SCIF SOFTWARE INC.

Society of Corporate Compliance and Ethics

Utilities Compliance Conference, March 2010

From Compliant to Compliance Management

Richard Dahl, CTO SCIF Software, Inc.

Agenda

- Introduction to Compliance
- Background on Evaluating Security
- Move From Evaluating to Managing Security
- Compliance Implementation Challenges
- Post-Implementation
- 'Institutionalizing' Compliance Management

Agenda

- ‘Institutionalizing’ Compliance Management
- Common Institutionalization Structures
- Proper Institutionalization Structure
- Interpreting the Standards
- Compliance Artifacts
- Compliance Assessments

Background

- Richard Dahl, Founder & CTO
  - Leading NERC CIP compliance and information security expert.
  - Expertise designing and implementing compliant, risk-based information security solutions based on NERC CIP, PCI, FFIEC & NIST standards.
  - Counterintelligence Special Agent, US Army Information Warfare Branch

Introduction to Compliance

- Compliance
  - Do stuff to things.
- Security Compliance
  - Apply Security Controls (stuff) to Assets in-Scope (things)
- Examples today are from CIP-002 - CIP-009
- Principles discussed today are Regulation Agnostic

Evaluating Security

- Compliance Assessment
  - Are prescribed controls in-place
- Vulnerability Assessment
  - Are prescribed controls working properly
- Risk Assessment
  - Are prescribed controls appropriate

Moral

- We must provide our own vision of how we achieve and maintain compliance.

CIP Implementation Challenges

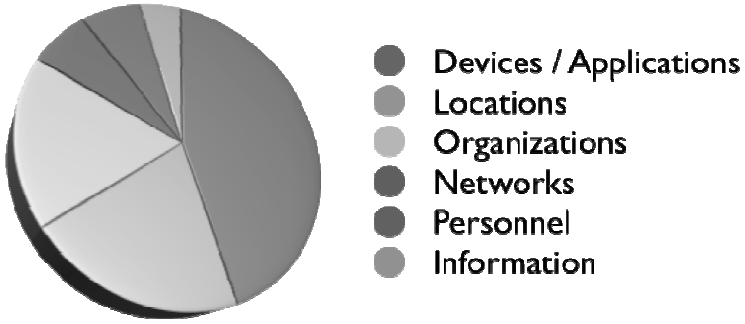
1. Confusing asset categories
2. Inconsistent requirement granularity
3. Inconsistent implementation within organization

CIP Challenge #1

- Confusing asset categories
  - CIP is “Cyber Security” Standard, but...

CIP Requirements By Asset Type

- Organizations, Locations, Networks, Personnel and Information all require compliance implementation as well. CIP is a business issue, not an IT issue!



CIP Challenge #2

- Inconsistent requirement granularity
  - Too Prescriptive (Hot)
  - Too Ambiguous (Cold)
  - Reasonable (Just Right)

Too Prescriptive

- CIP 007-1 R 5.3.2 At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible: Each password shall consist of a combination of alpha, numeric, and special characters.

Too Ambiguous

- CIP 005-1 R2.4 Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

Reasonable

- CIP 007-1 R2.1 The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

CIP Challenge #3

- Inconsistent implementation within organization
  - What does CIP-007 R6 mean to you?
    - The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
  - Does it mean the same to the person...
    - Down the hall?
    - At the alternate data center?
    - At another division?

Institutionalization

- Defined
  - Compliance is achieved and maintained simply by the execution of normal business activities
  - Personnel meet the CIP Requirements simply by doing their jobs.
- Characteristics
  - Horizontal integration of compliance activities
  - Clearly defined Responsibilities for compliance activities

Institutionalization

- Benefits
  - Reduced overhead of compliance management
    - Greater Efficiency
    - Greater Effectiveness
- Primary Requirements
  - Communicate and track compliance activities

Institutionalization Structure

- Three commonly espoused structures:
  - CIP Standards
  - Inherent Processes or Functions within CIP
  - Artifacts Required by CIP

Structural Issues

- Primary problem with these three structures is that they assume that compliance management (as opposed to compliance reporting) is disconnected from managing the security posture in place.
- NERC UAS 1200 Impact
  - Temporary cyber security measure
  - Required documentation and attestation of security posture in place

Structural Issues

- CIP Standards
  - Individual Requirements can apply to multiple asset types
    - CIP-006 R1.1
      - The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegates that shall address, at a minimum, the following: *Processes* ***to ensure*** *and document* ***that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter****.* Where a completely enclosed six-wall border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

Structural Issues

- CIP Standards - continued
  - Explicit cross reference of Requirements
    - CIP 005 R1.5
      - Cyber Assets used in the access control and monitoring of the Electronic Security Perimeters shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

- An organization cannot be compliant with CIP 005 R1.5 without being compliant with the other referenced Requirements for identified devices or applications

Structural Issues

- CIP Standards - continued
  - Implicit cross reference of Requirements
    - CIP 002-1 R 3
      - Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets ...
    - CIP 005-1 R 1.5
      - Cyber Assets used in the access control and monitoring of the Electronic Security Perimeters shall be afforded the protective measures specified ...
    - CIP 005 R 1.4
      - Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected ...

Structural Issues

- Inherent Processes or Functions within CIP
  - Organizations are not typically organized according to these functions
    - CIP-006 R1.1
      - The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegates that shall address, at a minimum, the following: *Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.* Where a completely enclosed six-wall border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

Structural Issues

- Inherent Processes or Functions within CIP
  - Audit and Accountability

Reference	Text	Asset(s)
CIP 005-1 R 3	The Responsible Entity shall implement and document an electronic or manual processes for monitoring and logging access at access points to the Electronic Security Perimeters twenty-four hours a day, seven days a week.	Devices (Network Access Points)
CIP 007-1 R 5.1.2	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	Devices Applications
CIP 007-1 R 6	The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	Devices Applications
CIP 003-1R 4	The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	Information

Institutionalization Structure

- Artifacts Required by CIP
  - 5 'P's
    - Program
    - Policy
    - Process
    - Plan
    - Procedure
  - Examples
    - "Access control program"
    - "Security plan"
    - "Operational procedures"

Institutionalization Structure

- Artifacts Required by CIP
  - Difficult to properly associate the completion of these artifacts with the responsible parties.
  - Few organizations have as formal a security program as a literal and dogmatic interpretation of the CIP Standards requires.

Institutionalization Structure

- What is the sense in creating one “Access Control Program” simply because CIP 003-1 R 5 requires “...a program for managing access to protected Critical Cyber Asset information” ? There is no requirement within CIP that mandates a particular structure for documentation.
- We must remember the rules of English grammar, a ‘program’ is not the same thing as a ‘Program.' Here, ‘program,' just like all references to ‘plans’, ‘processes’, ‘logs’, ‘documentation,' ‘policies’, ‘procedures’, etc ... are common nouns, and should therefore not be taken to imply a formality that is not required.

Institutionalization Structure

- Taking the artifact based approach to the extreme can hinder an appropriate security posture.
  - CIP 003-1 R 6
    - The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

Institutionalization Structure

- One unified process would have to incorporate changes to
  - Applications
  - Devices
  - Network access points
- The document could easily end up a convoluted mess that no one throughout their normal duties would require.
- System administrators, network administrators, and application administrators only would need to understand information relevant to the assets under their control.

Proper Structure

- Analysis of the CIP Standards Provide:
  - Compliance actions must be performed on or behalf of:
    - Applications
    - Devices
    - Networks
    - Organizations
    - Personnel
    - Information
    - Facilities

Asset Type Correlation

- CIP 005 R 1- Electronic Security Perimeter: The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeters and all access points to the perimeters.
  - Applies to:
    - Devices and Applications
      - Must reside within ESP
    - Organizations or Networks
      - Must document ESPs
    - Networks or Organizations
      - Must identify all access points
  - Applicability determined by responsibilities!

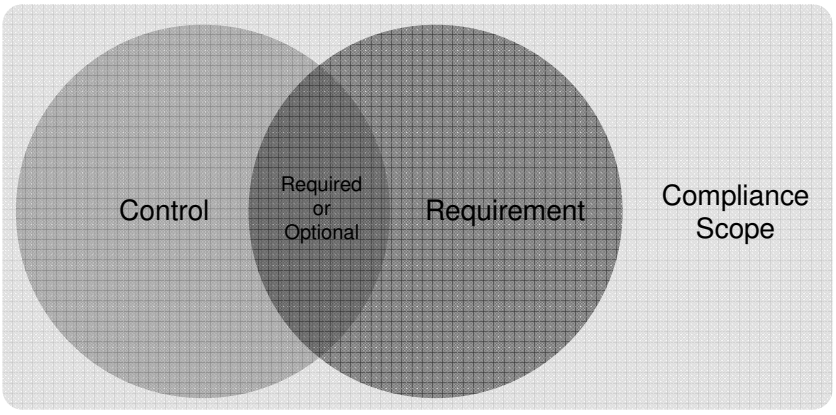
Asset Based Structure Limitation

- CIP 007 R 5.3 Account Management At a minimum, the Responsible Entity shall require and use passwords
  - Applies to:
    - Devices and Applications
      - Must reside within ESP
  - May be implemented differently according to risk
    - Telemetry server = passwords
    - Firewall at ESP Border = Tokens

Compliance Scope

- Definition
  - Distinct category of asset type(s) that meet conditions set within the CIP Standards mandating application of Requirement(s)
  - e.g. Critical Asset - Facilities that are essential to the reliable operation of the Bulk Electric System CIP-002 R 1
- Conditions
  - CIP-002 R 2
    - Provides the Criteria for inclusion.
- Requirements that apply
  - CIP-002 R 2 Critical Asset Identification
  - CIP-002 R 3 Critical Cyber Asset Identification
  - CIP-002 R 4 Annual Approval

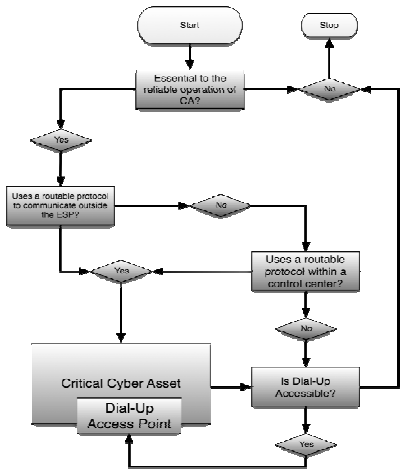
Compliance Scope Visualized



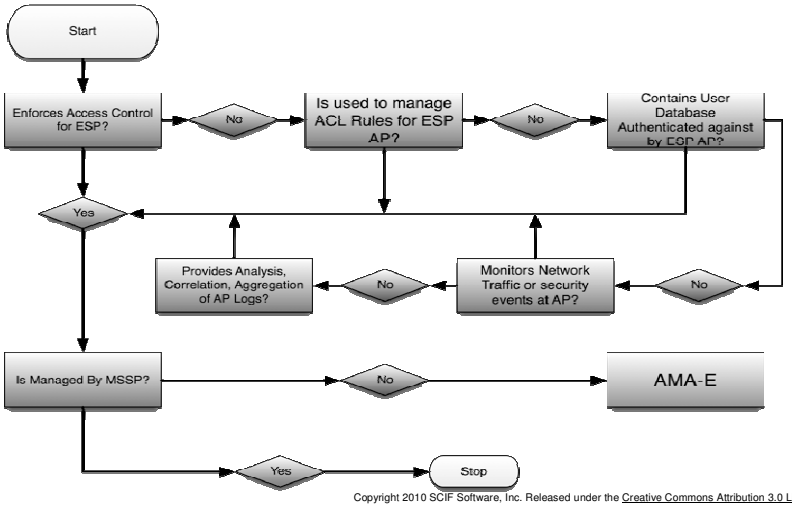
CIP Compliance Scopes

Compliance Scope	CIP Reference	Asset Applicability						
		Organization	Location	Personnel	Information	Device	Application	Network
Responsible Entity	*Throughout*	X						
Critical Asset	*CIP-002 R 2*		X					
Physical Security Perimeter	*CIP-006 R 1*		X					
Critical Cyber Asset	*CIP-002 R 3*					X	X	
Non-Critical ESP Cyber Asset	*CIP-005 R 1.4 CIP-007*					X	X	
Access Control or Monitoring Asset for the ESP	*CIP-005 R 1.5*					X	X	
Access Control or Monitoring Asset for the PSP	*CIP-006 R 1.8*					X	X	
Dial-up ESP Access Point	*CIP-005 R 1.1 CIP-005 R 1.2*					X	X	
Routable ESP Access Point	*CIP-005 R 1.1 CIP-005 R 1.3*					X	X	
Routable Electronic Security Perimeter	*CIP-005 R 1*							X
Non CCA Protected Network	*CIP-006 R 1.8 CIP-005 R 1.5*							X
NERC CIP Personnel	*CIP-004*			X				
Sensitive CCA Information	*CIP-003 R 4*				X			

Scope Assessment Logic



AMA-E Decision Tree



Standard Map For CCA

Reference	Text
CIP 002 R 3	Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facility at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary.
CIP 002 R 4	A senior manager or delegates shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets.
CIP 005 R 1	The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeters and all access points to the perimeters.
CIP 006 R 1.1	The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegates that shall address, at a minimum, the following: Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed six-wall border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
CIP 007 R 1	The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, application, database platforms, or other third-party software or firmware.
CIP 007 R 1.2	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.
CIP 007 R 2.1	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
CIP 007 R 2.2	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeters.
CIP 007 R 2.3	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measures applied to mitigate risk exposure or an acceptance of risk.
CIP 007 R 3.1	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

CIP Interpretation

- Project team members rely largely on their own individual understanding of the CIP Requirements and information security to determine the gaps and appropriate resolution mechanisms.
  - They may not be accountable for compliance
- Organization's find themselves lacking confidence that they are indeed compliant.
  - Little centralized documentation that can provide any kind of traceability of what fulfills the CIP Requirements
  - Trusting the assertions of their project team.
    - "Thus sayeth the consultant"
- Understanding what controls have been determined to meet the requirements is essential to ensuring ongoing compliance.

Control Framework

- Control Purpose
  - Provide consistent and granular interpretation of security requirements
- Control Sources
  - NIST SP 800-53
  - BITS
  - ISO 2700X
- Control Mapping
  - Controls to CIP Requirements By Compliance Scope

CIP-007-1 R6

CIP 007 R 6	The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	
AU 2	Audit records are generated for defined events.	Req
AU 2.1	Auditable events include all attempts to login.	Req
AU 2.2	Auditable events include successful user logins.	Req
AU 2.3	Auditable events include user logoffs.	Req
AU 2.4	Auditable events include attempts to switch users.	Req
AU 2.5	Auditable events include attempts to access sensitive applications or resources.	Req
AU 2.6	Auditable events include attempts to access sensitive data.	Req
AU 2.7	Auditable events include attempts to modify sensitive data.	Req
AU 2.10	The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html that provide recommended lists of auditable events are followed.	Opt
AU 4	There is sufficient audit record storage capacity available.	Req
AU 5	The selection of events to be audited is managed by individual components of the system.	Opt
AU 6	Sufficient information is captured in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.	Req
AU 6.1	Audit record content includes the date and time of the event.	Req
AU 6.2	Audit record content includes the component of the information system (e.g., software component, hardware component) where the event occurred.	Req
AU 6.3	Audit record content includes the type of event.	Req
AU 6.4	Audit record content includes subject identity.	Req

CIP-007-1 R6

CIP 007 R 6	The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	
AU 6.5	Audit record content includes the outcome (success or failure) of the event.	Req
AU 6.6	The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.	Opt
AU 6.7	The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.	Opt
AU 7	In the event of an audit failure or audit storage capacity being reached, the information system takes pre-determined action.	Req
AU 7.1	In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials.	Req
AU 7.1.1	The information system provides a warning when allocated audit record storage volume reaches a pre-determined percentage of the maximum audit record storage capacity.	Req
AU 7.1.1.2	The information system provides a warning when allocated audit record storage volume reaches 90 percent of the maximum audit record storage capacity	Req
AU 7.2.3	In the event of an audit failure or audit storage capacity being reached, the information system archives audit records to a remote system.	Req
AU 10	The information system provides time stamps for use in audit record generation.	Req
AU 10.2	Time stamps of audit records are generated using internal system clocks that are synchronized system wide.	Req
AU 11	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Req
AU 11.1	The information system produces audit information on hardware-enforced, write-once media.	Opt

CIP-007-1 R2.1-2.3

CIP 007 R 2.1	**The Responsible Entity shall enable only those ports and services required for normal and emergency operations.**	
CM 7	*The information system is configured to provide only essential capabilities and functions.*	*Req*
CM 7.1	*Essential capabilities and functions are documented for each information system.*	*Req*
CM 7.1.1	*Documentation of essential capabilities and functions include the business process facilitated.*	*Req*
CM 7.1.2	*Documentation of essential capabilities and functions include all appropriate configuration information.*	*Req*
CM 7.1.3	*Documentation of essential capabilities and functions include all network ports enabled.*	*Req*
CM 7.1.4	*Documentation of essential capabilities and functions includes the executable program listening on any enabled ports.*	*Req*
CIP 007 R 2.2	**The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeters.**	
CM 7.2	*Functions and services, provided by default, that are not necessary to support essential organizational operations are disabled.*	*Req*
CIP 007 R 2.3	**In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measures applied to mitigate risk exposure or an acceptance of risk.**	
CM 7.2	*Functions and services, provided by default, that are not necessary to support essential organizational operations are disabled.*	*Req*

CIP Complexity

- Organizations must be very careful to granularly define the interpretation of this Requirement
  - Granular interpretation reduces any confusion

Password composition rules are enforced through user training.
Password composition rules are technically enforced.

    - These are not mutually exclusive
      - Personnel training requirements should include guidance on password composition even if it is technically possible to enforce the specific character types required.
      - If the three specific character types cannot be technically enforced, an organization could reach the conclusion that enforcement through user awareness training, combined with controls that ensure there are three distinct character types (by counting upper case and lower case alpha distinctly) is appropriate to meet the requirement.

Interpretation

- The interpretation of the Requirements is what always happens... it is just not usually documented.
  - Everyone who looks at the CIP Requirements interprets their meaning based on their own understanding of security and their level of technical competence.
  - The real issue is whether the individual interpretations are consistent with one another throughout the enterprise.

Compliance Artifacts

- Auditable Evidence of Compliance
- Types of Artifacts
  - Documentation
    - Policies or policy statements
    - Lists
  - System Configuration Settings
    - Logging
    - Authentication Mechanisms
  - Third-Party Applications
    - Correlation Engine Reports
  - Exceptions

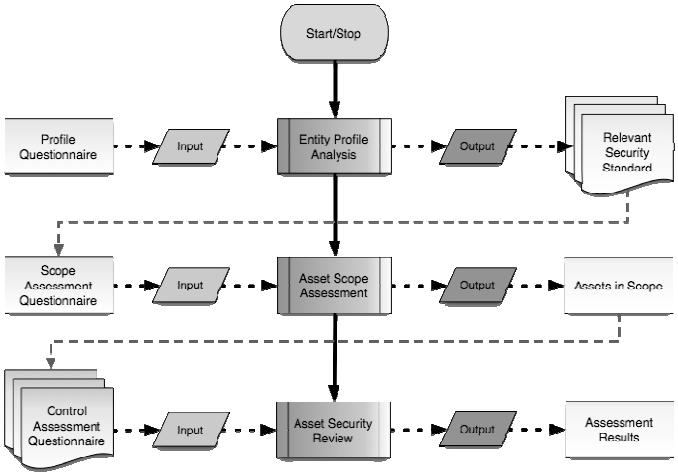
Compliance Questionnaires

- One Questionnaire for each Compliance Scope
  - Contains controls deemed relevant for each asset-type/compliance scope combination
  - Granularly focuses questions for a specific asset or group of assets within scope
- Increases efficiency and effectiveness of audit program

Questionnaire Format

Control Family	Reference	Question Text	Yes/No/NA/TI
Authentication Management	2	The information system uniquely identifies and authenticates users (or processes acting on behalf of users).	
Authentication Management	2.1	Authentication of user identities is accomplished through approved mechanisms.	
Authentication Management	2.1.1	Authentication of user identities is accomplished through the use of usernames and passwords.	
Authentication Management	2.1.2	Authentication of user identities is accomplished through the use of usernames and biometric devices.	
Authentication Management	2.1.3	Authentication of user identities is accomplished through the use of usernames and tokens.	
Authentication Management	2.1.4	Authentication of user identities is accomplished through the use of digital certificates.	
Authentication Management	2.1.5	Authentication of user identities is accomplished through the use of multi-factor authentication.	
Authentication Management	2.2	FIPS 201 and Special Publications 800-73 and 800-76 guidance regarding personal identity verification (PIV) card token for use in the unique identification and authentication of federal employees and contractors is followed.	
Authentication Management	2.3	NIST Special Publication 800-63 guidance on remote electronic authentication is followed.	
Authentication Management	2.4	User identification and authentication within a specified security perimeter follows NIST SP 800-63 guidance.	
Authentication Management	3	The information system identifies and authenticates specific devices before establishing a connection.	
Authentication Management	3.1	The information system uses pre-defined mechanisms to identify and authenticate devices on local and/or wide area networks.	
Authentication Management	3.1.1	The information system uses shared known information (e.g., Media Access Control (MAC) or Transmission Control Program/Internet Protocol (TCP/IP) addresses) to identify and authenticate devices on local and/or wide area networks.	
Authentication Management	3.1.2	The information system uses an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks.	
Authentication Management	4	The organization manages user identifiers.	
Authentication Management	4.1	The organization manages user identifiers by uniquely identifying each user.	
Authentication Management	4.2	The organization manages user identifiers by verifying the identity of each user.	
Authentication Management	4.3	The organization manages user identifiers by receiving authorization to issue a user identifier from an appropriate organization official.	
Authentication Management	4.5	The organization manages user identifiers by disabling user identifier after a pre-defined time period of inactivity.	
Authentication Management	4.5.1	The organization manages user identifiers by disabling user identifier after 6 months of inactivity.	
Authentication Management	4.5.2	The organization manages user identifiers by disabling user identifier after 3 months of inactivity.	
Authentication Management	4.6	The organization manages user identifiers by archiving user identifiers.	

Compliance Review Process



Governance Actions

- Document ongoing activities required by standard, e.g.
  - Review logs
  - Review users
  - Update and approve policies
  - Review compliance Artifacts
- Correlate those activities to assets in-scope
- Create checklists to ensure activities are completed

Summary

- The difficulties inherent in the CIP Standards:
  - Inconsistent granularity of requirements
  - Inconsistent implementation within an organization
  - Confusing asset categories
- Are best mitigated through a documented interpretation of the Requirements based on the assets within scope
  - This provides a high level of effective communication and supports an efficient compliance management program

Thank You

- Questions ?
- Comments .
- Concerns !