NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Study Final Report

CIP Version 5 Transition Program

October 2014

RELIABILITY | ACCOUNTABILITY



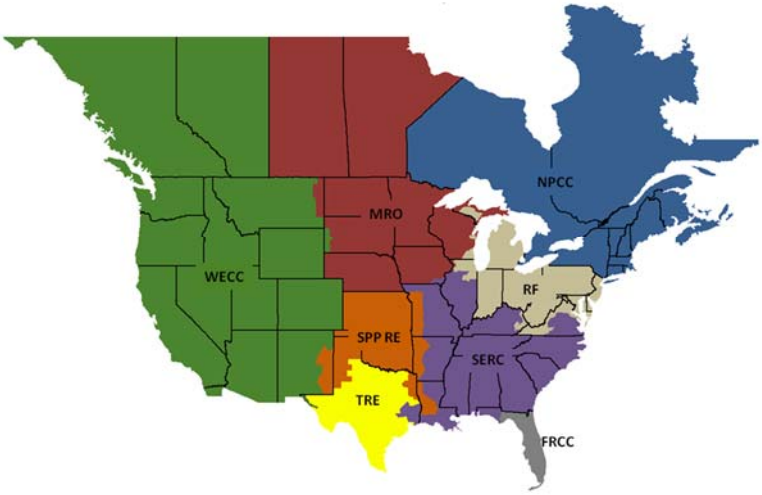

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into several assessment areas within the eight Regional Entity (RE) boundaries, as shown in the map and corresponding table below.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP-RE	Southwest Power Pool Regional Entity
TRE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

On November 22, 2013, FERC issued Order No. 791, approving new and revised Critical Infrastructure Protection (CIP) Reliability Standards, referred to as CIP Version 5.[1] NERC initiated a transition program (the CIP Version 5 Transition Program) to: (1) improve industry's understanding of the technical security requirements for CIP Version 5, as well as the expectations for compliance and enforcement of those standards; and (2) help industry implement CIP Version 5 in a timely and effective manner.

As part of this program, NERC conducted a study, referred to as the Implementation Study for the CIP Version 5 Transition Program in which six industry participants (the study participants) implemented elements of CIP Version 5 in an accelerated time frame to help the ERO understand the challenges entities may face transitioning to CIP Version 5, identify guidance topics, and provide feedback to other entities on such topics to help ensure an efficient and effective transition industry-wide. This report discusses the results of the Implementation Study and was developed in collaboration with the study participants.

Acknowledgements

NERC would like to thank those who contributed their time, expertise, and resources to make the Implementation Study for the CIP Version 5 Transition Program a success. The Implementation Study would not have been possible

[1] In Order No. 791, the Commission approved NERC's request to allow entities to transition to compliance with CIP Version 5 directly from the currently effective CIP Reliability Standards, referred to as CIP Version 3, bypassing an interim set of CIP Reliability Standards, referred to as CIP Version 4, that were approved by FERC but not yet effective.

without the commitment and active contribution of each of the following participants selected from industry volunteers:

- Dayton Power & Light (DP&L)
- MidAmerican Energy (MidAmerican)
- Sacramento Municipal Utility District (SMUD)
- Southern Company (Southern)
- Tennessee Valley Authority (TVA)
- Westar Energy (Westar)

Of particular importance was the willingness of study participants to share their issues, challenges, and solutions with other study participants, NERC, and the Regional Entities, and now, through this report, with the rest of the industry. This information was invaluable and enabled NERC to develop and share lessons learned with all responsible entities.[2] This collaboration will greatly facilitate the transition of all responsible entities to the CIP Version 5 standards.

Appendix A identifies the individuals from NERC, the Regional Entities, and study participants directly involved in the Implementation Study.

[2] For the purpose of this report, the term "responsible entity" has the same meaning as that specified in the CIP Version 5 standards.

Executive Summary

The CIP Version 5 standards represent a significant improvement—and change—over the currently-effective CIP Version 3 standards as they include new cybersecurity controls and extend the scope of the systems that the CIP Reliability Standards protect. Therefore, NERC initiated the CIP Version 5 Transition Program in an effort to collaborate with Regional Entities and responsible entities to understand how best to implement the CIP Version 5 standards in a manner that is timely, effective, and efficient.

The Implementation Study, an important part of NERC's overall CIP Version 5 Transition Program, centered on a representative sample of six responsible entities that volunteered to transition to compliance with the new standards during an accelerated time frame. During the Implementation Study, the study participants focused on technical solutions and processes needed to implement the CIP Version 5 standards, and they developed a deeper understanding of compliance and enforcement matters unique to CIP Version 5. As anticipated, NERC, the Regional Entities, and the study participants identified a number of issues through the course of the study that called for additional guidance and clarity. Some of these issues were of a technical nature; others related to how to adequately demonstrate compliance with a particular CIP Version 5 standard or requirement. NERC and the Regional Entities collaborated with study participants to develop guidance for broad stakeholder review. While many of the issues were relatively straightforward, some were particularly challenging and required significant time and effort of the study participants, Regional Entities, and NERC to address sufficiently.

Considering the diversity of the study participants in terms of their responsibilities under the NERC functional model and the assets they own and operate, there was surprising consistency regarding the issues they identified as the most challenging. While none of the participants planned or expected to completely transition to CIP Version 5 during the period of the study, they indicated that they made considerable progress and that their efforts substantially increased their confidence that they will be ready to implement the CIP Version 5 standards successfully on or before their effective date.[3] Each of the study participants emphasized that they appreciated taking the opportunity to begin their transition early.

This report describes how each study participant approached their transition to CIP Version 5, including how they planned and organized their contribution to the study, assigned the necessary resources, and identified aspects of the transition they found most challenging. The report also provides a summary of the guidance documents developed or being drafted as a result of the lessons learned during the Implementation Study. To date, approximately 20 lessons learned documents and many more frequently asked questions (FAQ) documents have been developed or are in the process of undergoing broad stakeholder review. While these documents are designed to represent a comprehensive set of guidance documents that will help all responsible entities transition to CIP Version 5, NERC and the Regional Entities will continue to collaborate with stakeholders to develop additional documents as new issues are identified.

Following the issuance of this report, NERC, in collaboration with the Regional Entities and the study participants, expects to take the following actions to help all responsible entities meet the implementation date for CIP Version 5:

1. During Q4 2014, NERC, in collaboration with stakeholders, expects to implement a process to continue to develop lessons learned and FAQ reference documents, as identified by responsible entities, which will include a mechanism for obtaining broad industry stakeholder review, and results in the posting of these documents on the NERC website once completed.

[3] NERC has published "CIP V5 Transition Guidance" that outlines NERC's approach to compliance and enforcement activities as entities transition to CIP Version 5: http://www.nerc.com/pa/CI/Documents/V3-V5%20Transition%20Guidance%20FINAL.pdf

2. By the end of Q1 2015, NERC and the Regional Entities expect to develop a plan for and begin conducting additional CIP Version 5 transition outreach efforts as well as provide sample CIP Version 5 implementation reviews to as many responsible entities as possible. The intent of these outreach efforts is to provide responsible entities with opportunities to learn from the experiences of study participants and include a mechanism to identify new or unresolved issues for NERC and the Regional Entities to develop a coordinated response. The outreach will leverage existing industry stakeholder mechanisms and media such as webinars, recorded presentations, web postings, and in-person sessions.
3. By the end of Q2 2015, NERC expects to review, revise, or retire CIP Version 3 documents, as applicable, for consistency with CIP Version 5. These documents include, for example, Appendix 4D of the NERC Rules of Procedure related to Technical Feasibility Exceptions, Compliance Analysis Reports, Compliance Application Notices, CIP Interpretations, and mechanisms to retire CIP Version 3 Technical Feasibility Exceptions.
4. Through Q3 2015, NERC and the Regional Entities will follow up with study participants to review their experience with their continued implementation of CIP Version 5, particularly those requirements that were outside the scope of the study to determine if these areas require additional attention and guidance (i.e., CIP-003-5, CIP-004-5, CIP-008-5, CIP-009-5, and CIP-011-1).

Introduction

CIP Version 5 Transition Program Goals

Based on its prior experience, NERC understands that a myriad of issues can arise as entities transition to new or revised versions of reliability standards. If these issues are not properly understood and addressed through guidance documents and other outreach efforts, they could result in a spike of noncompliance upon the effective date of the new or revised reliability standards. There is a great deal of interest by NERC and its stakeholders to ensure that responsible entities implement CIP Version 5 in a timely manner that enhances cybersecurity without imposing unnecessary or burdensome administrative processes. To that end, NERC initiated the CIP Version 5 Transition Program to collaborate with Regional Entities and responsible entities to understand how best to implement the CIP Version 5 standards in a manner that is timely, effective, and efficient. As described further below, the ultimate goal of the transition program is to reduce uncertainty regarding the approaches to be adopted during the transition period, and to instill confidence in responsible entities that their approaches to implementation will result in compliance with CIP Version 5.

NERC established the CIP Version 5 Transition Program with the following goals:

Goal 1 – Implementation
Improve industry's understanding of the technical security challenges that need to be addressed to comply with the CIP Version 5 standards, with emphasis on the material differences between Version 3 and Version 5.

- Responsible entities will confirm their understanding of new or different technical security solutions needed to comply with the CIP Version 5 standards.
- Responsible entities will understand how to comply with CIP Version 5 in situations where a technical solution is not feasible.

Goal 2 – Compliance and Enforcement Expectations
Provide industry with a clear path and approach to transition from CIP Version 3 to CIP Version 5 that includes expectations for compliance and enforcement.

- Responsible entities will know what evidence they need to retain to demonstrate compliance with the CIP Version 5 standards.
- Regional Entities will have a consistent view of how to monitor compliance of responsible entities.

Goal 3 – Resource Requirements
Provide industry and Regional Entities an understanding of the technical- and compliance-related resources and efforts needed to transition and manage compliance with the CIP Version 5 standards.

- Responsible entities will understand what resources they need to transition to and comply with the CIP Version 5 standards.
- Regional Entities will understand what resources they need to monitor responsible entities' compliance with the CIP Version 5 standards.

Key Elements of the Transition Program
The transition program is composed of five key elements.

- **Periodic Guidance:** To provide guidance to industry, through posting lessons learned and frequently asked questions documents, as they are developed throughout the transition period.

- **Implementation Study**: To work closely with a small number of responsible entities that will implement aspects of CIP Version 5 in an accelerated time frame, and to share lessons learned based on that study with all responsible entities.
- **Compliance and Enforcement:** To further develop approaches to demonstrate compliance consistent with the risk-based Compliance Monitoring and Enforcement Program, as transformed through the Reliability Assurance Initiative.[4]
- **Outreach and Communications:** To keep all stakeholders informed of developments related to the implementation of CIP Version 5 and invite their input throughout the entire CIP Version 5 Transition Program.
- **Training:** To provide timely training to Regional Entities and responsible entities on topics related to CIP Version 5 implementation in a manner suited to their needs.

The Implementation Study has been an important part of the transition program. It provided an opportunity for NERC, Regional Entities, and responsible entities to experience what is required to implement the CIP Version 5 standards in operational environments. The Implementation Study helped inform the entire transition program by creating an opportunity for NERC and the Regional Entities to engage with responsible entities to answer their questions well in advance of the implementation date.

[4] Ref. NERC website http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx.

Implementation Study Methodology

Overview of the Implementation Study

The Implementation Study centered on a representative sample of volunteer responsible entities that agreed to transition to compliance with CIP Version 5 in an accelerated time frame. Study participants were selected based on their history of successful CIP Version 3 compliance, demonstrated effective internal controls, and a willingness to commit the required resources to support their transition.

The Implementation Study began on October 1, 2013. Participants focused on technical solutions and processes needed to meet the CIP Version 5 standards and developed a deeper understanding of compliance and enforcement matters unique to CIP Version 5. Study participants asked questions, identified issues, offered their own perspectives, and collaborated with NERC and the Regional Entities to develop solutions that would be applicable to all responsible entities. These solutions were shared publicly on the NERC website and through outreach mechanisms such as webinars and training sessions. Topics included:

- Differences between CIP Version 3 and CIP Version 5
- Technical security practices needed to meet the CIP Version 5 requirements
- Practices need to demonstrate compliance with the CIP Version 5 requirements, including effective internal controls to address deficiencies

The Implementation Study concluded on June 30, 2014, with in-person close-out meetings at each of the participating entities to review the progress they had made, identify key lessons learned, and discuss any remaining issues that had not yet been completely addressed. NERC and the Regional Entities will continue to work with study participants to address outstanding issues through the remainder of the transition program.

Responsible entities provided subject matter expertise in areas such as operations, cybersecurity, and compliance. These individuals were intimately familiar with the tools and processes needed to comply with the CIP Version 3 standards and had been directly involved in recent CIP audits. The Regional Entities were the primary liaisons with participating responsible entities. NERC led the overall project, provided support and expertise as needed, and prepared lessons learned and other guidance documentation in collaboration with the study participants.

The Implementation Study was composed of three phases: (1) deciding the study's scope, (2) conducting a series of detailed studies with selected responsible entities, and (3) communicating progress and final results with all NERC stakeholders. There was continuous overlap in the second and third phases to help ensure that lessons learned during the study were developed with all responsible entities in mind, not just the study participants.

Participating Responsible Entities

While many responsible entities from across the industry had expressed an interest to participate in the Implementation Study, it was important that selected participants collectively provided a representative sample of the functional entities and assets that comprise the Bulk Electric System (BES). After considerable discussion with interested responsible entities and their Regional Entities, NERC selected six participants.

Table 1 describes the selection criteria used to decide optimal participation.

Table 1: Responsible Entity Selection Criteria	
Criterion	**Description**
Regional Entity Participation	Maximum of two responsible entities from each Regional Entity. Each Regional Entity may participate in at least one study with a responsible entity (i.e., not necessarily within the Region).
Compliance History and Performance	Limited number of outstanding CIP violations. Minimal CIP Version 3 violations identified during an audit. Responsible entity has recently been audited under CIP Version 3.
Diversity of BES Cyber Assets	Responsible entities collectively span all functional entities subject to CIP Version 3 and CIP Version 5 standards. Responsible entities collectively operate a mix of generation, substation, and Control Center assets. Responsible entities own diverse BES Cyber Assets and BES Cyber Systems.
Responsible Entity Engagement and Available Resources	Responsible entity has demonstrated a willingness to proactively address challenging technical security and compliance issues. Responsible entity has sufficient resources available to participate and comply with CIP Version 5 during the study period. Responsible entity has demonstrated a high level of communication with NERC staff and the Regional Entities.

Scope of the Implementation Study

Throughout the Implementation Study, emphasis was placed on the more significant changes between CIP Version 3 and CIP Version 5. These include:

- CIP-002-5: BES Cyber System Categorization, including:
  - Applying Impact Rating Criteria and the 15-minute impact on real-time operations
  - New term, BES Cyber Asset
  - New term, BES Cyber System
- CIP-005-5: Electronic Security Perimeter(s) including new requirements for Interactive Remote Access
- CIP-006-5: Physical Security of BES Cyber Systems
- CIP-007-5: Systems Security Management
- CIP-010-1: Configuration Change Management and Vulnerability Assessments
- Process to identify and address low-risk violations consistent with the Reliability Assurance Initiative
- Other areas as identified by study participants

BES Cyber Systems with a low impact rating were out of scope for the study as the standards drafting team was in the process of preparing new CIP Version 5 standard requirements as directed by FERC Order No. 791.

While the study participants considered the parts of the CIP Version 5 standards identified above to be the most resource intensive, they were encouraged to include additional requirements according to their individual needs as part of their contribution to the study. For example, one utility added CIP-009-5 Recovery Plans for BES Cyber

Systems to the scope of its study. Study participants were asked to evaluate their high- and medium- impact rating facilities as determined by applying the criteria in Attachment 1 of CIP-002-5 R1. Some study participants selected their main and backup control centers to be included in the study, while others selected key substations and generation resources. NERC and the respective Regional Entity evaluated these selections to determine if the proposed scope would provide optimal value to the industry.

Table 2 illustrates the scope of the Implementation Study, the breadth of facilities, and the impact rating of their BES Cyber Systems.

Table 2: Scope of Study

Facility	DP&L	MidAmerican	SMUD	Southern	TVA	Westar
Control Centers, Backup Control Centers		High	High	High	High	
Substations without routable communications protocol		Medium				Medium
Substations with routable communications protocol	Medium	Medium	Medium	Medium	Medium	Medium
Generation Facilities Greater than 1500 MW	Medium	Medium		Medium		Medium

Communicate Results

Throughout the Implementation Study, it was important that lessons learned were shared with all study participants. Much of this information was sensitive from a security perspective, as it could identify BES Cyber Assets and the controls in place to protect them. Therefore, one of the Regional Entities hosted a web-based portal to provide a secure collaboration work space for the study.

While it was important to share information with and between study participants, the ultimate goal was to share results in the form of lessons learned and other guidance with all responsible entities. For this purpose, NERC established dedicated web pages on its public website to ensure that study results were made available throughout the Transition Program as quickly as possible, without waiting for the entire project to conclude.

- **Transition Program Web Page.** This page provides an overview of the entire transition program and answers to FAQs and various communications outreach initiatives.
- **Implementation Study Web Page.** This page provides details specific to the Implementation Study, such as FAQs and answers related to technical topics or specific CIP Version 5 requirements. It also provides individual lesson learned documents that address more complex topics.

Discovering Implementation Challenges

This section provides an overview of how study participants committed the right resources to identify and address issues through the Implementation Study. In general, each of the participants successfully completed their Implementation Study within the scope of their plan. That said, study participants needed to commit additional resources to the Implementation Study. This was noteworthy, as some study participants experienced a substantial increase in the number of Cyber Assets considered to be in scope for CIP Version 5 compared with CIP Version 3.

All study participants concluded that the Implementation Study enabled them to identify the key issues and challenges they needed to address in order to transition to the CIP Version 5 standards. While some of these issues were of a technical nature (e.g., the best method to adequately protect a BES Cyber System), others were related to how to adequately demonstrate compliance with a particular CIP Version 5 standard. Study participants included all of the NERC functional entities specified in the CIP Version 5 standards: balancing authority, distribution provider, generator operator, generator owner, interchange coordinator, reliability coordinator, transmission operator, and transmission owner. In spite of their diverse functional responsibilities, study participants found they had a common view regarding many aspects of CIP Version 5 implementation they considered to be most challenging. For example, understanding how to identify their BES Cyber Systems and BES Cyber Assets (i.e., CIP-002-5 BES Cyber System Categorization) and committing the right resources to their transition efforts stood out as important starting points for study participants.

The study participants were selected in part based on their track record in implementing the CIP Version 3 standards. Bearing this in mind, for those responsible entities who have not yet begun to transition to CIP Version 5, perhaps the most revealing feedback was that each of the study participants saw great value in starting early.

Resources Committed to the Implementation Study

Without exception, each of the study participants committed the necessary personnel to participate fully in the Implementation Study. This required the dedicated involvement of management and staff at all levels in their organizations, including:

- Executive management who provided organization-wide leadership and committed the necessary resources;
- Managers and supervisors who provided direction and oversight;
- Engineering subject matter experts who helped ensure that security solutions were designed to provide the appropriate protection to enhance BES reliability (e.g., develop policies and controls for deploying systems, evaluate new systems for appropriate protection and compliance);
- Field technical subject matter experts who helped ensure that security solutions were implemented, operated, and maintained in a manner that provided the appropriate protection and sufficient evidence to demonstrate compliance (e.g., implement controls and access requirements, coordinate corrective actions if issues arise);
- Enterprise-level security personnel who provided consistent direction across the organization to monitor security controls and associated workflows (e.g., work management tickets, detecting incidents or events); and
- Compliance and regulatory personnel who provided consistent direction across the organization to help ensure that security solutions met compliance and audit requirements.

Study participants recognized the need for a structured compliance program: one that promotes a consistent culture and approach across the entire organization. Processes need to be documented in a clear and concise manner so they can be readily understood and used to identify and protect BES Cyber Assets as well as demonstrate compliance. Some participants noted the advantages associated with separating workflow roles, for example, by assigning different people or teams to be responsible for implementing security processes from those validating them.

Study participants managed their transition to CIP Version 5 as a formal project within their organizations. While few, if any, staff were assigned to the study on a full-time basis, many noted that a substantial amount of their time was committed to the study through the course of the project. This varied from about 20 individuals in some study participant organizations to 50 or more in others.[5] No study participant planned or expected to complete the transition to CIP Version 5 during the study period. All study participants acknowledged that substantial effort would need to carry on for some months to complete the transition to CIP Version 5.

Impact on Existing Processes

In general, study participants were able to leverage their existing CIP Version 3 processes to implement CIP Version 5, but had to revise their documentation to meet the new requirements. One participant indicated that about 70 percent of their existing processes would continue to be applicable, but had to revise all their documentation. In many cases, however, participants found it essential to involve new staff in these processes, particularly those responsible for areas related to protecting transmission and generation assets at field locations. While study participants acknowledged that orienting and training these new staff on the CIP Version 5 standards was time-consuming, they considered it essential to involve field staff at an early stage as these individuals would ultimately be responsible for implementing, maintaining, and demonstrating compliance.

Study participants found it important to integrate CIP Version 5 requirements related to configuration and change management with their existing workflow management processes. Study participants with many medium-impact rating BES Cyber Systems at their transmission or generation facilities recognized that spreadsheets alone would not be an effective or efficient method to manage and document how they protect their BES Cyber Assets. In addition to advantages such as single-source data entry and consistency, automated workflow systems also provide easier mechanisms to support the capture of evidence needed to demonstrate compliance. Study participants emphasized the need to automate. Responsible entities with relatively few medium-impact rating BES Cyber Systems at their transmission or generation facilities may find spreadsheet-based documentation processes to be sufficient.

CIP Version 5 Implementation Challenges

The study participants identified the following challenges.

Challenges Identified by Study Participants at Study Kickoff

On September 20, 2013, NERC hosted an Implementation Study kickoff meeting with study participants and the Regional Entities at its Atlanta offices. The meeting provided participants the opportunity to develop a common understanding of the goals and scope of the study. Discussion topics included:

- Overview of draft project plan (scope and required resources, key project milestones)
- Significant differences between CIP Version 3 and CIP Version 5
- Perspectives of Regional Entities and responsible entities

[5] Other responsible entities with fewer BES Cyber Assets than those of the study participants may not require this level of resourcing to transition to CIP Version 5.

- Overview of the Reliability Assurance Initiative
- Draft CIP Version 5 Reliability Standard Audit Worksheets (RSAWs)

The meeting also provided an opportunity for participants to identify what they anticipated to be the more significant issues to be addressed during the study. Participant understanding of some aspects of the CIP Version 5 requirements varied, but most concurred on how to implement the CIP Version 5 requirements and what resources are required to do so.

Challenges Related to Understanding the CIP Version 5 Requirements

- Developing a complete understanding of the definitions for BES Cyber Assets and BES Cyber Systems
- How to treat non-routable Cyber Assets
- How to treat facilities with discrete Electronic Security Perimeters under CIP Version 3, and how routable Cyber Assets are treated under CIP Version 5
- Implementing solutions for new inventory and change management requirements
- Mapping CIP Version 3 Critical Cyber Assets to CIP Version 5 BES Cyber Assets without missing any
- Anticipating future changes after CIP Version 5 is approved
- The need to adapt the Implementation Study to address new challenges that emerge
- Current uncertainty regarding the substance of FERC's final order
- Possibility of telecommunications assets being included in CIP Version 5

Challenges Related to Implementing the CIP Version 5 Requirements

Study participants expressed particular interest in including new facilities (e.g., certain generators and substations) as a result of the bright-line criteria that were not in the CIP Version 3 requirements. Other areas of interest included:

- Understanding how the Identify, Assess, Correct (IAC)[6] language will be used for audits and enforcement
- Consistency across all Regional Entities

Issues Related to Building Resource Capability

Participants expressed particular interest in training staff to understand and implement the CIP Version 5 requirements. Other areas of interest included:

- Supporting those who are not involved in the transition study to implement CIP Version 5
- Committing sufficient resources to support the study
- Maintaining two programs in parallel: compliance with CIP Version 3 while implementing CIP Version 5, and the associated change management
- Ensuring sufficient resources and time to comply with CIP Version 5

[6] NERC decided to remove the IAC process from within the scope of the Implementation Study as it is being addressed by a Standards Drafting Team in response to FERC Order 791.

This early feedback from study participants during the kick-off meeting helped shape how NERC, the Regional Entities, and study participants focused their time and effort during the Implementation Study. In particular, it was apparent that new in-scope facilities as a result of the CIP Version 5 bright-line criteria (e.g., certain generation resources and substations) represented the most significant item of change from CIP Version 3, closely followed by the need to train entity staff not yet familiar with any of the CIP standards.

Understanding Compliance Requirements

As the Implementation Study progressed, a persistent theme emerged. Study participants wanted to clearly understand the evidence they needed to have in place to demonstrate compliance for audit purposes. This was true even for requirements where the technical security solutions were relatively straightforward. Study participants acknowledged that their goal was to reach the point where compliance is recognized as an integral part of security performance.

From this perspective, the Implementation Study provided an excellent opportunity for participants to develop a common understanding of compliance expectations with their respective Regions. Perhaps even more importantly, the Implementation Study provided a forum for compliance staff at NERC and the Regional Entities to collaborate to develop consistent expectations. While progress was made to achieve these objectives with study participants, the Implementation Study served as a platform to develop training and education material for all responsible entities not involved in the study, as well as compliance and enforcement staff in NERC and the Regional Entities.

Topics of Particular Interest

While study participants themselves identified and addressed a myriad of issues and challenges through the course of the study, some issues needed to be addressed in consultation with NERC and Regional Entity cybersecurity and compliance staff. Toward the end of the study, participants converged on a relatively small number of issues considered to be of high interest, as outlined in Table 3.

Table 3: Topics of High Interest to Study Participants

CIP Version 5 Reference	Topic
CIP-002-5	Definition of “programmable”
CIP-002-5	Impact rating of generation resources (i.e., options to segment generating units at a single plant location)
CIP-005-5	Virtual computing environments
CIP-006-5	Impact rating of relays at connected substations (i.e., far-end line protection relays)
CIP-010-1	Configuration change management and vulnerability assessments

Table 4 identifies other topics that were of more moderate interest to study participants.

Table 4: Topics of Moderate Interest to Study Participants	
CIP Version 5 Reference	**Topic**
CIP-002-5	Determining BES Cyber Systems that could adversely impact the BES within 15 minutes
CIP-004-5	Personnel risk assessments
CIP-005-5	External routable connectivity as it applies to serially connected devices
CIP-005-5	Routable communication used in substations
CIP-005-5	Intermediate systems
CIP-006-5	Response to unauthorized physical access within 15 minutes
CIP-006-5	Two-factor access control
CIP-007-5	Patch management process
CIP-007-5	Logging of shared access accounts
CIP-007-5	Read-only access
CIP-007-5	Password management for line protection relays

Study Participant Approaches to CIP Version 5 Transition

This section provides each study participant's description of how they approached their transition to CIP Version 5. It discusses how they planned and organized their contribution to the study, assigned the necessary resources, and identified aspects of the transition they found most challenging. Given that participants were selected to represent a mix of responsible entities, it is not surprising that the approaches differed from participant to participant. The individual study participants tailored their approaches to meet the needs and characteristics of their organizations. Accordingly, the approaches described below may not work for other responsible entities, given their unique set of circumstances. The approaches offered here are only examples that other responsible entities may consider as they develop their CIP Version 5 transition approach.

Sacramento Municipal Utility District (SMUD)

Planning the Transition to CIP Version 5

Key to creating a successful CIP Version 5 transition program was the early and visible support of executive management. SMUD's executive team understood the benefits of participation in this program and thus made it an organizational priority, assigning an executive-level sponsor for the effort. To that end, SMUD's Chief Regulatory and Legislative Officer and CIP Senior Manager served as the project sponsor. The SMUD executive management team has subsequently supported the program implementation goals despite the challenges encountered along the way.

To launch, manage, and oversee the Implementation Study, SMUD created a CIP core team composed of subject matter experts from the key work groups and departments with responsibility for CIP compliance. This team included all primary requirement owners who are currently responsible for demonstrating compliance with the CIP Version 3 standards, as well as those personnel who will be responsible for protecting Cyber Assets that were not subject to compliance with previous versions of the CIP standards (i.e., field personnel responsible for substation equipment). Once the team completed CIP-002-5 procedures to identify new BES Cyber Assets, even more personnel were added to the team.

Despite the significant challenges associated with the effort, it was understood that participating in the Implementation Study was an organizational priority that would yield significant benefits to SMUD and the industry. This message was conveyed throughout the organization during the course of the Implementation Study. A program manager was appointed to oversee the implementation effort, and individual project managers were also assigned to coordinate the efforts of the Information Technology (IT), Energy Management System (EMS), and Compliance teams.

The following is a list of departments and number of personnel directly involved with the Implementation Study team activities. Departments that had no previous responsibilities under CIP Version 3 are indicated as "New."

- EMS (3)
- IT Information Security (2)
- Human Resources (2)
- Physical Security (1)
- Telecom (2)
- IT Networking (3)

- System Protection & Control (1) - New
- Metering (1) - New
- Reliability Compliance (3)
- Facilities (1)
- Substation Maintenance (1) - New
- Program Management (1)
- Organization and Workforce Development (1)

Total = 22 employees

The core team met on a weekly basis to discuss the status of action items, address emerging issues, and make strategic and technical decisions. Detailed notes were taken at each meeting to allow impacted personnel and other interested parties to monitor the Implementation Study's progress. The program manager and the IT and EMS project managers also met on a weekly basis to work through action items and issues.

When the core team could not reach agreement on pivotal issues, an executive-level Steering Committee (Committee) was appointed to drive solutions and arrive at a consensus. This Committee met every two weeks and as needed to monitor progress and help address difficult issues and their organizational impact. For example, extending CIP Version 5 asset protection protocols to the Implementation Study substation presented a complex challenge in assigning responsibility for the support of new technology (e.g., firewalls and routers). While SMUD's corporate IT team was best suited to manage the devices themselves, they lacked the necessary expertise from an operational perspective. Conversely, SMUD's EMS technicians had the long-standing expertise to operate assets from a reliability perspective but lacked the infrastructure to manage the firewalls. Ultimately, the Committee selected corporate IT to support the firewalls, and IT committed to changing their processes to support reliability.

The Committee also worked collaboratively to understand and resolve issues related to SMUD's system reliability policies and strategic directives to ensure that the necessary resources were allocated for the Implementation Study. The Committee also provided regular reports on the status of the CIP Version 5 implementation effort to SMUD's executive management.

SMUD also deployed a separate project team to address issues associated with implementing CIP-004-5 Personnel & Training. Due to the inclusion of new medium-impact substations requiring CIP protection, the number of field personnel subject to CIP requirements has been greatly expanded. SMUD determined that a separate effort was needed to ensure that the appropriate personnel completed their CIP-004-5 training and personnel risk assessments in a timely manner and that those new processes associated with the CIP requirements were properly communicated.

During the initial phase of the Implementation Study, SMUD held weekly teleconferences calls with NERC and WECC subject matter experts to review milestones and discuss technical issues requiring their interpretation of various CIP Version 5 requirements. SMUD's plans to address the compliance gaps between CIP Version 3 and CIP Version 5 were discussed and evaluated during these calls.

Designing Security Solutions

SMUD combined the hours spent for planning, design, and implementation into one project work order, so the exact breakdown of man-hours dedicated to each defined task is not available. However, SMUD estimates that at

the time of the Implementation Study close-out meeting, SMUD had dedicated 40 percent of project man-hours to planning, 40 percent to design, and the remaining 20 percent to implementation.

SMUD has devoted considerable resources[7] to CIP Version 5 implementation, as illustrated in Table 5.

Table 5: SMUD Cost Summary

Cost Element	Hours	Amount
Program Management	2,060	$270,000
Technical – Design, Planning, and Implementation	9,700	$1,220,000
Materials	Not Applicable	$110,000
External Resources	Not Applicable	$600,000
Total		$2,200,000

SMUD created a gap analysis document for each CIP Version 5 standard to address all new requirements. These gap analysis documents provide a roadmap to guide the transition and verify that all potential compliance gaps are adequately addressed. Leveraging SMUD's SharePoint system as the repository for Implementation Study documents, subject matter experts from the various business units worked collaboratively to identify and align CIP Version 3 compliance practices with those that are necessary under CIP Version 5.

SMUD employed a "top-down" approach to complete CIP-002-5, Requirement R1. Once SMUD determined the impact rating of each asset and facility and analyzed the associated Cyber Assets, they arrived at a list of qualified BES Cyber Assets. This resulted in a list of all Cyber Assets for high- and medium-impact assets, along with documented rationale for why each asset was or was not qualified as a BES Cyber Asset. SMUD used the BES Reliability Operating Services (BROS) functions described in the *Guidelines and Technical Basis* section of CIP-002-5 to determine whether a Cyber Asset could impact the reliable operation of the Bulk Electric System pursuant to the definition of "BES Cyber Asset."

During the design phase and weekly calls with NERC and WECC, several lessons learned were captured that affected SMUD's methodology and overall approach to achieve compliance. These lessons learned were documented and submitted to NERC during the Implementation Study.

SMUD leveraged its existing tools to implement CIP Version 5, including applications for automated workflows and customized in-house solutions. A long-term project is underway to identify and implement new automation for CIP-004-5 process that will improve provisioning for access to BES Cyber Systems, enhance record keeping for training and personnel risk assessments, and provide an additional layer of controls to address the reduced time frame for access revocations found in CIP Version 5.

Implementing Security Solutions

SMUD stated that their biggest challenge during the implementation of CIP Version 5 involved engaging new business units that were not previously subject to CIP reliability standards and requirements (primarily at substations). For any entity that has never before implemented CIP requirements at substations or generators, this challenge cannot be overstated. SMUD relied on existing CIP subject matter experts to communicate CIP

[7] These figures do not include costs for management and executive oversight and do not reflect costs associated with mitigation of any subsequently identified program gaps.

concepts and practices to these newly impacted groups and individuals. This is an ongoing process, and SMUD anticipates spending significant additional time and resources to ensure that personnel have the training and tools necessary to achieve the compliance and security objectives under CIP Version 5. Substation personnel responsible for Protection Systems, Remote Terminal Units (RTUs), and tie-line metering will need to integrate their core job functions with new policies and procedures governing CIP compliance. The substation facilities themselves require physical hardening to become CIP-compliant. This includes designing and installing Personnel Access Control Systems (PACS), firewalls, and Physical Security Perimeters (PSPs), and implementing and reinforcing associated controls.

Identifying metrics to measure the additional workload was a significant challenge and should not be minimized when quantifying a previously unbudgeted project of this magnitude. It was obvious that additional resources were necessary, but the difficulty in capturing that data became evident as the Implementation Study progressed. Entities should consider the merits of granular recordkeeping of time invested in CIP Version 3 processes in order to create a realistic baseline from which to measure the incremental increases in time, labor, and materials required to transition to CIP Version 5, as well as the increased time needed for additional operational requirements.

Tennessee Valley Authority (TVA)

Planning the Transition to CIP Version 5

TVA had a substation project already underway that focused on making enhancements to their CIP Version 3 compliance posture. Upon industry approval of CIP Version 5, TVA reassessed the project scope to ensure changes were compliant with CIP Version 5. The project was still in the planning phase, so making the shift to CIP Version 5 was relatively easy. TVA utilized the same resources for the revised scope. For TVA, projects such as these typically need to be proposed at least 18 months in advance of beginning work, allowing time for the project to be included in the business planning process.

One benefit of the initial project was that TVA had already designed and built a substation test lab. It required approximately one year to design and set up. TVA's goal was to obtain an example of each type of field asset across all substations in scope, and it succeeded in outfitting the lab with most asset types.

TVA's typical project management process is very regimented with the functions of Planning, Design/Engineering, Construction, and Operations/Maintenance. TVA's organization structure is set up to parallel this process with further segmentation into "Power" and "Telecommunications." For transmission substations entering into the CIP Version 5 program, equipment and processes will impact both power and telecommunications equipment. This made assigning responsibilities very challenging. To address these issues, TVA made two changes. They identified and staffed a new position, the CIP V5 Program Manager for Transmission, who is responsible for identifying any "seams" issues between business functions and reporting status to senior executives. TVA also set up a steering committee consisting of the department heads of each affected department. The CIP Version 5 Program Manager brings forward any seams-related challenges for the steering committee's guidance.

Designing Security Solutions

Telecommunications Engineering had the lead on developing the solution for substations. They engaged resources (power engineering, power and telecommunications planning, and information technology) to develop a standard format for documenting a baseline configuration for each type of device found at a substation. This document contains the firmware/software revision, ports and services required, patches that have been applied, and password capability for each device type. Anytime a change is made to one of these items, a new document is generated for that device. Developing each baseline was time consuming. Vendor documentation was not always readily available for older devices, but in most cases vendors were able to supply the information upon request.

Prior to the Implementation Study, TVA had been working on a methodology to identify BES Cyber Assets and BES Cyber Systems. TVA found that a bottom-up approach to asset functional review worked well for substations, and an application review by platform worked well for control centers. TVA found these two separate methodologies to be appropriate.

TVA performed weekly meetings to review the schedule and identify any hard spots; the company set aside two weeks at the end of the project to conduct a review of the solutions, compliance evidence, etc. This was helpful for identifying enhancements required for procedure development and evidence needed for each requirement.

Implementing Security Solutions

TVA also recognized that the transition to CIP Version 5 for their substations would impact field staff processes. Due to the limited scope of the Implementation Study, TVA has not yet determined the full impact on staffing or developed specific strategies to be addressed. However, TVA did identify a few unforeseen issues. The level of effort required to review and update the tables and forms within TVA's work management system to manage assets and systems in accordance of CIP Version 5, and the culling of the information to populate those fields, was much more labor intensive than expected. TVA's work management system serves the entire company. Changes to it require significant review and coordination, and gathering this information often requires field verification prior to final documentation.

TVA's substation included in the Implementation Study was a 161 kV substation, a low impact rating facility mocked up to be medium impact rating with external routable communications. TVA has not yet implemented a solution at a 500 kV site and has not yet determined the overall resource requirements needed to transition to CIP Version 5 at this medium impact rating facility.

The Control Center portion of the Implementation Study took advantage of many of the existing processes that were developed for CIP Version 3 compliance as the starting point for CIP Version 5. One of the most significant changes is related to CIP-002-5 and the shift to identifying BES Cyber Systems. This took considerably more time than originally anticipated. The personnel who work in the Control Center are well-experienced with security and compliance for CIP Version 3, so the transition to CIP Version 5 for this group will have minimal impact to the way they routinely conduct business.

Southern Company

Planning the Transition to CIP Version 5

One aspect of Southern's overall compliance program for NERC CIP was the creation of a NERC CIP Governance Team. This governance structure supports a consistent philosophy that accommodates both system and business unit perspectives, creates an effective environment for sharing best practices and auditing tested ideas, engages personnel responsible for the required daily activities, and brings compliance knowledge closer to those responsible personnel. This approach recognizes the evolving nature of cyber legislation and educates a much broader range of employees on the regulatory requirements. By incorporating expertise from multiple business areas, the end product is a more collaborative effort that accounts for the real-life practices at the core of Southern's business. This has been an extremely important concept as the CIP standards expand into new areas of the business where the field forces will be responsible for many of the daily activities.

The governance team is made up of approximately 100 employees from the different business units across the system. These employees ensure the varying business needs are considered as the team creates the CIP

procedures and develops acceptable compliance practices. The major areas of the governance team are highlighted below:

- Executive Sponsors – the NERC CIP Senior Manager and an Executive Advisory Committee
- Policy Development – a CIP Advisory Team and six functional teams (e.g., Access Control, Information Protection) made up of representatives from business units across the system (primarily Control Centers, Substations, Generation, Information Technology, Security, and Compliance). Each business unit has at least two team members on each of the six functional teams.
- Implementation Teams – each business unit noted above has a corresponding team that ensures the procedures are implemented within their respective areas.

This team also creates system-wide procedures that apply to all functions and are coordinated and implemented across Southern Company. These system-wide procedures will be documented in a NERC CIP Manual. This manual will define common, repeatable, and inclusive processes to meet the standards, set the evidentiary requirement using the measures noted in the standards, and account for all applicable device types.

Southern originally dedicated its own "Core Study Team" to the Implementation Study. It consisted of several individuals already performing certain CIP-related duties that would be pivotal to the overall pilot activities and provide consistency to the different business units. The resources needed to perform the specific activities associated with categorization, analysis, and documentation for each of the different areas required many additional employees and are discussed in more detail below. The Core Study Team was comprised of:

- Generation/Transmission IT employees – 2 employees
- Technical Services Instrumentation and Controls (Generation) – 2 employees
- Operations Compliance – 3 employees. Compliance had the lead role for managing Southern's contribution to the Implementation Study.
- Substations – 1 employee
- Control Centers – 2 employees

Approval for each of the employees dedicated to the Core Study Team was discussed and approved by that business unit's management.

Designing Security Solutions

To address the requirements for CIP-002-5, each business unit created a draft procedure for categorizing the cyber assets within their respective facilities. The categorization process included both a word document that described the thought process and an accompanying flow chart to help illustrate the process. These documents were updated several times throughout the Implementation Study period to incorporate lessons learned. The generation categorization flow chart has been included in a NERC Lessons learned document regarding generation segmentation.

For generation, the goals of being a study participant were:

- Develop a methodology for CIP-002-5 categorization
- Identify BES Cyber Assets and BES Cyber Systems
- Create an evidence package for documentation
- Create a how-to package that was scalable and repeatable for plants greater than 1500 MW

- Pilot this philosophy at large generating plants

The resulting how-to package contains:

- Categorization Procedure for CIP-002-5 for Generation (includes a 2-page flow chart)
- Cyber Asset inventory
- Shared component list and engineering assessments
- Shared BES Cyber System list and engineering assessments
- External interface connectivity diagrams
- Firewall rule documentation
- Inventory, analysis, and documentation checklist

Implementing Security Solutions

Performing the categorization and documentation process at the plant required both plant resources and the Core Study Team. To start the process, the Core Study Team met with plant management to give an overview of the CIP standards, explain how the standards impacted their plant, and discuss the Cyber Asset inventory, categorization, and documentation process. At one pilot plant location, the Instrumentation and Control team leader led the Cyber Asset inventory, categorization, and documentation process with a core team of eight to twelve other plant employees. These eight to twelve employees relied on many additional plant subject matter experts to update the inventory and perform the required engineering assessments to determine the proper impact rating. This effort took several months for the combined Core Study Team and plant teams to complete. A major lesson learned from a generating plant categorization perspective is that the process takes several months, is resource intensive, and has a steep learning curve for the plant employees to understand the CIP standards.

Substations focused on the categorization process and high-level Physical Security Perimeter and Electronic Security Perimeter concepts. Most of the individuals who performed these tasks for substations were already members of the NERC CIP Governance Team, but many of these individuals also have other non-CIP-related duties. A team of eight to ten employees from Substations, Security/Facilities, and Compliance, in addition to the Core Study Team, created the proposed documentation for the Implementation Study deliverables. Similar to the plant experience, the team of eight to ten employees also had to engage multiple substations subject matter experts from various departments to assist in the inventory, categorization, and documentation process. A similar lesson learned was also evident from a substation perspective in that the categorization process took more time than originally thought, required more resources, and had a steep learning curve for the substation employees to gain an understanding of the CIP standards.

Both Generation and Substations relied on in-house resources for Implementation Study participation. The Control Center team relied on both in-house resources and an outside consultant for the creation of the categorization process and gap analysis from CIP Version 3 to CIP Version 5.

All business units are researching tools to assist with CIP Version 5 compliance. In addition to several in-house products, supplemental software solutions include:

- Patch management products for both Substations and Control Centers for CIP-007-5
- A change management database and additional vendor products for Configuration Change Management/Monitoring for CIP-010-1
- A log management system for Event Monitoring for CIP-007-5

- An enterprise-wide access control system
- An evidence repository

With the ever-increasing complexity and overall expansion of the scope of the CIP requirements, these tools will complement the compliance program by increasing automation and overall tracking capabilities. For example, an enterprise-wide access control system will be better suited to manage the increase in the number of Physical Security Perimeters and more stringent time frames for revoking access to the CIP-access-controlled areas. Certain aspects of the access provisioning process can be automated within the tool, which will provide a more consistent approach across the multiple business units and decrease the administrative attention required for manual updates.

Change management policies and practices for each business unit are also being updated and formalized to transition to the new CIP Version 5 requirements. This was true not only for Control Centers, it also became another lesson learned as the CIP Version 5 scope extended into the Substations and Generation areas. While these areas had certain change management processes already in place, the increased level of detail and the number of new systems incorporated will require additional modifications. For example, one in-house application that is currently utilized to track inventories and maintenance must undergo several major enhancements to document the required changes.

As noted above, one challenge encountered during the Implementation Study is the steep learning curve associated with the CIP requirements for the Substation and Generation business units. Many of these resources had not been exposed to in-depth cybersecurity regulations in the past and had to reprioritize their existing work obligations to accommodate the new responsibilities. CIP Version 5 compliance will require resource additions for all business units, but at this time an exact number per business unit is unknown.

Westar Energy (Westar)

Planning the Transition to CIP Version 5

Westar's transition from CIP Version 3 to CIP Version 5 for purposes of the Implementation Study involved adding medium-impact generation and transmission assets. The majority of the Implementation Study was focused around the Generation and Transmission business units, as they have had little exposure to the CIP standards prior to CIP Version 5. Westar's Critical Asset substations in CIP Version 3 did not contain Critical Cyber Assets. Westar assembled a transition team to provide direction for the CIP Version 5 efforts required to implement the transition. The transition team was led by the NERC Compliance Group in the Regulatory Affairs Department and included over 20 resources from Generation, Substation, Protection and Control Engineering, IT Security, Physical Security, Communication, and EMS. The NERC CIP Manager acted as the project lead and was fully committed throughout the Implementation Study. Participation in the Implementation Study was approved by the company's FERC Executive Steering Committee. The transition team participated in planning, designing, and implementing security solutions throughout the project.

Designing Security Solutions

Westar's focus for the Implementation Study initially centered on validation and implementation of the BES Cyber System identification methodology. The Implementation Study also included a Physical Security Perimeter design at an in-scope generation station, development of a standardized security design at one in-scope transmission substation, and implementation of several technical solutions.

A sub-project of the Implementation Study involved determining if the BES Cyber Assets at the in-scope transmission substations would move from the current serially connected infrastructure to utilizing external

routable protocol. An engineering design firm was contracted to assist with this decision. In order to make the decision, the classification of the assets in addition to a standardized security and technical infrastructure design was created for both scenarios. Other factors taken into consideration were the cost to implement and maintain an Electronic Security Perimeter and Physical Security Perimeter, the cost to manage access at remote substations, and the advantages of accessing BES Cyber Assets remotely. The transmission business unit made the decision to continue utilizing the serially connected infrastructure through the near future but will re-evaluate this decision periodically.

The transition team also provided the guidance and direction for design aspects of the CIP Version 5 transition efforts. Considerable time and effort were dedicated to completing the CIP-002-5 BES Cyber System identification process at the newly identified assets. The transition team worked closely with the Generation and Transmission business units to inventory all cyber assets at the applicable locations and classify them accordingly. A project manager was contracted to oversee the technical solution implementation to automate processes for logging, password management, and change management.

Implementing Security Solutions

The transition team addressed implementation challenges as they arose. Implementation of the technical solutions has presented several challenges, including vendor communication and expectations. The standardized substation security design included several critical decision points (e.g., use of externally routable protocol) that needed to be made prior to finalization of the design. The subject matter experts for the Generation and Transmission business units had previously not been impacted by the CIP Version 3 standards and therefore had limited knowledge of the CIP standards. A significant amount of time and effort was and continues to be focused on increasing the knowledge of the CIP standards requirements. It was also clear through interaction with the engineering design firm that CIP Version 5 understanding and knowledge in the vendor community has yet to evolve. Challenges continue to arise, and Westar addresses these through internal discussions and interaction with other study participants, as well as NERC and SPP. Implementation of solutions for the transition continues, including drafting processes and procedures for these new technical tools. Resource needs continue to be evaluated and adjusted as necessary. It is anticipated that additional resources will be required in Field Operations and potentially IT Security.

Dayton Power & Light (DP&L)

Planning the Transition to CIP Version 5

DP&L chose to include all the CIP Version 5 standards within the scope of their Implementation Study. In general, they leveraged the expertise of existing CIP Version 3 subject matter experts to review the changes needed to transition to CIP Version 5.

Designing Security Solutions

Within the scope of the Implementation Study, DP&L revised their CIP Version 3 policies and procedures to meet the CIP Version 5 standards. They found a large portion of these policies and procedures could be reused for CIP Version 5, as follows:

- CIP-003 – 90%
- CIP-004 – 80 to 90%
- CIP-005 – 85%
- CIP-006 – 85% (review required for newly identified assets)
- CIP-007 – 80%

- CIP-008 – 95%
- CIP-009 – 90% (review required for newly identified assets)
- CIP-010 – 50%
- CIP-011 – 50%

Implementing Security Solutions

DP&L found it important to involve subject matter experts early and often. Areas of particular interest within certain standards included:

- **CIP-002-5 BES Cyber System Categorization:** A large portion of DP&L's effort focused on CIP-002-5 BES Cyber System Categorization as it applies to their generation facilities and substations. DP&L found it important to focus efforts first on identifying high, medium, and low BES Cyber Assets before getting too far in developing security solutions to meet the remainder of the CIP Version 5 standards. They found it was important to directly involve engineering, generation, and substation personnel. Their CIP Version 3 Risk-Based Assessment Methodology proved to be a good starting point for developing their Cyber Asset list. After developing their Cyber Asset lists, they then grouped them into Cyber Systems, but only if it was beneficial.
- **CIP-005-5 Electronic Security Perimeters:** DP&L found this requirement to be clear and was able to use many of the same processes related to managing access in place for CIP Version 3. Intrusion prevention and detection processes will need to be implemented at their medium- and high-impact rating Electronic Security Perimeters.
- **CIP-006-5 Physical Security:** Processes related to managing Physical Security Perimeters at substations and generating stations need to be automated as much as possible to maintain compliance. Cameras and card readers may require that employee representatives be involved to address possible collective agreement implications.
- **CIP-007-5 Systems Security Management:** DP&L found this requirement to be clear and was able to use many of the same processes in place for CIP Version 3. They found that automation is needed to cope with the accelerated schedules required to manage processes related to patch management and security event monitoring.
- **CIP-010-1 Configuration Change Management and Vulnerability Assessments:** DP&L learned that change procedures at substations needed to be different than those employed in other environments.

MidAmerican Energy (MidAmerican)

Planning the Transition to CIP Version 5

MidAmerican's focus for the Implementation Study was to fully implement and achieve compliance with CIP Version 5 by March 10, 2014, for:

- All requirements in standards CIP-002-5, CIP-005-5, CIP-006-5, CIP-007-5, and CIP-010-1
- Transmission and generation control centers and backup control centers
- Selected substations. Of note, the selected substations:
  - were compliant with CIP Version 3 standards CIP-002-3 through CIP-009-3
  - were not accessible by external routable protocol. One was dial-up accessible. One had internal routable protocol.

- Generating units. Implementation of CIP-002-5 required analysis of all generation, including a group of generating units at a single plant location that exceeded 1500 MW.

MidAmerican had extensive experience maintaining compliance with the CIP standards for CIP Versions 1 through 3 for transmission and generation control centers, substations and generating units. Prior to the Implementation Study, MidAmerican had already completed:

- Analysis of CIP Version 4 Attachment 1 to identify Critical Assets and Critical Cyber Assets.
- Transition for the differences in Critical Assets and Critical Cyber Assets between the CIP Version 3 risk-based assessment methodology and CIP Version 4's Attachment 1.

MidAmerican accessed CIP Version 3 in-scope substations with dial-up, not with external routable protocol.

Designing Security Solutions

Overall, subject matter experts were confident technically. Subject matter experts had:

- Extensive experience from CIP Version 3 on these cyber assets.
- Extensive experience with non-CIP, enterprise-wide cyber and physical security controls that correlated to some of the revisions to CIP controls.
- Questions about evidence for and compliance of their technical solutions when evaluating technical solution options. Their questions were not on how to technically achieve a reliable security result.

MidAmerican did not have technical experience complying with CIP Version 3 in substations with external routable connections. MidAmerican's CIP Version 3 in-scope substations are dial-up accessible. MidAmerican decided to continue dial-up accessibility at CIP in-scope substations at least until after the April 1, 2016, enforcement date[8] for CIP Version 5.

Over 70 percent of MidAmerican's approximately 90 successes and challenges were related to compliance and evidence as discussed during the March 10–14 on-site review.

Themes for compliance confidence for programs including design strategies and decision criteria include:

- CIP-002-5 application of decision criteria to determine if:
  - a device is a Cyber Asset.
  - a Cyber Asset is a BES Cyber Asset.
  - a Cyber Asset is shared.
  - a BES Cyber Asset is accessible by External Routable Connectivity (especially in substations).
- CIP-005-5 Intermediate System and encryption design
- CIP-005-5 Electronic Security Perimeter designs, especially:
  - in substations
  - for changes in CIP Version 5 that may be applicable from the CIP Version 3 Compliance Analysis Report CIP-005
  - for the new definition for Electronic Access Point

[8] The enforcement date for responsible entities in Canada may differ.

- CIP-006-5 program strategy for:
  - "operational or procedural controls to restrict physical access"
  - "issue an alarm or alert … within 15 minutes of detection"
- CIP-007-5 security patch monitoring mitigation plan design, especially for Windows or other Cyber Assets with high volumes of security patches
- CIP-010-1 vulnerability assessment scope strategy and design

Themes related to compliance evidence included:

- Evidence for audit requests for information – Revisions are needed.
- Evidence for a null – What evidence is sufficient to prove a null (e.g., no shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW).
- Evidence an asset or a Cyber Asset wasn't left out – How much documentation is required for assets and Cyber Assets that were not included in scope?
- Evidence cannot always be system generated – When and what evidence is needed? For example:
  - Does the responsible entity have to photograph a display on a relay?
  - When will attestations be sufficient?
- Evidence scale – How much evidence is enough? Some controls involve extensive detailed data that exists real time but would have to be manually copied and saved for historical compliance monitoring, for example:
  - CIP-010-1 configuration baseline changes and testing.
  - CIP-007-5 security patch assessments and mitigation plans.
- Evidence for device capability or device maximum – How much documentation is required? Device capability and device maximum are solutions to undue administrative burden of TFEs in CIP Versions 1 through 3. The documentation burden for CIP Version 5 needs to be less than the documentation burden for CIP Version 3 TFEs.

Implementing Security Solutions

Key implementation results for standards CIP-002-5, CIP-005-5, CIP-006-5, CIP-007-5, and CIP-010-1 for the assets in scope follow.

Identified CIP Version 5 High and Medium BES Cyber Systems and Low Assets

- Control Centers – did not find any additional Cyber Assets.
- Substations – identified approximately a dozen new Cyber Assets that are in-scope for CIP Version 5 at each substation in the Implementation Study that were not in scope at that substation for CIP Version 3, due to CIP-002-3 connectivity exclusions.
- Generation – utilized experience with CIP Version 3 to document that the single generating plant location with an aggregate of 1500 MW did not have any shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW.
- Low assets – preliminarily identified the assets with low-impact BES Cyber Systems.

- BES Cyber Systems – determined not to group. To date for MidAmerican, each BES Cyber System is one BES Cyber Asset.

Implemented Controls

- Implemented revisions to controls for the differences between CIP Version 3 and CIP Version 5 requirements.
- Implemented the new CIP Version 5 requirements, including, for example:
  - Installing a CIP Version 5 Intermediate System.
  - Starting baseline monitoring per prescriptiveness of CIP-010-5 for high impact.
- Implemented more automation, especially for prescriptive CIP-010-1 configuration management.

Revised Documentation

- Revised all CIP Version 3 documentation.
- Identified a significant reduction in TFEs required for these standards for these assets for CIP Version 5 TFEs due to CIP Version 5 device capability and device maximum language.

For the assets and requirements in the scope of the Implementation Study, and considering MidAmerican's starting point, MidAmerican plans to continue to comply with CIP Version 3 while implementing CIP Version 5. MidAmerican:

- Did not identify situations where complying with CIP Version 3 caused noncompliance with CIP Version 5.
- Identified two situations where implementation of CIP Version 5 could possibly cause noncompliance with CIP Version 3.
  - MidAmerican will use CIP Version 5 – CIP Exceptional Circumstances after April 1, 2016.
  - CIP-005-5 R2.1 and R2.3 Interactive Remote Access: R2.1 requires an Intermediate System to initiate Interactive Remote Access. R2.3 requires multi-factor authentication for all Interactive Remote Access. CIP-005-3 R2.4 requires "strong procedural or technical controls at the access points" for "external interactive access into the Electronic Security Perimeter." MidAmerican is authenticating at both until April 1, 2016.

Impact on Resources

MidAmerican assessed the effort required to implement each requirement part for CIP Version 5 standards CIP-002-5, CIP-005-5, CIP-006-5, CIP-007-5, and CIP-010-1 at the start of the Implementation Study in 2013 and again in March 2014.

MidAmerican's initial assessments were generally on target for whether the CIP Version 5 requirement would take more, less, or about the same ongoing work as CIP Version 3, or if it was a new requirement.

Table 6: MidAmerican Impact on Resources

CIP Version 5 Ongoing Work Impact on Resources	Approximate % of Requirement Parts Standards 002, 005, 006, 007, 010
More than CIP Version 3	50
About the same as CIP Version 3	45
Less than CIP Version 3	5

It is important to view the information in Table 6 in context by keeping the following concepts in mind:

- MidAmerican's CIP Version 3 program in place was extensive.
- MidAmerican personnel have extensive experience from implementing and maintaining compliance with CIP standards CIP-002 through CIP-009 for CIP Versions 1 through 3 for transmission and generation control centers, substations, and generating units.
- MidAmerican's assessments were for ongoing effort, not the extensive one-time effort to transition from CIP Version 3 to CIP Version 5. MidAmerican anticipated that significant revisions were possible in the CIP standards following CIP Version 1 and developed a design strategy to address this. This design strategy greatly helped in revising the program. However, it was still a significant amount of work.
- Assessments of "more than CIP Version 3" have a wide variation in how much "more." Some requirement parts are a little more, but many require a lot more ongoing work.

In summary, as an entity with an extensive CIP Version 3 program, MidAmerican identified:

- Significant increased resource impacts for ongoing work for CIP Version 5.
- Significant resource impacts to transition to CIP Version 5.

MidAmerican used very minimal external resources to augment internal resources for transition.

Lessons Learned

Throughout the Implementation Study, study participants identified potential issues and asked NERC and Regional Entity staff to clarify certain aspects of the CIP Version 5 standards, or confirm that their approach was consistent with good security practices and compliance expectations. In addition, NERC invited all other responsible entities not involved in the Implementation Study to submit questions via a link on the public website. By the end of the formal portion of the Implementation Study on June 30, 2014, approximately 20 lessons learned and many more FAQ topics were identified by study participants and the Regional Entities. While the documents being developed to address these topics are intended to represent a comprehensive set of guidance that will help all responsible entities transition to CIP Version 5, new documents will continue to be developed throughout the remainder of the transition period as additional questions arise.

- **FAQs:** This document, in the form of a table sorted by each of the CIP Version 5 standards, addresses questions raised by study participants that could be answered in the space of a paragraph or two. This document is updated periodically and is available on the NERC website.
- **Lessons Learned Documents.** A series of lessons learned documents are being developed throughout the Transition Program to address questions requiring more detailed analysis and discussion. These documents are also available on the NERC website.

Lessons learned and FAQ reference documents are being developed in collaboration with an advisory group consisting of NERC, Regional Entities, and study participants, and are vetted with stakeholders.

Summary of Lessons Learned and FAQs

Table 7 provides a list of the 23 key questions identified during the Implementation Study and whether they are being addressed as an FAQ or lesson learned. Note that all of the questions identified by study participants have been or are being addressed through extensive stakeholder review.

Almost half of these questions relate to CIP-002-5.1 - BES Cyber System Categorization. This underscores an important first step when transitioning to CIP Version 5: responsible entities need to understand the scope of the CIP Version 5 standards and how they apply to the BES Cyber Systems they own or operate.

Table 7: Summary of Key Lessons Learned and FAQs

CIP Version 5 Reference	Description	Degree of Interest by Study Participants	Lesson Learned or FAQ
1. CIP-002-5 R1: Impact rating of generation resources (generation segmentation)	What options are available to categorize the impact rating of BES Cyber Assets at plants greater than 1500 MW?	High	Lesson Learned
2. CIP-002-5 R1: Relay protection in substations with different impact ratings (i.e., far-end relay/transfer trip)	How should the impact rating of line protection relays at each end of a transmission line connecting two substations be determined?	High	Lesson Learned
3. CIP-002-5 R1: Programmable electronic devices	What are some practical examples for what is or is not a programmable electronic device?	High	Lesson Learned
4. CIP-002-5 R1: BES impact of transmission scheduling systems	Should transmission scheduling systems be considered medium- or high-impact rating BES Cyber Systems?	Moderate	Lesson Learned
5. CIP-002-5 R1: Identifying BES Cyber Systems and BES Cyber Assets	What are some practical approaches to identify BES Cyber Systems and BES Cyber Assets?	Moderate	Lesson Learned
6. CIP-002-5 R1: Distributed BES Cyber Assets at generating plants and substations	Are instrumentation devices such as sensors, actuators, and controllers considered to be programmable electronic devices? If so, what methods would be appropriate to secure them from a compliance perspective?	Moderate	Lesson Learned
7. CIP-002-5 R1: Grouping BES Cyber Assets	What are the advantages of grouping BES Cyber Assets into BES Cyber Systems, and how can this help demonstrate compliance?	Moderate	Lesson Learned

Table 7: Summary of Key Lessons Learned and FAQs			
CIP Version 5 Reference	**Description**	**Degree of Interest by Study Participants**	**Lesson Learned or FAQ**
8. CIP-002-5 R1: Shared equipment at a substation	What issues need to be addressed related to substations that are shared by different entities (e.g., identifying ownership, compliance responsibilities, emergency management, physical access controls)?	Moderate	Lesson Learned
9. CIP-002-5 R1: Applicability of Control Centers to Transmission Operators (TOP) and Transmission Owners (TO)	How would CIP-002-5 Attachment 1 criterion 2.12 apply to medium-impact Control Centers if the functional obligations are performed by the TO on behalf of the TOP?	Moderate	Lesson Learned
10. CIP-002-5 R1: Generation interconnection points	Clarify the terms "generation interconnection point," "generation interconnection Facility," and "collector bus" for the purposes of applying CIP-002-5 Attachment 1 impact rating criteria 2.1 and 2.2.	Moderate	Lesson Learned
11. CIP-003-5 R2: Medium-impact rating, non-routable, no dial-up access Cyber Assets	What is the complete set of CIP Version 5 requirements that apply to BES Cyber Systems without routable or dial-up access?	Moderate	Lesson Learned
12. CIP-005-5 R1: Virtual server and network environments	How can virtual environments that physically reside inside and outside an Electronic Security Perimeter be secured and considered compliant?	High	Lesson Learned
13. CIP-002-5 R1.2: Serial devices with External Routable Connectivity	Are serial based systems with local serial connections considered to have External Routable Connectivity if they are remotely accessible via routable protocol?	Moderate	Lesson Learned
14. CIP-005-5 R1.5: Intrusion detection systems	Discuss the merits of installing intrusion detection systems outside the Electronic Security Perimeter.	Moderate	Lesson Learned
15. CIP-005-5 R2: Interactive remote access	What needs to be considered to determine if an electronic connection is Interactive Remote Access?	Moderate	Lesson Learned
16. CIP-005-4: Electronic Access Monitoring and Control Systems	How should mixed-trust authentication processes (e.g., corporate active directory systems that authenticate access to an energy management system) be managed to ensure compliance?	Moderate	Lesson Learned

Table 7: Summary of Key Lessons Learned and FAQs			
CIP Version 5 Reference	**Description**	**Degree of Interest by Study Participants**	**Lesson Learned or FAQ**
17. CIP-006-5 R1: Multiple physical access controls	Discuss options for using two or more physical access controls for high-impact BES Cyber System Physical Security Perimeters.	Moderate	FAQ
18. CIP-007-5 R1: Protecting physical ports	How can tamper tape be used to protect physical ports to comply with this requirement?	Moderate	FAQ
19. CIP-007-5 R2: Identifying sources for patch management	How should the appropriate sources for obtaining security patches be determined and documented?	Moderate	FAQ
20. CIP-007-5 R3.2: Mitigate the threat of detected malicious code	Clarify if entities are required to mitigate the threat of detected malicious code regardless of the methods they choose to deter, detect, or prevent malicious code.	Moderate	FAQ
21. CIP-010-2 R1: Change management	What are some methods to automate the change and configuration management process for substation equipment?	Moderate	Lesson Learned
22. CIP-010-2 R3: Vulnerability testing of Physical Access Control Systems	How should active vulnerability scans be managed for Physical Access Control Systems given their sensitivity to denial of service attacks?	Moderate	FAQ
23. CIP-010-2 R4: Protection of transient devices	What are the protection requirements for transient devices used for maintenance activities?	Moderate	FAQ

Conclusion and Next Steps

The Implementation Study succeeded in supporting the goals of the CIP Version 5 Transition Program. Study participants and their Regional Entities appreciated the opportunity to be involved in the Implementation Study, and through their active involvement were able to substantially increase their confidence that they will be ready to implement the CIP Version 5 standards effectively on or before the effective date. Throughout the course of the Implementation Study, NERC, Regional Entities, and study participants developed many lessons learned and answers to FAQs. Following broad stakeholder review, NERC will continue to post these reference documents on the public NERC website to be available to all stakeholders. NERC anticipates that by sharing the results of this Implementation Study, and through continued engagement involving NERC, the Regional Entities, and all responsible entities, the industry will learn from the experiences of the study participants and increase their own confidence in successfully implementing CIP Version 5.

The following describes the extent to which each of the goals of the Implementation Study has been addressed and proposes next steps to continue the work begun with the Implementation Study.

Goal 1 – Implementation

Improve industry's understanding of the technical security challenges that need to be addressed in order to comply with the CIP Version 5 standards, with emphasis on the material differences between Version 3 and Version 5.

- Responsible entities will confirm their understanding of new or different technical security solutions needed to comply with the CIP Version 5 standards.
- Responsible entities will understand how to comply with CIP Version 5 in situations where a technical solution is not feasible.

Goal 1 Accomplishments

Key technical issues: Study participants identified, discussed, and addressed key technical issues through periodic conference calls and in-person meetings with Regional Entities and NERC. Issues included:

- Clarifying new CIP Version 5 requirements. While the majority of the CIP Version 5 requirements build on CIP Version 3 of the CIP standards, participants benefitted from discussions that clarified their understanding of certain requirements that were new in CIP Version 5.
- Applying the requirements to their own situation. Participants benefitted from one-on-one discussions that clarified their understanding of certain requirements as they applied to their own specific situation and local circumstances.

Sharing security solutions: Study participants shared approaches and solutions with each other using the secure portal, and during in-person meetings.

Lessons Learned and FAQs: Participants identified the need for approximately 20 lessons learned and many more FAQs to be shared with all stakeholders. Each of the reference documents undergo a stakeholder review process, as discussed above.

Recommendation 1: During Q4 2014, NERC, in collaboration with stakeholders, expects to implement a process to continue to develop lessons learned and FAQ reference documents, as identified by responsible entities, which will include a mechanism for obtaining broad industry stakeholder review, and results in the posting of these documents on the NERC website once completed.

Recommendation 2: Through Q3 2015, NERC and the Regional Entities will follow up with study participants to review their experience with their continued implementation of CIP Version 5, particularly those requirements that were outside the scope of the study to determine if these areas require additional attention and guidance (i.e., CIP-003-5, CIP-004-5, CIP-008-5, CIP-009-5, CIP-011-1).

Goal 2 – Compliance and Enforcement Expectations

Provide industry with a clear path and approach to transition from CIP Version 3 to CIP Version 5 that includes expectations for compliance and enforcement.

- Responsible entities will know what evidence they need to retain to demonstrate compliance with the CIP Version 5 standards.
- Regional Entities will have a consistent view of how to monitor compliance of Responsible entities.

Goal 2 Accomplishments

Key compliance and enforcement issues. Identified, discussed, and addressed key compliance and enforcement issues raised by study participants through periodic conference calls and in-person meetings involving study participants, Regional Entities, and NERC.

Sharing security solutions. Regional Entities participated collaboratively with study participants and developed consistent approaches to what evidence is needed to demonstrate compliance.

Established advisory group. NERC established an advisory group composed of compliance and enforcement staff from NERC, Regional Entities, study participants, and other industry stakeholders to proactively identify and address CIP Version 5 implementation issues in a consistent manner.

Recommendation 3: By the end of Q2 2015, NERC expects to review, revise, or retire CIP Version 3 documents, as applicable, for consistency with CIP Version 5. These documents include, for example, Appendix 4D of the NERC Rules of Procedure related to Technical Feasibility Exceptions, Compliance Analysis Reports, Compliance Application Notices, CIP Interpretations, and mechanisms to retire CIP Version 3 Technical Feasibility Exceptions.

Goal 3 – Resource Requirements

Provide industry and Regional Entities an understanding of the technical- and compliance-related resources and efforts needed to transition and manage compliance with the CIP Version 5 standards.

- Responsible entities will understand what resources they need to transition to and comply with the CIP Version 5 standards.
- Regional Entities will understand what resources they need to monitor responsible entities' compliance with the CIP Version 5 standards.

Goal 3 Accomplishments

Understanding resource requirements. Study participants assigned the necessary resources on a pilot basis, allowing them to project resource requirements needed for full implementation of CIP Version 5.

Recommendation 4: By the end of Q1 2015, NERC and the Regional Entities expect to develop a plan for and begin conducting additional CIP Version 5 transition outreach efforts as well as provide sample CIP Version 5 implementation reviews to as many responsible entities as possible. The intent of these outreach efforts is to provide all responsible entities with opportunities to learn from the experiences of study participants and include a mechanism to identify new or unresolved issues for NERC and the Regional Entities to develop a coordinated response. The outreach will leverage existing industry stakeholder mechanisms and media such as webinars, recorded presentations, web postings, and in-person sessions.

Appendix A – Implementation Study Team

Table 8: Implementation Study Team	
Core Team	**Role**
Steve Noess	Program Director
Matt Blizard	Program Sponsor
Tobias Whitney	Program Manager
Felek Abbas Scott Mix	Core Team Liaison
Carter Edge	Regional Leadership Liaison
Nicholas Santora	CIP Standards SME
Tom Hofstetter	CIP Compliance SME
Stuart Brindley	Project Management Support
Regional Entity Study Leads	**Region**
Jim Dodge Barry Pagel Chris Holmquest	FRCC
Joe Gay	MRO
John Muir	NPCC
Tony Purgar Bob Yates	RFC
Chip Lees Lonnie Ratliff	SERC
Kevin Perry	SPP-RE
Bill Beaver	TRE
Brent Castagnetto Joe Baugh	WECC
Study Participant Lead	**Company Name**
Jeff Fuller Chip Wenz Hertzel Shamash	Dayton Power & Light
Annette Johnston	MidAmerican Energy
Tim Kelley Scott Saunders	Sacramento Municipal Utility District
Helen Nalley Jay Cribb Rebecca Ann Martin	Southern Company
Cynthia Rutledge	Tennessee Valley Authority
Bo Jones Megan Wagner Eric Ervin	Westar Energy