# Auditing NERC CIP Version 5 Compliance
# August 23rd, 2016

AGA American Gas Association

EEI Edison Electric Institute

Power by Association℠

# Agenda

- Overview of NERC & The CIP Standards
  - Key Dates
  - High Level CIP overview
- Risk Based Compliance Monitoring & Enforcement
  - Developing and auditing a robust program
- Auditing The CIP Standards
  - Specific areas of focus for CIP-002 through CIP-011
- Prepping For An Audit By Regulators

# Background

- Sean is the Manager for the Risk Management – Compliance area for Dominion.
- Sean has been in that role for over 4 years and oversaw the NERC CIP v3 audit (with 0 findings) and the development of our version 5 program.
- Dominion is in SERC, RF, NPCC and WECC.
- Dominion has Transmission (6,500 miles) and Generation (24,300 MW)
- We are integrated into PJM as the Balancing Authority and the TOP (Transmission Operator).
- In addition to NERC compliance, we also have TSA Pipeline with 12,200 miles of Natural Gas transmission, gathering and storage.
- We are also subject to PCI, SOx, NRC, CFATS, DODI, CoC, HIPAA.

# Key NERC Version 5 Dates

- Although often referred to as “version 5”, the current NERC standards are a combination of v5, v6, v1 and v2 iterations on the individual requirements.
- There are certain dates commonly talked about but there are some exceptions to those dates that are noted in the Implementation Plan.
- The Implementation Plan also explains things such as when to be compliant with unplanned changes after the effective dates.
- Effective July 1st 2016, all High and Medium Impact BES Cyber Systems had to be compliant with version 5 of the standards.
- Effective July 1st 2017, all Low Impact BES Cyber Systems have to be compliant with a subset of the version 5 standards.

# NERC Website

- To obtain a complete list of the dates and copies of other official documents we will talk about:
  1. Go to www.NERC.com
  2. Click on Program Areas & Development -> Standards
  3. On the left side is a link to “One-Stop-Shop”
- From there you can scroll to the CIP section and obtain:
  - Copies of the current standard language
  - The implementation plan
  - The current version of the RSAW (Reliability Standard Audit Worksheet)
  - Any Compliance Guidance or Lessons Learned that are available
  - Enforcement Dates and Retirement Dates

# Guilty Until Proven Innocent

- Unlike auditing for SOx or other regulatory requirements, the NERC standards require utilities to prove compliance.
- A lack of proof of compliance means an entity is non-compliant.
- The adage of "If its not written down, it doesn't exist" should be applied to the program.
  - SME testimony is not generally sufficient to prove compliance moving forward.
  - Attestations can only be used to confirm you don't do something because its not applicable. Don't use them to assert you did do something.
- Proof of compliance needs to be maintained at least back to your last audit by your regulator.
  - Check with your region(s) to ensure you adhere to their guidance.
- As an auditor, one way you can help your compliance programs is by reviewing their collection and retention of compliance evidence.

# The CIP Standards

- There are 10 Standards, 33 Requirements and a combined 120 Requirements + Sub-Requirements to be compliant with.
  - CIP-014 is not included in this discussion. Many entities handle it separately from the 'core' CIP standards.
  - A new "Supply Chain" focused standard will be coming that will add another section to this list and may also be handled separate from the core CIP standards by your entity.
- The standards are evolving.
  - Over the coming months official audit results will begin to occur which will be provide insight on how the standards are enforced.
  - Lessons Learned/Official Guidance will continue to be published and that will evolve the understanding and enforcement.
  - The Standards Drafting Team is currently engaged in a number of modifications to the standards that we will learn more about later this year or early 2017. This will include a new Supply Chain standard.

# The CIP Standards

| CIP-002 | CIP-003 | CIP-004 | CIP-005 | CIP-006 | CIP-007 | CIP-008 | CIP-009 | CIP-010 | CIP-011 |
|---|---|---|---|---|---|---|---|---|---|
| **BES Cyber System Categorization** | **Security Management Controls** | **Personnel & Training** | **Electronic Security Perimeter(s)** | **Physical Security of BES Cyber Systems** | **System Security Management** | **Incident Reporting & Response Planning** | **Recovery Plans for BES Cyber Systems** | **Configuration Change Management & Vulnerability Assessments** | **Information Protection** |
| 1. Process to Identify and Categorize BES Cyber Systems<br>2. Review and Approval of Identified BES Cyber Systems and Categoriza-tions | 1. BES Cyber System Cyber Security Policy<br>2. Low Impact BES Cyber System Cyber Security Plan ATCH<br>3. CIP Senior Manager<br>4. Delegation of CIP Authority | 1. Security Awareness Program<br>2. Cyber Security Training Program<br>3. Personnel Risk Assessment Program<br>4. Access Management Program<br>5. Access Revocation | 1. Electronic Security Perimeter TFE<br>2. Interactive Remote Access Management TFE | 1. Physical Security Plan TFE<br>2. Visitor Control Program<br>3. Physical Access Control System Maintenance and Testing Program | 1. Ports and Services , TFE<br>2. Security Patch Management<br>3. Malicious Code Prevention<br>4. Security Event Monitoring , MAX, SysCAP, TFE<br>5. System Access Control , TFE, MAX | 1. Cyber Security Incident Response Plan Specifications<br>2. Cyber Security Incident Response Plan Implemen-tation and Testing<br>3. Cyber Security Incident Response Plan Review, Update, and Communica-tion | 1. Recovery Plan Specs SysCAP<br>2. Recovery Plan Implemen-tation and Testing<br>3. Recovery Plan Review, Update and Communica-tion | 1. Configuration Change Management , TFE<br>2. Configuration Monitoring<br>3. Vulnerability Assessments TFE<br>4. Transient Cyber Assets and Removeable Media ATCH | 1. Information Protection<br>2. BES Cyber Asset Reuse and Disposal |

**ATCH** – The requirement has associated attachments that must be addressed for compliance.

**MAX** – A 'part' of the requirement contains "Maximum supported by the Cyber Asset" language .
- CIP-007-5, Part 5.5

**SysCAP** – A 'part' of the requirement contains " Per Cyber System / Asset Capability" language.
- CIP-007-5 Part 4.1, 4.2, 5.4
- CIP-009-5 Part 1.5

**TFE** – A 'part' of the requirement contains "Technical Feasibility Exception" language .
- CIP-005-5 Part 1.4, R2
- CIP-006-5 Part 1.3
- CIP-007-5 Part 1.1, 4.3, 5.1, 5.6, 5.7
- CIP-010-1 Part 1.5, 3.2

# Risk Based Compliance Monitoring & Enforcement

- Originally termed “RAI” (Reliability Assurance Initiative) there is an optional component to the CIP standards in version 5 now known as the RBCMEP.
- The idea is that entities will assess their programs based on risk -> build controls for those areas of higher risk -> monitor those controls for compliance -> periodically test those controls to ensure they are working.
- The better an entity performs the RBCMEP role, the more confidence your regulator can have in your program.
- The more confidence they have, the less deeply they need to dig during an audit.
- During the version 5 transition pilot, it was reported that good controls programs could result in a 40% reduction in audit scope.

# RBCMEP Continued…

- One area that internal auditing can add value to a NERC CIP program is to participate in the RBCMEP effort.
- Since auditors are typically in a different organization, with a different goal structure, than the personnel primarily responsible for NERC CIP, their results can be value added when attempting to demonstrate robust controls are in place.
- As auditors you are already familiar with what makes for a good control and with methods to test a control for effectiveness.
- The idea behind a RBCMEP program is to both prevent impact to the Bulk Electric System by detecting incidents before they happen, and to build confidence in your regulator that you are effectively doing that.

# RBCMEP Continued…

- Areas to focus on when evaluating the RBCMEP program include:
  - What is the Risk Based Methodology your entity used to risk rank the NERC CIP requirements? Is that methodology well defined? Can the criteria be defended from an 'auditor' perspective?
  - For the areas of highest risk, were "good" controls identified? Good controls:
    - Don't just restate the Requirement
    - Are a blend of Preventative, Detective and Corrective
    - Are repeatable
    - Are effective
    - Are verifiable
  - Are there both Entity level controls (ex: an enterprise system to manage access?) and Activity level controls (ex: how group X ensures that all cyber security tests are accurately and completely performed before a change goes into production)?

# RBCMEP Continued…

- Areas to focus on when evaluating the RBCMEP program also include:
  - Is there audit quality evidence that shows the control was performed? If its not written down, it did not happen.
  - How do you know the controls are effective?
    - Are they periodically tested to ensure they are working?
    - Are they based on an industry standard?
    - Are they automated so there is little change for human error?
    - Can the regulators reasonably conclude that the controls are working effectively.
- While the RBCMEP is both optional and nebulous, it is an area the regulators are very interested in. An investment in this area can reap rewards both in terms of reducing Self Reports and reducing your audit scope.
- As auditors, you have a value added perspective to the development of your entities RBCMEP program.

# Auditing The CIP Standards

- Certain standards are inherently more risky than others.
  - Some rely on a high degree of Human Performance to be successful.
  - Some, if failed, pose a significant risk to the Bulk Electric System.
  - Some already have complexities and/or subtleties in their guidance from regulators that should be accounted for.
- The intent of the following slides is to provide key areas to review during an internal audit of your CIP program.
- This is not intended to be a comprehensive overview of all 120 Requirements/Sub-Requirements.

# CIP-002-5.1

- This standard is the under-pinning of your entire CIP program.
- The largest fines for CIP violations happen when a CIP-002 execution is flawed.
- Under version 5, CIP-002 will 'bucket' your assets into High, Medium and Low classifications.
- Based on that classification, some or all of the Requirements/Sub Requirements will need to be applied.
- CIP-002 was 'simplified' under Version 5 to remove the need to develop & maintain a methodology.
- Instead, a series of objective criteria are applied to all assets from a specific list such as Control Centers, Transmission Substations and Generation resources.

# CIP-002 continued…

- Show Your Work
  - Although the results matter, entities must show how they achieved those results to pass an audit by the regulators.
  - Evidence that the entire population of assets was considered must be retained.
- Misuse
  - One of the subtleties of this standard is the idea of ‘misuse’ as it applies to supporting systems (such as your Patch Management system).
  - Show the work that documents that all systems were evaluated.
  - Show the proof (vendor documentation? Firewall rules?) that proves a system cannot be misused to impact the BES within 15 minutes.
- There is no such thing as “No Impact”

# CIP-003-6

- This standard is much more brief than under version 3.
- Major components were moved to CIP-010 and CIP-011.
- Primarily it revolves around having Policies (signed by the CIP Senior Manager) that govern your program and protecting Low Impact assets.
- Low Impact protections do not need to be in place until 7/1/2017 and include:
  - Ensure your policies address Lows
  - Have a Security Awareness Program at Lows
  - Have Physical Access Controls at Lows
  - Restrict electronic access where devices are network accessible or dial-up accessible
  - Ensure your Incident Response Plan addresses Lows

# CIP-004-6

- Areas to focus on during an internal audit include:
  - Review proof that a Quarterly Security Awareness message was provided to all personnel with authorized electronic or authorized unescorted physical access to BES Cyber Systems.
    - It is NOT necessary to prove personnel reviewed the materials.
  - Training must be provided prior to gaining access and at least every 15 calendar months. Evidence should show this.
  - Training must be 'appropriate' to individual roles, functions or responsibilities. Therefore evidence of what those 'roles' are and how you classify personnel into them should exist.
  - Ensure your training program covers all 9 topics/areas, for all personnel, as outlined in Requirement 2.1.
  - Review your Personnel Risk Assessment Program against the R3 sub requirements to ensure all required elements are captured.

# CIP-004-6 continued…

- Areas to focus on during an internal audit also include:
  - Review the process used, every calendar quarter, to ensure that Access that has been given has a corresponding Authorization record.
  - Review the process used, at least every 15 calendar months, to ensure that the electronic access that exists is the correct access.
  - Access Removal has changed significantly under Version 5 and was one of the most commonly failed standards under Version 3.
    - Evidence should exist that physical and interactive remote access was removed within 24 hours of any termination access (including retirements and voluntary departures).
      - This is 24 hours… not a calendar day… and weekends/holidays count.
    - Evidence should exist that for reassignments or transfers, access that is no longer necessary was revoked by the end of the next calendar day.
    - Evidence that access to 'information' was removed by the end of the next calendar day for all terminations.
    - There are additional '30 day' removal requirements that can be checked.

# CIP-005-5

- Areas to focus on during an internal audit include:
  - What evidence is there that ALL applicable Cyber Assets, connected via a routable protocol, reside within an Electronic Security Perimeter (ESP)?
    - Some regions are interpreting serially connected relays as needing to be classified within the ESP. Check with yours.
  - All ESPs, need an EAP (Electronic Access Point) through which all External Routable Connectivity (ERC) passes.
    - Typically this is a Firewall. How does your organization define it and does every 'breach' in the ESP perimeter have an associated device?
  - Check for Dial-Up connectivity. Is that exists (ex: a modem in a substation allowing remote connectivity to a communications processor), R1.4 applies or a TFE needs to be filed.
  - Is there evidence that all Interactive Remote Access sessions utilize an intermediate system? (*i.e. do you have, perhaps, a Jumphost running something like Citrix, that your remote personnel use to access BES Cyber Systems/Assets*).
    - Ensure there is no direct interactive connectivity through the Access Point.

# CIP-006-6

- Areas to focus on during an internal audit include:
  - Review the Physical Security Plan.
    - Under version 3 different rules applied (i.e. a 6 walled border was required).
    - Under version 5 the plan must include “controls to restrict physical access.”
    - What evidence exists that your plan will restrict access that utilizes at least 1 physical access control (for Medium Impact) and 2 or more different physical access controls (for High Impact)?
  - Monitoring, Alerting and Logging of various things are required. Your PACS (Physical Access Control Software) likely handles this but evidence could be reviewed.
  - When wiring leaves the PSP, is it protected? If not, are the allowed electronic controls in place? (R1.10)

# CIP-006-6 Continued…

- Areas to focus on during an internal audit also include:
  - Review evidence that all visitors had continuous, escorted access whenever they were within a PSP.
    - Often this is a log showing the person was signed in and 'escorted' by an authorized individual and a procedure stating that person must continually escort them while inside the PSP.
  - Ensure logging occurred for all visitor entry into and exit from the PSP.
    - If you have a location with multiple PSPs (perhaps multiple control houses at a substation or multiple secured areas within a power plant), how did you log the visitors into each of those? Or was logging only done at the main gate?
  - Review evidence of Maintenance and Testing (every 24 months) of each PACS and locally mounted hardware.
    - Don't forget about things such as the magnetic locks that you likely have on the doors.

# CIP-007-6

- Areas to focus on during an internal audit include:
  - A list of necessary 'logical network accessible ports' will exist.
    - Review the evidence that the ports are deemed necessary.
  - Review evidence of how the physical ports (*such as a USB port*) on the BES Cyber Assets are protected.
    - This may include Port Locks or Signage or they may be logically disabled.
  - Patch Assessment was a highly failed requirement under version 3. Under version 5 it becomes more complex since patches now need to be applied as well.
    - What are your Patch Sources? Are those sources reasonable ones such that your entity would learn about important security patches?
    - Review evidence that all security patches were tracked and 'evaluated' (for applicability) at least once every 35 calendar days.
    - Review evidence that the patches were applied within 35 calendar days of being 'evaluated'.

# CIP-007-6 Continued…

- Areas to focus on during an internal audit also include:
  - If a Mitigation Plan (MP) was created, in place of applying a patch, that MP needs to include specific actions that address the vulnerabilities within that security patch (*i.e. an entity cannot just have a generic statement for all MPs that reads that they have a firewall therefore no one can reach the asset therefore the risk is mitigated*).
  - Review evidence that 'events' are being logged at the BES Cyber System level per R4.1. Are those events triggering alerts if detected?
  - For your High Impact locations, every 15 calendar days a method must be used to see if there were any undetected Cyber Security Incidents (sampling or summarization is acceptable).
  - Review evidence that access to 'Shared Accounts' is tracked. Who knows the password? What do you do when someone leaves the group who knows the password?
- There are other requirements in CIP-007 that could be sampled and reviewed. These were some of the more common challenge areas.

# CIP-008-5

- This standard is all about your Cyber Security Incident Response Plan.
- The Version 5 requirements are very similar to the Version 3 requirements. If you had a strong program under v3 then you are likely in good shape under v5.
- Generally this does not require much effort to review and is relatively low risk.
- Some areas to consider reviewing are:
  - Does your plan "identify, classify and respond" to incidents? - Plans sometimes start by assuming an incident was already identified and thus fail to include that component.
  - Are the roles and responsibilities of involved groups clearly defined?
  - Have you ever had an incident? If so, records must be retained.
  - Is the plan being tested at least every 15 calendar months?

# CIP-009-6

- This standard is about recovering your asset. The key to CIP-009 is having a "technical recovery plan" that has sufficient level of detail that a 'mid level' technical person could follow it successfully.
  - One way to think about that is to ask the question: If you had an emergency and brought in trained personnel from another company and handed them your procedure, could they follow it, without any additional help or guidance, and recover your asset?
  - If not, then there is not enough technical detail in the procedure.
  - Does your plan include the 'conditions' that would cause it to be activated?
  - Are the roles and responsibilities clearly defined?
  - Is there a process to verify SUCCESSFUL backups? And fix unsuccessful?
  - Is the plan tested at least every 15 calendar months?
  - Is an actual recovery done every 36 months for High Impact assets?

# CIP-010-2

- Under version 3, configuration and change management was largely limited to CIP-003 R6 which required entities to “control change”. Under version 5, the requirements are much more explicit and related requirements are consolidated into CIP-010.
- Areas to focus on during an internal audit include:
  - There will exist a “baseline”. Does it contain all the elements in R1.1?
    - Custom Software is inclusive of “scripts” your entity has written.
    - Guidance from our lead region (who said NERC and the other regions concur) is that ALL custom scripts must be included even if they just generate a report or run a WinAudit scan.
  - Is there evidence that all changes to the baseline are “authorized” and “documented”?
  - Is there evidence that PRIOR to the change being implemented, impacted cyber security controls were identified?

# CIP-010-2 Continued…

- Areas to focus on during an internal audit also include:
  - FOLLOWING the change (i.e. in Production), is there evidence that those cyber security controls are not adversely affected?
  - For your High Impact systems, were the changes tested in a test environment? (or if they were tested in production, was it done in a way so as to minimize adverse effects such as doing them on a fail over server first?)
  - What evidence is there that at least every 35 days your High Impact systems were monitored to detect changes in their baseline?
  - Vulnerability Assessments are largely the same under version 5 but a change is that an 'active' scan needs to be performed every 36 months for High Impact systems.
  - If your environment uses Removable Media (i.e. USB drives) or Transient Devices (i.e. a laptop your technicians bring around to substations) there are requirements in CIP-010 Attachment 1 that need to be adhered to. Auditing for those controls would be useful.

# CIP-011-2

- Information needs to be protected. The explicit requirement to "label" your information no longer exists under version 5.
- Areas to focus on during an internal audit include:
  - If your program is not labeling information, how does a person know what information has to be protected? One possible answer is a training program that teaches them how (i.e. all drawings of X and Y type are considered BES Cyber System Information)
  - Review evidence of how your information is 'identified' as needing to be protected.
  - Review the procedure for protecting the information including while the information is in transit (i.e. is placing it in the trunk required when someone leaves a vehicle unattended?).
  - Have any assets been disposed of? Or reused? If so, is there evidence that they were wiped clean such that the information on them could not be retrieved?

# Prepping For An Audit By Regulators

- Some high level considerations for an external audit by your regulators include:
  - Will your audit be an off-site audit? Many future audits will follow an off-site model. That means that SME testimony plays a very small role.
  - As such, your Procedures should be written in such a way that a third party can clearly understand them without needing a SME to testify.
  - NERC has provided an Evidence Spreadsheet. The regions will be using that for their audits. Obtaining it now and filling it out may be easier than trying to complete it right before an audit.
  - If your program is large and/or complex, you may want to consider an overall narrative for each area that explains how the pieces fit together. Does one group patch the server while another group tests the changes and a third group operates the system? That can be difficult to glean from 3 different procedures during an off-site audit without an overall narrative explaining your processes.

# Questions?