

# **Risk-based Security Assessments:**

## ***A Perspective on How the Energy Industry in Complying with the Critical Infrastructure Protection Reliability Standard***

*Anita Tallarico, Certified Business Resilience Manager  
June 18, 2009*



1. The Requirement: NERC's Reliability Standard CIP 001-009
2. Research and Findings
3. My 3 Overall Findings
4. Recommendations

## Outline

## Disaster

*Over 50 million people were left without power on August 14, 2003, when a blackout cascaded across the Mid-West and Northeast U.S. and Canada within a matter of minutes. The Blackout challenged the energy industry and key agencies like DHS and DOE to react in a coordinated manner to the energy emergency.*

## The Requirement

*The North American Electric Reliability Corporation (NERC) responded to the event by developing a voluntary standard that the Federal Energy Regulatory Commission (FERC) adopted.*

*Compliance penalties for the Critical Infrastructure Protection (CIP) Reliability Standards for the electric energy industry began July 1, 2008 for parts of the industry, July 1, 2009 for additional segments of the industry, and so on.*

# The Reliability Standard CIP

## Requirements

- CIP-001-1 Sabotage Reporting
- CIP-002-1 Critical Cyber Asset Identification
- CIP-003-1 Security Management Controls
- CIP -004-1 Personnel and Training
- CIP-005-1 Electronic Perimeter(s)
- CIP-006-1 Physical Security
- CIP-006-1a 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

**The Reliability Standard for CIP**

## Requirement CIP-001

### Sabotage Reporting

- R1. Have procedures for the recognition of sabotage on single and multiple facilities affecting the Interconnection.
- R2. Have procedures for the communication of information to parties in the Interconnection.
- R3. Provide emergency contact information and emergency response procedures to operations personnel.
- R4. Develop reporting procedures with FBI or Royal Canadian Mounted Police as appropriate.

**The Reliability Standard for CIP**

## Requirement CIP-002

### Critical Cyber Asset Identification

- R1. Identify and document a risk-based assessment methodology to use to identify Critical Assets.
- R2. Develop a list of assets through an annual application of the risk-based assessment methodology.
- R3. Develop a list of associated Critical Cyber Assets.
- R4. Approve the list of Critical Assets and Critical Cyber Assets annually by senior management.

**The Reliability Standard for CIP**

## Requirement CIP-003

### Security Management Controls

- R1. Document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
- R2. Assign a senior manager for leading and managing the entity's implementation of and adherence to 002-009.
- R4. Implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
- R5. Document and implement a program for managing access to protected Critical Cyber Asset information.
- R6. Establish a process for document, change control, and configuration management, for Critical cyber Asset hardware or software.

# The Reliability Standard CIP

## Requirement CIP-004

### Personnel and Training

- R1. Establish, maintain, and document a security awareness program to ensure personnel having physical access receive on-going training in sound security practices on a quarterly basis.
- R2. Establish, maintain, and document an annual cyber security training program for personnel with access to cyber assets.
- R3. Have a documented personnel risk assessment program in accordance with f/s/l laws, for personnel with access to cyber assets.
- R4. Maintain lists of personnel with access to cyber assets including their electronic and physical access rights to assets.

## The Reliability Standard CIP

## Requirement CIP-005

### Electronic Security Perimeter

- R1. Ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. Identify and document the Perimeter and all its access points.
- R2. Implement and document the organizational processes and mechanisms for control of electronic access at all electronic access points to the Perimeter.
- R3. Implement and document electronic or manual processes for monitoring access points 24/7.

**The Reliability Standard CIP**

## Requirement CIP-005

### Electronic Security Perimeter (cont'd.)

- R4. Perform a cyber vulnerability assessment of the electronic access points to the Perimeter annually.
- R5. Review, update, and maintain all documentation to support compliance with this standard.

**The Reliability Standard CIP**

## Requirement CIP-006

### Physical Security

- R1. Create and maintain a physical security plan, approved by a senior manager.
- R2. Document and implement the controls to manage physical access at all access points to the Physical Security perimeter 24/7.
- R3. Document and implement the controls for monitoring physical access at all point to the Perimeter 24/7. Unauthorized access shall be reviewed immediately and handled I/A/W CIP-008.

**The Reliability Standard for CIP**

## Requirement CIP-006

### Physical Security (cont'd.)

- R4. Record sufficient information to uniquely identify individuals and the time of access 24/7. Log physical entry at all access points.
- R5. Retain physical access logs for at least 90 calendar days or in accordance with CIP-008.
- R6. Implement a maintenance and testing program to ensure that all security systems function properly.

**The Reliability Standard for CIP**

## Requirement CIP-007

### Systems Security Management

- R1. Ensure that new cyber assets and significant changes to existing assets within the Perimeter do not adversely affect cyber security controls, e.g., patches, service packs, version upgrades.
- R2. Establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
- R3. Establish and document a security patch management program for tracking, evaluating, testing, and installing cyber security software patches for all assets within the perimeter.

**The Reliability Standard for CIP**

## Requirement CIP-007

### Systems Security Management (cont.)

- R4. Use anti-virus software prevention tools to detect, prevent, deter, and mitigate the exposure of malware on all assets within the Perimeter.
- R5. Establish, implement, and document controls that enforce access authentication of and accountability for all user activity.
- R6. Ensure that all assets within the Perimeter have automated controls to monitor system events.

**The Reliability Standard for CIP**

## Requirement CIP-008

### Incident Reporting and Response Planning

- R1. Develop and maintain a cyber security incident response plan.
- R2. Keep relevant documentation related to cyber security incidents reportable per R.1.1 for 3 calendar years.

**The Reliability Standard for CIP**

## Requirement CIP-009

### Recovery Plans for Critical Cyber Assets

- R1. Create and annually review recovery plans for critical cyber assets.
- R2. Exercise recovery plans annually. They can range from a paper drill to a full operational exercise, to recovery from an actual incident.
- R3. Update plans to reflect changes or lessons learned and updates communicated to affected personnel within 90 days of change.
- R4. Include procedures for backup and storage of information required to restore cyber assets.
- R5. Store information essential to recovery on backup media. Test it annually.

**The Reliability Standard for CIP**

## Research and Findings

### Small Sample Interviewed

- Two, top twenty utilities
- The Edison Electric Institute (EEI)
  - The Association of Shareholder-owned Electric Companies
- The Federal Energy Regulatory Commission (staff)

# The Reliability Standard for CIP

## Research and Findings

1. Industry wrote the CIP Standards, not the North American Electric Reliability Corporation (NERC). The NERC is a facilitating organization.
2. Big industry says they had already complied with most of the Standard (002-009).
3. Industry is complying with the letter of the Standard rather than spirit of the Standard or approaching it as a “set of standards,” as required.
4. Some facilities are using the lack of specificity as a loop hole to not comply.

# The Reliability Standard for CIP

## Research and Findings

5. When the Federal Energy Regulatory Commission adopted the CIP Standard in January of 2008 it required NERC to revisit certain issues including the lack of a risk-based methodology. Nonetheless, the schedule for compliance marches on.
6. The Federal Energy Regulatory Commission doesn't have the authority to write security regulations for the electric industry.
7. The electric utility industry is very distant from the Department of Homeland Security's goals and programs.

# The Reliability Standard for CIP

## 3 Major Findings

1. The Standard doesn't measure up to past preparedness and protection standards because it doesn't have performance standards.
  - **Three Mile Island 1979** President creates Radiological Emergency Preparedness Program for off-site preparedness
    - Requires industry to fund state and local programs to develop plans and conduct biennial exercises to “ensure public safety and health” as part of the initial and biennial renewal of power plant licenses.
  - **Bhopal India 1984 (release of methylisocyanate kills thousands)** Congress enacted Emergency Planning and Community Right-to-Know Act of 1986
    - Requires industry to report inventories of hazardous chemicals to local government who must make information available to the public. The local government must also develop hazmat emergency response plans for high risk facilities.
  - **Exxon Valdez 1989** Congress enacted Oil Pollution Act of 1990 (amended Clean Water Act)
    - Requires industry to plan for worst-case scenarios for use and storage of oil and to fund and execute full scale exercises.

# The Reliability Standard for CIP

## 3 Major Findings

- The Standard doesn't measure up to past preparedness and protection standards because it doesn't have performance standards. (Cont'd.)
- **September 11, 2001** Congress enacted the PATRIOT Act that includes the Critical Infrastructure Protection Act of 2001 and subsequently Homeland Security Presidential Directive 7 (HSPD 7)
- HSPD-7 requires the Secretary of DHS to coordinate the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States including coordinating implementation of efforts among Federal departments and agencies and the private sector.
- Further it will establish uniform policies and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors along with metrics and criteria for related programs and activities.
- **Northeast Blackout of 2003** NERC responds with industry standards that are adopted by FERC
  - Requires applicable owners/operators to comply with Reliability Standards.
  - Requires industry to conduct security vulnerability assessments and implement site security plans.

# The Reliability Standard for CIP

## 3 Major Findings

2. The Standard doesn't address current emergency management or business continuity best practices.
  - Business continuity and comprehensive emergency management standards are 20 years old.
  - A universal tenant is all-hazard.
  - The industry uses N1 and N2 Standards, but they were not designed to address multiple attacks from terrorists or natural pandemics.

# The Reliability Standard for CIP

## 3 Major Findings

3. The Standard allows a patchwork approach to protecting our nation's grid.
  - Each industry owner/operator independently identifies its critical assets and critical cyber assets as if it were a closed system. Whereas the grid operates as a system.
  - The lack of a risk-management methodology in Standard 002 and the closed system concept allows owners to claim that they have no critical assets and thus not comply with Standards 003-009.

# The Reliability Standard for CIP

## Recommendations

1. A risk-based Standard should address all-hazards.
2. A Standard similar to the CIP Standard must be complied with as an entire Standard.
  - This is best tested through a functional (peer or federal) evaluated exercise.
3. Congress should give FERC regulatory authority to promulgate nationwide rules that begin to protect the grid from criminals and allow the industry to recover part of the costs of protection.
4. FERC should continue to work with DHS to implement its role under the National Infrastructure Protection Plan to further the goals of the NIPP through the identification and protection of assets under their control.
5. Continue to track compliance with the Standard and the evolution of the CIP Standard as required by FERC.



**Questions?**

Contact us at:

[www.conopsconsulting.com](http://www.conopsconsulting.com)

[anita@conopsconsulting.com](mailto:anita@conopsconsulting.com)