 - Information Protection

- **Access during project**
  - CIP-005-3 Electronic and CIP-006-3 Physical

- **Requirements of the project**
  - CIP-004, CIP-005, CIP-006, Cip-007, CIP-008 and CIP-009

- **Update documentation (after project)**
  - CIP-004, CIP-005, CIP-006, Cip-007, CIP-008 and CIP-009
Critical Asset or not? CCA?

• Before beginning the project, you should ask if the new (or modified) facility will be a critical asset?
• You should apply the standards when you connect the facility.
• With new facility, chance are pretty high that you will have Critical Cyber Asset (CCA) because new systems use IP.
• Even if it is not a Critical Asset, you should think of physical security (at least pass wires in wall during the construction) because, in future version, CA's definition may be changed (bright line).
Standards and Accepted Items

- **Critical asset or not? CCA?**
  - CIP-002

- **Classification and Information Protection**
  - CIP-003-3 R4 and R5 -Information Protection

- **Access during project**
  - CIP-005-3 Electronic and CIP-006-3 Physical

- **Requirements of the project**
  - CIP-004, CIP-005, CIP-006, Cip-007, CIP-008 and CIP-009

- **Update documentation (after project)**
  - CIP-004, CIP-005, CIP-006, Cip-007, CIP-008 and CIP-009
Classification and Information Protection

- **CIP-003-3, Security Management Controls**
  - **R4 - Information Protection**
    - The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
  - **R5 - Access Control**
    - The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
Identification

• R4.1 - The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.
NYISO Facility Modernization Project

Challenges

• Modernization of facilities under NERC CIP required process enhancements and new processes
• Facility, project management and executive support
• Practices with local and state government reviewed, examined, negotiated and implemented

Solutions

• Team Approach:
  Executives, Facility, Project Management, Legal, Security, Records Management and Compliance

• Process Developed
  – Education and awareness
  – Contracts and agreements
    • Agreement for Proposal Services
    • Master Agreements
    • Non Disclosure Agreements
Project Guidelines Scope

1. Definition of classifications
2. Process to classify project documents
3. Access and exchange of documents
   - Access
     * Project Team Members
     * Project Team Members and their Sub-Contractors and Vendors
   - Exchange processes
     * Hardcopy – Transmittal
     * Electronic - Encryption
4. Training for Project Team Members
NYISO Working with Government

Local and State Government

• Local Government
  – Local planning and zoning
  • FOIL
  – Emergency responders

• State Government
  – PSC proceedings and information requests
  – Mature and defined process
  – Hand-delivered materials

Process

• Education and awareness
  – Classification
  – Protection
  – Handling

• Negotiate
  – Protecting access and details
  – Obligations and requirements

• Agreements – NDA
  – Formal acknowledgement and protection of information
Conclusion

• Team approach support at all organization levels
• Education and awareness
• Partner with contractors, vendors and government
• Negotiate solutions
• Agreements
  – Agreements for proposal service
  – Non Disclosure Agreements
References

• FERC CEII

• NERC
  – CIP-003 R4
    • http://www.nerc.com/page.php?cid=2|20
  – Rules of Procedure Section 1500 – Confidential Information
    • http://www.nerc.com/page.php?cid=1%7C8%7C169
Agenda

- **Critical asset or not? CCA?**
  - CIP-002

- **Classification and Information Protection**
  - CIP-003-3 R4 and R5 - Information Protection

- **Access during project**
  - CIP-005-3 Electronic and CIP-006-3 Physical

- **Requirements of the project**
  - CIP-004, CIP-005, CIP-006, Cip-007, CIP-008 and CIP-009

- **Update documentation (after project)**
  - CIP-004, CIP-005, CIP-006, Cip-007, CIP-008 and CIP-009
Access during project

• For a new project, CIP Standards apply only when you connect the new facility.
• You should plan your access before connecting the facility because it is take time (create list, background check, training,...)
• For an update of a facility, or even a new facility, you should apply access requirements so that everyone knows the new rules
Agenda

- **Critical asset or not? CCA?**
  - CIP-002
- **Classification and Information Protection**
  - CIP-003-3 R4 and R5 - Information Protection
- **Access during project**
  - CIP-005-3 Electronic and CIP-006-3 Physical
- **Requirements of the project**
  - CIP-004, CIP-005, CIP-006, CIP-007, CIP-008 and CIP-009
- **Update documentation (after project)**
  - CIP-004, CIP-005, CIP-006, Cip-007, CIP-008 and CIP-009
Requirements of the project

• CIP-004
  – People who will access the facility (physical or electronic) (background check, training)
  – Explain to the contractor that access is given to people and not to function

• CIP-005
  – Need an electronic security perimeter
  – You need the flow of information of the system, especially at the point of control (PCS)
  – Make sure the system is compatible with what you already have
Requirements of the project

• CIP-006
  – Need an physical security perimeter
  – Make sure the system is compatible with what you already have

• CIP-008 & CIP-009
  – Make sure the system is compatible with what you already have or
  – Develop a new incident plan and continuity plan
Requirements of the project

- CIP-007, for each system (IT and OT), ask for
  - Test procedure and results (R1)
  - List (and explanation of ports and services (R2)). We talk of logical ports right now, but...
  - Update support (R3)
    - Do not be caught by your warranty!
  - Malicious Software Prevention (R4) or mitigation
  - Account Management that respect NERC requirement (R5) (and more) and your infrastructure
Requirements of the project

• CIP-007, for each system (IT and OT), ask for
  – List of type of message of the logs and compatibility with your log system (R6)
  – The process for disposal (R8) (and still have warranty)
  – Cyber Vulnerability Assessment as a criteria of acceptance (R8)
  – Documentation of the system to be compliant with NERC CIP (they should know) (R9)
Requirements of the project

• For each system (IT and OT), ask for
  – Any document to support TFE if a requirement cannot be support
  – Make sure you also compliance with your own policy
Requirements of the project

• New system or technology
  – With IED, SmartGrid, Wi-Fi, remote access,... you may need to change your policy, your critical asset criteria or list
  – Your vendor may ask for remote access to the system. How to do that and still be compliant, in control and secure

• Make contact during the break
  – With NERC Requirements, you are not alone on cyber / physical security. Ask your vendor how other companies deal with their product, consult their website for list of client... or better, make new contacts during the break with people who may have the same project!
Critical asset or not? CCA?
  - CIP-002

Classification and Information Protection
  - CIP-003-3 R4 and R5 - Information Protection

Access during project
  - CIP-005-3 Electronic and CIP-006-3 Physical

Requirements of the project
  - CIP-004, CIP-005, CIP-006, Cip-007, CIP-008 and CIP-009

Update documentation (after project)
  - CIP-004, CIP-005, CIP-006, Cip-007, CIP-008 and CIP-009
Update documentation (after project)

• Change management process

• Create (update) your list
  – CCA, logical and physical access, documents

• Create (update) your process
  – Incident respond
  – Backup and business continuity

• Create (update)
  – Schematic, floor plan, network plan, ...

• Update your list of document, classify and protect them
Questions ? Comments ?

• NYISO’s Facility Project – Information Protection
  – Greg Goodrich
• ConEd’s Facility Plan
  – John Lim
• TransEnergie Facility
  – Martin Ferland