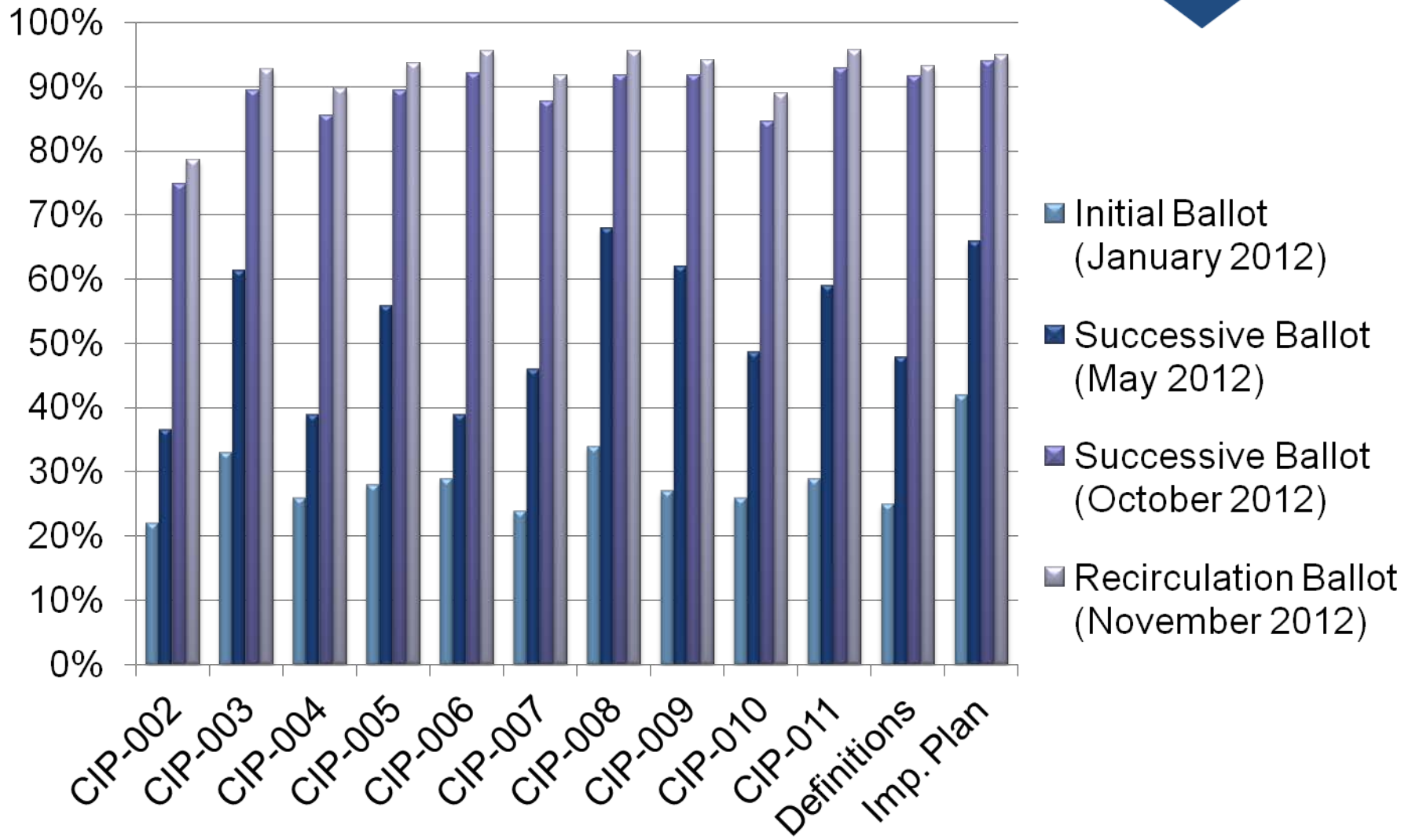
NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security Standards Update

Version 5

RELIABILITY | ACCOUNTABILITY

Version 5 Ballot Results



Ongoing Steps

- Filed with FERC February 1, 2013 (after 5:00 PM on 1/31)
  - FERC Docket RM13-5
  - 10,483 page filing (yes, ten thousand pages)
  - Available on NERC Website at:
    - http://www.nerc.com/files/Final_Petition_CIP_V5_01-31-13%20and%20Exhibits%20A-E.pdf
    - http://www.nerc.com/fileUploads/File/Filings/Exhibit%20F%20(Part%201%20of%202).pdf
    - http://www.nerc.com/fileUploads/File/Filings/Exhibit%20F%20(Part%202%20of%202).pdf
    - http://www.nerc.com/fileUploads/File/Filings/Exhibits%20G-H.pdf
  - FERC version at http://elibrary.ferc.gov/idmws/common/OpenNat.asp?fileID=13167892 (76MB file)
- FERC will need to go through its process
- Filings to Canadian Regulators made on February 7, 2013

CIP Standards – Version 5

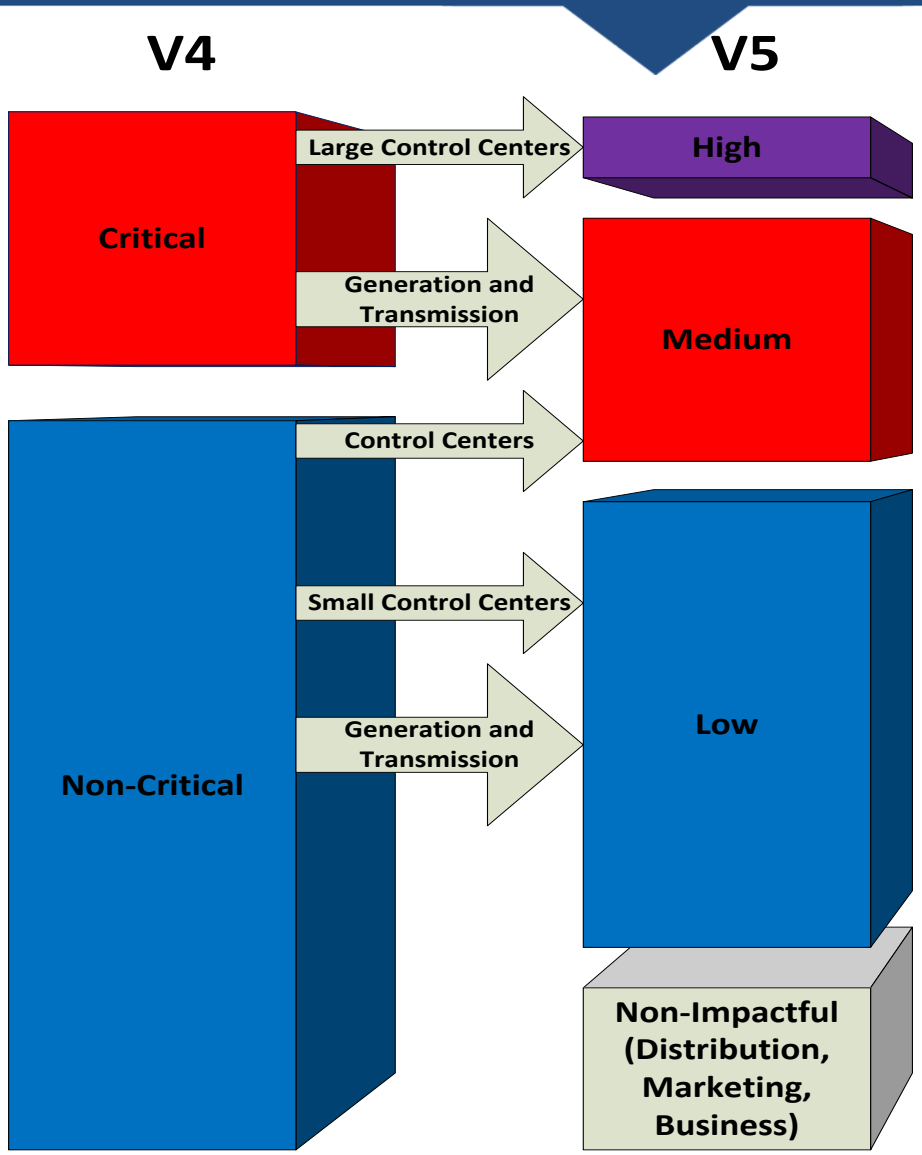
- New / Modified Terms:
  - BES Cyber Asset
  - BES Cyber System
  - BES Cyber System Information
  - CIP Exceptional Circumstance
  - CIP Senior Manager
  - Control Center
  - Cyber Assets
  - Cyber Security Incident
  - Dial-up Connectivity
  - Electronic Access Control and Monitoring Systems (EACMS)
  - Electronic Access Point (EAP)
  - Electronic Security Perimeter (ESP)
  - External Routable Connectivity
  - Interactive Remote Access
  - Intermediate Device
  - Physical Access Control Systems (PACS)
  - Physical Security Perimeter (PSP)
  - Protected Cyber Asset (PCA)
  - Reportable Cyber Security Incident

CIP Standards – Version 5

- CIP-002
  - Eliminates the "Critical Asset" step of the identification process
  - Builds on "bright lines" from CIP-002-4
  - "Version 4" Critical Asset control centers – High
  - Other "Version 4" Critical Assets – Medium
  - Larger "Version 4" non-critical asset control centers – Medium
  - Transmission now looking at a "capacity calculation" rather than number of lines at a voltage level
  - Catch-all category for non-specifically categorized – Low
    - "Something everywhere" – within the BES
    - Programmatic requirement: CIP-003-5 Requirement R2

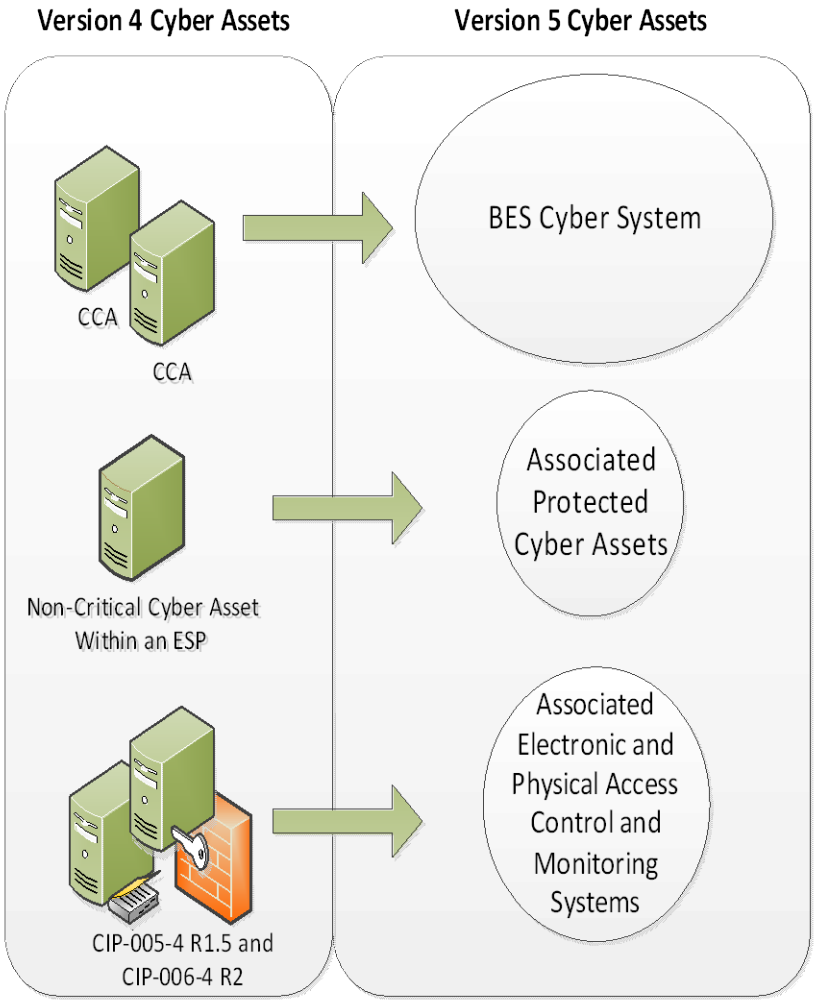
CIP Standards – Version 5

- High Impact
  - Large Control Centers
  - CIP-003 to 009 V4 "plus"
- Medium Impact
  - Generation and Transmission
  - Control Centers
  - Similar to CIP-003 to 009 V4
- All other BES Cyber Systems (Low Impact) must implement a policy to address:
  - Cybersecurity Awareness
  - Physical Security Controls
  - Electronic Access Controls
  - Incident Response



CIP Standards – Version 5

- Non-CCA assets in Version 4 are also covered
  - "Non-Critical Cyber Assets within an ESP" are now named Protected Cyber Assets, are associated with a BES Cyber System, and called out in the Applicable Systems column
  - EACMS and PACS are associated with a BES Cyber System, and are called out in the Applicable Systems column



CIP Standards – Version 5

Rationale, Guidance & Changes,

Rationale for R3: To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

Main Requirement and Measure

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

Applicable Systems for requirement part

Requirement part text

Requirement part Measure text

CIP-004-5 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
Reference to prior version: *CIP004-4, R3.1*		**Change Rationale:** *Addressed interpretation request in guidance. Specified that identity confirmation is only required for each individual's initial assessment. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.*	

Requirement part Reference

Requirement part change rationale

CIP V5 Approach to Correcting Deficiencies

- Empowers industry
  - Shifts focus from *whether* deficiencies occur to *correcting* deficiencies
  - Continuous Improvement
    - ***From:*** backward-looking, individual violations
    - ***To:*** forward-looking, holistic focus
- Reliability and security emphasis that promotes the identification and correction of deficiencies
- Consistent with NERC "Internal Controls" approach to compliance
- Version 5 triggering language: "… implement, in a manner that identifies, assesses, and corrects deficiencies, …"

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Questions

Scott Mix, CISSP
scott.mix@nerc.net
215-853-8204

RELIABILITY | ACCOUNTABILITY

Critical Infrastructure Protection & Cybersecurity

An Industry Perspective – Josh Sandler, Duke Energy 4/24/13

DUKE ENERGY®

Input - List of Critical Assets

Based on input - Cyber Assets supporting Critical Assets

Filtering - Essential to operation of Critical Asset and meets CIP 002 R3

Output - List of Critical Cyber Assets

Examples from CIP002 Version 3 R3:

For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

NERC CIP Version 4

- Replaces CIP-002-3 Risk-Based Assessment Methodology with “Bright-Line” Criteria
  - Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.
  - Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon required for reliability purposes.
  - Each Blackstart Resource identified in the Transmission Operator's restoration plan.

- ~~Effective 4/1/14~~ – SUPERSEDED by NERC CIP Version 5!

NERC CIP Version 5

- FERC Issued NOPR 4/18/13
  - V4 is no longer effective 4/1/14
  - Industry will be subject to NERC CIP V3 until V5 becomes effective
    - 7/1/15 – High/Med Impact BES Cyber Systems
    - 7/1/16 – Low Impact BES Cyber Systems

- 24 Month Implementation Window may be shortened
- All BES Facilities are in scope

- Starts with Cyber Asset inventory/assessment
- Budgetary Impacts at each facility vary greatly but can be large
  - $250k - $5MM+
- Need a balance of security, reliability, and compliance

Questions

Josh Sandler - Duke Energy
704-382-4504
josh.sandler@duke-energy.com

DUKE ENERGY®

SOUTHERN COMPANY

Critical Infrastructure/Cyber Security

April 24, 2012

Scott Fallon

SOUTHERN COMPANY

One GREAT Team — Southern Company Generation

NERC CIP 4 STANDARDS

Eight Standards / 41 Requirements

CIP-002 — CRITICAL CYBER ASSETS

- CRITICAL ASSETS
- CRITICAL CYBER ASSETS
- ANNUAL REVIEW
- ANNUAL APPROVAL

CIP-003 — SECURITY MANAGEMENT CONTROLS

- CYBER SECURITY POLICY
- LEADERSHIP
- EXCEPTIONS
- INFORMATION PROTECTION
- ACCESS CONTROL
- CHANGE CONTROL

CIP-004 — PERSONNEL AND TRAINING

- AWARENESS
- TRAINING
- PERSONNEL RISK ASSESSMENT
- ACCESS

CIP-005 — ELECTRONIC SECURITY

- ELECTRONIC SECURITY PERIMETER
- ELECTRONIC ACCESS CONTROLS
- MONITORING ELECTRONIC ACCESS
- CYBER VULNER-ABILITY ASSESSMENT
- DOCUMEN-TATION

CIP-006 — PHYSICAL SECURITY

- PLAN
- PHYSICAL ACCESS CONTROLS
- MONITORING PHYSICAL ACCESS
- LOGGING PHYSICAL ACCESS
- ACCESS LOG RETENTION
- MAINTE-NANCE & TESTING

CIP-007 — SYSTEMS SECURITY MANAGEMENT

- TEST PROCEDURES
- PORTS & SERVICES
- SECURITY PATCH MANAGEMENT
- MALICIOUS SOFTWARE PREVENTION
- ACCOUNT MANAGEMENT
- SECURITY STATUS MONITORING
- DISPOSAL OR REDEPLOY-MENT
- CYBER VULNERABILITY ASSESSMENT
- DOCUMEN-TATION

CIP-008 — INCIDENT REPORTING & RESPONSE PLANNING

- CYBER SECURITY INCIDENT RESPONSE PLAN
- DOCUMEN-TATION

CIP-009 — RECOVERY PLANS FOR CCA

- RECOVERY PLANS
- EXERCISES
- CHANGE CONTROL
- BACKUP & RESTORE
- TESTING BACKUP MEDIA

NERC Cyber Security Standard

- CIP 002-009 Version 3—Current version
  - No generation critical assets
- CIP 002-009 Version 4
  - Compliance April 1, 2014
  - “Brightline” criteria
    - Sites greater than 1500 MW
    - Blackstart facilities
- CIP 002 Version 5
  - Adoption April 1, 2014
  - Low, Medium, High

NERC CIP v.4 Plants

	APC	GPC	Gulf	MPC	SPC
>1500MW					
Blackstart					
Associated					

NERC CIP v.5 Plants

	APC	GPC	Gulf	MPC	SPC
High					
Medium					
Low					

SOUTHERN COMPANY

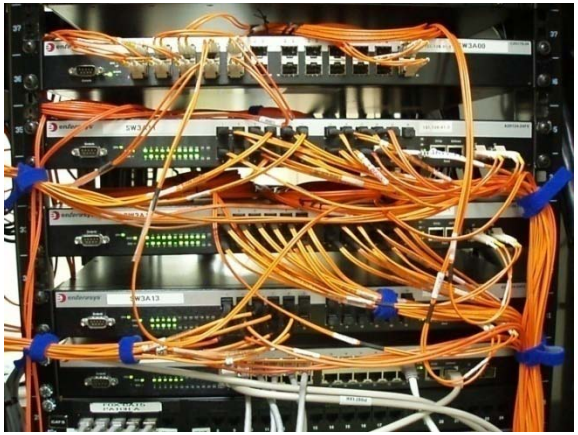
One GREAT Team Southern Company Generation

For Each Critical Cyber Asset we must…..

- Establish a 6 wall physical security perimeter around the device that is monitored and access logged 24X7 (PSP)
- Establish an electronic security perimeter around the device that is monitored and access logged 24X7 (ESP)
- Test all software patches for the device within 30 days of release by the vendor and develop a strategy to deploy the patch to affected devices
- Conduct annual vulnerability assessments of the device
- Have and test an incident response and recovery plan for each device type
- Ensure that anyone that comes in contact with the device has a current background check (repeated every 7 years) and has annual CIP training
- Have an up-to-date list of everyone that has access to the device
- Revoke access to the device within 7 days if the individual is terminated or transferred, revoke access to the device within 24 hours if termination is for cause (this includes any contractors or vendors with access)
- Maintain up-to-date diagrams of each device, the open and disabled ports, and services allowed to run on the device

Plant Cyber Asset Identification

- Routable Protocol devices
- Top to bottom walkdown
- Physical hardware collection
- Script hardware collection
- Initial ESP/PSP development
- Equipment classification
- Initial configuration



Physical Security Walkdown

- Clustered devices within definable boundaries
- Physical security hardware
  - Card readers, i-Stars, locks, doors, penetration closure
  - Cameras
- Budgetary Estimates

SOUTHERN COMPANY

One GREAT Team

Southern Company Generation

Plant Activities

- Perform annual inventory of Cyber Assets (CA)
- Complete administrative requirements
- Perform list management (CA's, people, logs)
- Perform site vulnerability assessments
- Demonstrate patch management implementation
- Implement and maintain information management process(Document control)
- Demonstrate adequate change management
- Support required training
- Procure capital equipment
- Implement physical controls (badge readers, cameras, etc.)
- Implement systems processes
- Install patches and anti-virus
- Perform system data/configuration backups
- Implement system hardening requirements
- Ensure all CCA's are monitored
- Report incidents
- Participate in tabletop exercises
- Understand disaster recovery plans and implement if required
- Manage access control
- Initiate background and training requests
- Grant logical and physical access
- Revoke logical and physical access in a timely manner

Generation Corporate Activities

- Compliance (Operations)
  - Develop policies
  - Manage background investigation process
  - Develop and manage training programs and requirements
  - Perform compliance assurance activities, example: log reviews
  - Lead audit preparations and documentation
  - Lead annual senior manager and documentation reviews
  - Coordinate tabletop exercises
  - Coordinate Technical Feasibility Exception process
  - Facilitate annual program vulnerability assessment
- Other Groups
  - Security
    - Perform physical security vulnerability assessment
    - Establish Physical Security Perimeter (PSP)
  - Southern Company Compliance
    - Support background investigation process

Generation Corporate Activities

- Generation Technical Services
  - Inventory Critical Assets (CA) and identify Critical Cyber Assets (CCA)
  - Develop and oversee change management process
  - Determine Electronic Security Perimeter (ESP)
  - Identify Physical Security Perimeter (PSP)
  - Develop and manage patch management and process(150+ patches per year per control system), anti-virus updates, ports and services process, testing, account management policies
  - Participate in disaster recovery tabletop exercises per site
  - Develop incident response process and respond to incidents
  - Develop technical procedures
  - Manage Technical Feasibility Exception process
  - Implement and manage above processes for hydro plants
  - Perform technical vulnerability assessments

Southern Hydro Generation Cyber Security Plans

- Policies and Procedures for Compliance CIP-002-009 Version ???
- System Black Start Units
- Control Centers
  - Large
  - Smaller/regional
- Policies and Procedures for Good Business Practices to manage all cyber assets

SOUTHERN COMPANY

One GREAT Team

Southern Company Generation

Questions?