



# Surviving A CIP Version 2 Audit

June 9, 2010 - Webinar

Patrick C Miller, CISA CISSP-ISSAP



# Company Information

## ■ Overview

- 41 years of experience
- Headquarters Fairfax, Virginia
- 15+ US Offices
- 3,000 + employees
- 100+ employees dedicated to Cybersecurity
- 10+ employees dedicated to NERC

## ■ Cybersecurity Markets

- Energy
- Control Systems Solution Providers
- Department of Homeland Security
- Federal Agencies
- Transportation Security Administration

# ICF Cybersecurity Capabilities

- **Key Federal and Commercial Cybersecurity Initiative Support**
  - Comprehensive National Cybersecurity Initiative (CNCI)
  - North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cybersecurity Standards
  - National Infrastructure Protection Plan (NIPP)
  - NIST Risk Management Framework
  
- **Core Competencies**
  - Security Program Management
  - NERC CIP Compliance
  - Vulnerability Assessment
  - Incident Response Management

# What's New In CIP V2?

- Removal of “reasonable business judgment”
- Removal of “acceptance of risk”
- Included “implement” where it was implied earlier
- CIP-003-2.R2 – Leadership
  - Single Senior Manager
  - Authority
  - Delegation documentation (R2.3, new)

# What's New In CIP V2?

- CIP-004-2
  - R2.1 – Training is now required prior to access instead of within 90 days of access
  - R3 – Personnel Risk Assessment is now required prior to access instead of within 30 days of access

# What's New In CIP V2?

- CIP-006-2
  - “Continuous” escorted access
  - Updates to physical security plan now required within 30 days instead of 90 days after redesign/reconfig
  - R2 is new and dedicated to physical access control and monitoring devices; was R1.8 in version 1
  - R3 is new and dedicated to electronic access control systems

# What's New In CIP V2?

- CIP-007-2
  - R9 now only allows 30 calendar days to document changes resulting from modifications to the systems or controls instead of 90
- CIP-008-2
  - R1.6 now only allows 30 calendar days to update the Incident Response Plan after changes instead of 90
- CIP-009-2
  - R3 now only allows 30 calendar days to update the Recovery Plan after changes instead of 90

# Audit Approach

- Audits and Spot Checks of all 43 requirements and all adopted versions of the CIP standards have started
- Most Regions are expected at least two weeks of effort for BA/TOP (Table 1) functions
  - Probably one week offsite, one week onsite depending on Regional approach
- Tremendous effort on both sides

# Preparing For The Audit

- Get to know the [GAGAS \(Yellow Book\)](#)
- It's all about the documentation...
  - Revision history w/ specific changes recorded
  - Classification
  - Version numbers
  - Applicable dates
  - Entire audit period
  - Approver, owner, signatures
  - Holistic, formalized, intentional

# Preparing For The Audit

- Train staff on interview techniques
  - Only answer what is asked; don't ramble
  - Never be hostile
  - Don't make stuff up; "I don't know" is a great answer
- Prepare for the work effort
  - Set day-length expectations appropriately
  - Set vacation expectations appropriately
- Practice doing data requests (w/ hashing or encryption if your Region requires)

# Show And Tell

- Tell the auditor how you meet the requirement (protocol)
  - Often policy, process, procedure, etc
- Show the auditor that you are actually meeting the requirement (proof)
  - Supporting evidence: logs, spreadsheets, documents, database extracts, captures, etc
- Attestations alone are not sufficient except for “no event” situations

# Preparing CIP Evidence

- Protocol and Proof:
  - Have your policy, procedure, process, etc
  - Have at least one, preferably two artifacts for each Requirement
- Run your own samples as practice
  - [RAT-STATS](#) – GAO tool
  - Document known universe
  - Build test set at 95% level of confidence
  - Pseudorandom sample the resulting set

# Preparing CIP Evidence

- Crosswalk each standard, requirement and sub-requirement for protocol and proof
  - “Person on the street” test
  - Highly beneficial in preparing the [RSAWs](#)
- Copy the evidence to a secure repository, or...
- Stub-reference the source within original system of record within repository/catalog
- Assemble full package from a comprehensive view – parent/child relationships, cover sheets,

# Presenting CIP Evidence

- Include very specific references to where evidence can be found in catalog
- Provide only what is necessary (protocol and two artifacts of proof, where possible)
- No “dumptrucking”
- Source documents are fine (.doc, .xls, .pdf, etc)
  - Should be searchable, no restrictions on copy/paste
- Highlighting can be useful

## During The Audit

- Show of support at kick-off, including all relevant staff and senior/executive management
- Have the Region maintain constant, transparent communication
- Track all data requests and interviews
- Strictly manage time for deliverables
- Be hospitable
- Send a group of subject matter experts if only offsite audit (Table 3 Entities)

## CIP-002

- **Impact** study; but impact to the BES not impact to asset
- Set probability to 100%
- Factor in misuse, abnormal circumstances
- Applicable to all required assets (R1.2.1 through R1.2.7)
- Redundancy (n-1) cannot be sole criteria
  - See [FAQ](#)

## CIP-002

- Good sources of supporting material:
  - TPL-004 Category D; Transmission Planning Studies
  - EOP-005, EOP-007; Emergency Ops Procedures
  - Regional Blackstart Capability Plans
  - Nuclear Plant Interface Requirements
  - Regional path catalogues
  - RC studies, base cases, Wide Area Analyses
- Reflect consideration of all owned and operated BES assets

## CIP-002

- Comprehensive lists of all cyber assets at each Critical Asset location
- Methodology for determining Critical Cyber Assets (CCAs) not required but decision process should be evident
- Redundancy of CCAs doesn't count, see [FAQ](#)
- Annual exercise; annual approval
- Even null lists need to be documented

## CIP-003

- Cyber Security Policy addresses all requirements over entire audit period
  - Can be one document or many
  - Implementation of the Policy counts
  - “Readily available” can be difficult to demonstrate
- Exceptions
  - Not an exception from standard, but from Policy
  - Explanation and mitigating measures
  - Reviewed and authorized

## CIP-003

- Information protection can be very challenging
- Change control and configuration management should be comprehensive; parallels to CIP-007.R1 and R7

## CIP-004

- Most violated CIP standard, by far
- Awareness is different than Training
- Training should be:
  - Based on roles/responsibilities
  - Entity-specific
- Be mindful of contractor/vendor training
- Documented list of specific access rights
- Access revocation is challenging

## CIP-005

- Electronic Security Perimeter (ESP) diagrams will be primary form of initial evidence
  - Additional proof will be needed such as packet captures, net streams, net flow data, configurations
- Don't forget about Access Control and Monitoring devices (ACMs) – CIP-005.R1.5
- External interactive access
  - Strong authentication = multi-factor
  - Administrative access vs. Operational access

## CIP-005

- Monitoring and logging, 24/7/365
- Vulnerability assessments and “bookends”
- Regions will be using tools such as RedSeal, Nipper and SkyBox
- Installation of software on your systems will not be required for the audit – can be done with native capabilities and data extracts

# CIP-006

- Physical Security Plan
  - Evidence all **Cyber Assets** are within ESP and PSP
  - Visitor and escort management
  - Six-wall border alternative measures; TFE
- Access Control and Monitoring devices (ACMs)
  - Two new requirements; R2 and R3 instead of R1.8
- Monitoring and logging 24/7/365
- Proof of maintenance

# CIP-007

- Security testing, not functional testing; see [FAQ](#)
- Ports and services
  - Logical port, with listening service
  - Dump of TCP/UDP status; netstat command
- Patch management
  - Availability is tricky
  - Configuration management relationship
- Anti-x

# CIP-007

- Account management
  - Minimize shared accounts
  - Accountability is paramount; who did what and when
- Passwords; interesting TFE approach
- Security status monitoring 24/7/365
  - Can use SEM/SIM to parse for human alerting
- Disposal and redeployment documentation
- Vulnerability assessments

## CIP-008

- Incident response plan that you can actually follow; balance NIST 800-61 adoption
- Response needs to be immediate
- Roles and responsibilities; contact tree
- Emergency escalation/de-escalation
- Testing the plan
- ES-ISAC reporting
  - Security Guideline: Threat and Incident Reporting

## CIP-009

- True recovery plan, not business continuity
- How is the recovery plan activated? Triggers?
- Roles and responsibilities; contact tree
- Testing the plan
- Backup media testing; test the full restore

# Post-Audit Actions

- Receive exit briefing with a good attitude, even if you have negative findings
- Disputes, if any, have a process through Enforcement options
- Always ask for a copy of the exit presentation
- Confirm destruction/handling of sensitive data
- Confirm that the Region will not post the public report until you have redacted sensitive details

# Questions?



**Patrick C Miller**

CISA, CISSP-ISSAP, SSCP, CEH, NSA-IAM

[pmiller3@icfi.com](mailto:pmiller3@icfi.com)

[www.icfi.com/cyber](http://www.icfi.com/cyber)

503.887.5497