Deloitte.

Issue 3, April 2013

Power & Utilities Spotlight

Avoid a CIPwreck by Preparing for NERC CIP Version 5

In This Issue:

The Bottom Line

- *What is CIP?* — To maintain and protect U.S. infrastructure and operation, critical infrastructure protection (CIP) programs have been established for each major industry sector, including power and utilities. These programs standardize the description of critical infrastructure, allowing for consistent monitoring of, and preparation for, potential events that might disable vital assets in a particular industry sector.
- *Current state of NERC CIP requirements* — The CIP program of the North American Electric Reliability Corporation (NERC), among other things, includes nine separate standards, eight of which address cybersecurity-related matters. Over the past several years, NERC and the industry have continued to refine the CIP program. While the electric power industry is currently operating under NERC CIP Version 3, CIP Version 4 has been approved by the Federal Energy Regulatory Commission (FERC) and will become enforceable on April 1, 2014.
- *Future state of NERC CIP requirements* — To meet the requirements outlined by FERC Order No. 706, the CIP standards development team proposed NERC CIP Version 5, which resulted in a rewrite of the overall CIP program. Version 5, which includes 11 standards, would introduce new definitions and concepts yet build on earlier versions of the CIP program. While Version 5 has been approved by the NERC board of trustees, it has not yet been approved by FERC.
- *Call for action* — While it has been costly and burdensome for companies to comply with Version 3 and prepare to comply with Version 4, addressing the Version 5 requirements may prove even more difficult. Further, companies may need to consider how to incorporate the NERC CIP compliance requirements into a comprehensive organization-wide program.

While it has been costly and burdensome for companies to comply with Version 3 and prepare to comply with Version 4, addressing the Version 5 requirements may prove even more difficult.

Beyond the Bottom Line

This *Power & Utilities Spotlight* discusses many aspects of CIP, including (1) the overall initiatives in place to protect our electricity infrastructure, (2) understanding the future NERC CIP requirements, and (3) the impact of the requirements on businesses.

Further, this publication contains the following two appendixes:

- Appendix A — Evolution of Critical Infrastructure Protection.
- Appendix B — NERC Version 5 CIP Standards.

Protecting America's Critical Electricity Infrastructure

In today's global reality, a country's infrastructure is under constant threat of disruption or destruction, both domestically and abroad; governments, therefore, continue to work toward safeguarding critical infrastructure.[1] The United States has had a CIP program in place since 1998 when it issued American Presidential Directive No. 63, "Critical Infrastructure Protection," which was updated in December 2003 by Homeland Security Presidential Directive No. 7, "Critical Infrastructure Identification, Prioritization, and Protection." In addition, the federal government has established a number of initiatives to help power and utilities companies protect their electricity infrastructure.

In today's global reality, a country's infrastructure is under constant threat of disruption or destruction, both domestically and abroad; governments, therefore, continue to work toward safeguarding critical infrastructure.

NERC Critical Infrastructure Protection

NERC is the electric reliability organization (ERO) certified by FERC to (1) develop and enforce reliability standards, (2) monitor the bulk power system in North America,[2] and (3) educate and train industry personnel. One of NERC's key areas of focus is cybersecurity resilience; in that respect, NERC has made a concerted effort to issue alerts, conduct research, provide training, seek industry collaboration, and provide desktop simulation scenarios to help the industry identify and protect against cybersecurity-related threats. As part of this program, NERC has developed CIP standards that detail specific compliance requirements to be implemented by "responsible entities."[3] In short, the NERC CIP compliance program and its related activities, including the CIP standards, help protect the power generation and transmission systems in North America. See Appendix A for background on the NERC CIP program and details on the current reporting requirements.

FERC Office of Energy Infrastructure Security

FERC created the Office of Energy Infrastructure Security (OEIS) in September 2012 to address cyber and physical threats to energy facilities under the FERC's jurisdiction. The OEIS:

- Develops recommendations.
- Assists and offers its expertise to other stakeholders (e.g., federal and state agencies, jurisdictional utilities, Congress).
- Collaborates with other agencies and utilities by participating in conferences, workshops, and classified briefings.
- Reaches out to private-sector owners, users, and operators of energy delivery systems.

Upon announcing the creation of the OEIS, FERC indicated that it would continue to work closely with NERC and that the OEIS's efforts would complement, but not replace, those of NERC.

[1] The U.S. Patriot Act of 2001 defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

[2] NERC oversees various regional reliability entities, including the interconnected power systems in the United States, Canada, and parts of Mexico.

[3] The term "responsible entities" is identified in the applicability section of the NERC CIP and constitutes individuals, groups, or organizations that are subject to the compliance criteria of the NERC CIP; such entities include (1) balancing authorities, (2) distribution providers, (3) generator operators, (4) generator owners, (5) interchange coordinators or interchange authorities, (6) reliability coordinators, (7) transmission operators, and (8) transmission owners.

Future Legislation and Pending Executive Order

Congress is currently debating legislation that, if finalized, would bolster the nation's cybersecurity protection. In the interim, on February 12, 2013, President Obama issued an executive order aimed at curtailing cyber threats to the nation's critical infrastructure, including the bulk electric system (BES). The executive order's requirements include (1) more timely sharing of cyber-threat-related information between U.S. government agencies and private-sector companies; (2) development of a formal cybersecurity framework[4] that will "include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks"; (3) establishment of a voluntary critical infrastructure cybersecurity program to support the adoption of the cybersecurity framework; and (4) identification of the critical infrastructure that is subject to the greatest risk.

Understanding Future Requirements

Although responsible entities are currently required to comply with Version 3 of the NERC CIP standards, Version 4 is due to become effective in 2014 and Version 5, which includes certain wholesale changes in the program, has been approved by the NERC board of trustees and is currently awaiting final FERC approval.

Expanding Requirements to Safeguard Our Infrastructure — NERC CIP Version 4

While NERC CIP Version 4 slightly refines the language from Version 3, its only significant changes are to CIP-002, "Cyber Security — Critical Cyber Asset Identification." Specifically, Version 4 includes criteria for identifying critical assets that replace the Version 3 risk-based assessment approach that is currently being applied by responsible entities. Because CIP Version 4 will result in a "bright line" for identifying critical assets, it most likely will result in more assets being subject to the NERC CIP requirements since certain critical assets that were previously not subject to the requirements would now be within the scope of these standards.

The electricity industry approved NERC CIP Version 4 on December 30, 2010, after which it was submitted to FERC, which approved it on April 19, 2012. Version 4 will become enforceable on April 1, 2014. While the final rule significantly amended CIP-002, it did not add any new substantive standards or additional guidance. However, the final rule did give NERC until March 31, 2013, to fully comply with the requirements outlined in Order 706. NERC met this requirement by submitting Version 5 to FERC. The final rule requires NERC to provide quarterly status reports to FERC on its CIP development efforts.

Next Generation of CIP Requirements on the Horizon — NERC CIP Version 5

Background

The NERC standards drafting team, in developing Version 5, addressed the 50-plus remaining issues from Order 706. NERC rewrote much of the CIP program in Version 5, resulting in what is considered an improved framework for critical asset cybersecurity protection. Although Version 5 includes the nine original standards, it modifies them significantly to reflect enhanced requirements; it also contains two new standards, CIP-010 and CIP-011. The full list of standards[5] in Version 5 is as follows:

- CIP-001-2a, "Sabotage Reporting."
- CIP-002-5, "Cyber Security — BES Cyber System Categorization."
- CIP-003-5, "Cyber Security — Security Management Controls."

[4] Under the presidential executive order, the cybersecurity framework development would be led by the National Institute of Standards and Technology. This framework would incorporate voluntary consensus standards and industry best practices when practical.

[5] As each CIP standard is updated, the last digit in the standard numbering scheme is changed to reflect the most current version of the standard (e.g., standard number CIP-005-5 represents the fact that this is the fifth version of this standard 5 whereas CIP-010-1 represents the first version of standard 10).

- CIP-004-5, “Cyber Security — Personnel & Training.”
- CIP-005-5, “Cyber Security — Electronic Security Perimeter(s).”
- CIP-006-5, “Cyber Security — Physical Security of BES Cyber Systems.”
- CIP-007-5, “Cyber Security — Systems Security Management.”
- CIP-008-5, “Cyber Security — Incident Reporting and Response Planning.”
- CIP-009-5, “Cyber Security — Recovery Plans for BES Cyber Systems.”
- CIP-010-1, “Cyber Security — Configuration Change Management and Vulnerability Assessments.”
- CIP-011-1, “Cyber Security — Information Protection.”

New Concepts and Definitions Introduced by Version 5

Version 5 introduces the concepts of the (1) BES, which represents the infrastructure that would be covered under the CIP standards, and (2) BES reliability operating services, which are the following nine services considered most crucial to the reliable operation of the BES:

- Dynamic response to BES conditions.
- Balancing and load generation.
- Controlling frequency.
- Controlling voltage.
- Managing constraints.
- Monitoring and control.
- Restoration of BES.
- Situational awareness.
- Interentity real-time coordination and communication.

Version 5 introduces the concepts of the (1) BES, which represents the infrastructure that would be covered under the CIP standards, and (2) BES reliability operating services.

The power generation plant, related BES cyber assets, and operating services are interrelated; understanding these interrelationships is critical to proper application of the CIP requirements and related standards.

Version 5 also eliminates the use of certain terms, such as “critical asset” and “critical cyber asset,” replacing them with new terms like “BES cyber asset,” “BES cyber system,” and “protected cyber asset.”[6] In addition, Version 5 changes the method of considering the critical infrastructure and systems that would affect a responsible party’s BES, as is discussed further in the Evaluating and Identifying the Critical Cyber Systems section below.

Further, Version 5 specifically defines external connectivity as “routable or dial-up data communication through an electronic access point between a BES cyber asset and a device external to the electronic security perimeter.” This clarification is important because certain Version 5 standards or parts of standards (e.g., CIP-005, certain provisions of CIP-007) only apply to BES cyber assets with external connectivity; thus, Version 5 limits the flexibility that entities had under Version 4 and Version 3 to remove cyber assets from the scope of the CIP as a result of a less specific definition of routable protocols.

Finally, Version 5 introduces the concept of defined physical boundary (DPB), replacing the physical security perimeter (PSP) concept from prior CIP versions. Under the previous PSP concept, a “six-wall border” approach was used for the physical perimeter and an entity was required to protect the critical physical asset by surrounding it with walls, ceilings, or other barriers. Under the DPB approach, responsible parties would be allowed to implement one or more layers of access control and thus would have greater flexibility to design the physical security of critical cyber assets.

[6] A protected cyber asset is a separate cyber asset that is directly connected to a BES cyber asset.

Evaluating and Identifying the Critical Cyber Systems

Unlike prior versions of the CIP, in which a responsible party would consider a critical asset as the starting point for applying the CIP standards, the Version 5 determination is based on the identification of the various BES cyber systems[7] within the responsible entity's BES. CIP-002-5 provides guidance on identifying these critical systems as well as bright-line criteria that a responsible entity can use in identifying and characterizing them within its BES.

Underlying the BES cyber systems are various BES cyber assets[8] that make up each system. After considering the nature of these BES cyber assets, responsible entities would categorize the impact of each system on the overall BES (i.e., whether the BES cyber system would have a high, medium, or low impact on the overall BES). This determination would be based on the scope of the entity's operations as well as on which level is the most efficient and secure. The identification and proper categorization of the responsible party's BES cyber systems is the foundation for determining how to apply the remainder of Version 5. When a BES cyber system is classified as "high impact," an entity would more significantly apply certain standards; however, when the impact is deemed "low," such standards could have minimal or no impact on the cyber system.

Organizational, Operational, and Procedural Controls to Mitigate Risk

While CIP-002-5 is the basis for identifying and characterizing the BES cyber systems that are subject to the CIP requirements, the remaining standards provide guidance on the "minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems." The nature and extent of the procedures that an entity would perform for each Cyber System depend on the system impact characterization that is determined under CIP-002-5. Version 5 includes certain changes that would make the standards more operational, allowing responsible parties to function more efficiently. See Appendix B for more information about the nature of the Version 5 standards and how they differ from the earlier versions.

In November 2012, after soliciting comments and circulating ballots, the electricity industry approved NERC CIP Version 5.

Status of CIP Version 5 and Next Steps

In November 2012, after soliciting comments and circulating ballots, the electricity industry approved NERC CIP Version 5. Shortly thereafter, on November 16, 2012, the NERC board of trustees approved (1) Version 5 of the CIP reliability standards, (2) its related implementation plan, and (3) the set of new and revised CIP-related terms. However, FERC has yet to formally approve this CIP version.

Upon FERC's final approval of Version 5, responsible entities will be subject to its requirements as of a specific effective date,[9] which will be determined at a later time. The implementation plan proposes the following regarding the effective date:

- Version 5 standards, with the exception of the second requirement of CIP-003-5, will become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
- The second requirement of CIP-003-5 will become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.

As of the date of this publication, FERC had not approved Version 5 of the CIP reliability standards. Further, Version 4, though approved, had not become effective (the effective date is April 1, 2014). Thus, responsible entities are still subject to the requirements of CIP Version 3.

[7] A BES cyber system is one or more BES cyber assets grouped together for the application of common cybersecurity controls. These are typically grouped together, logically or physically, to operate one or more BES reliability operating services.

[8] A BES cyber asset is a cyber asset that, if rendered unavailable, degraded, or misused, could within 15 minutes cause a disturbance to the BES and adversely affect one or more BES reliability operating services.

[9] Unlike entities in the United States, where CIP standards are not enforceable until they are approved by FERC, Canadian responsible entities are subject to the requirements upon approval by the NERC board of trustees. Therefore, it is expected that Version 5 will become effective in Canada in 2015.

Business Impact

Compliance Considerations

Because CIP standards continue to top the list of the most violated NERC standards, companies must try to understand and measure key CIP compliance issues. Management needs to consider whether its CIP compliance program results in an appropriate level of security protection and risk mitigation. In doing so, management also needs to consider whether all appropriate individuals understand the risk decisions being made and their role within that process. Further, management needs to consider the extent to which its security employs automation versus manual efforts. Finally, management needs to consider whether it is underinvesting or overinvesting in its CIP compliance program.

Given the increased federal and state regulatory requirements, including those of the NERC CIP, companies will need to assess both physical and cybersecurity-related protection. As a result of this assessment, a company may need to enhance or expand its security protection to mitigate the risks associated with its critical infrastructure. To further complicate matters, federal and state governments continue to expand on risk management requirements (e.g., the pending approval of NERC CIP Version 5, the presidential executive order, the Reliability Assurance Initiative[10]). Companies should therefore assess their capital and people needs in relation to current and proposed compliance programs, since the financial impact might be significant.

Because CIP standards continue to top the list of the most violated NERC standards, companies must try to understand and measure key CIP compliance issues.

Implementation Challenges

Power and utilities companies are also facing certain implementation challenges as they struggle to manage security risks attributable to increased cyber threats and growing regulatory pressures. These challenges can be grouped into six broad categories: (1) compliance vision and strategy, (2) compliance program automation, (3) technology challenges, (4) data management, (5) interpretation of the requirements, and (6) resources.

Compliance Vision and Strategy

Entities often do not have a well-defined vision or strategy to address risks related to their critical infrastructure. Rather than developing this vision or strategy, management of certain responsible entities may succumb to compliance pressure that leads these entities to create silos within their organization, potentially resulting in duplicate efforts and redundant spending. In addition, short-term focused strategies may adversely affect the organization's long-term compliance vision, potentially resulting in a lack of teaming and clear communication between IT and business compliance resources.

Compliance Program Automation

Entities may be adversely affected if they do not use automated systems within their compliance programs, which may impose limitations on their reporting, monitoring, evidence handling, and sustainable compliance through repeatable processes. For example, an entity may have manual procedures for managing key security processes such as (1) quarterly access reviews, (2) access authorizations, (3) compliance management, and (4) evidence collection. In such cases, the entity's monitoring, alerting, and reporting capabilities may be limited or the security monitoring may occur in a vacuum within each distinct area of responsible entity rather than in a comprehensive, organized manner throughout the entire organization. Most importantly, the lack of automation could result in the ineffectiveness of controls, since manual tasks are more prone to error and may not provide the requisite level of protection or compliance evidence.

[10] The Reliability Assurance Initiative is designed to identify (and implement when appropriate) changes that enhance the effectiveness of NERC's compliance and enforcement program and thus to avoid cascading events and the resulting major loss of load.

Technology Challenges

In the ever-changing security landscape, companies often acquire technology to meet short-term needs but neglect to consider their long-term goals. Rushed technology acquisitions often result in poorly functioning compliance support solutions or single-use solutions that do not have a meaningful impact on the organization as a whole. While there are specific requirements for integrating cyber assets into the operational technology domain, broader IT control solutions can often be leveraged to provide value to the organization. Examples of such solutions include security monitoring, secure communications, and compliance management technologies.

Data Management

Power and utilities companies may also find it difficult to manage the new volume of data (evidence) they need to demonstrate compliance to regulators. Because the source documents for cyber assets and supporting technologies are frequently voluminous and disorganized, they often do not contain sufficient compliance evidence. In addition, on an organization-wide basis, the documentation standards are often inadequate and inconsistent.

Even when appropriate evidence is gathered, it results in a large new volume of data that must be indexed, managed, and sustained for the required regulatory durations. While many power and utilities companies started with simple document management solutions (e.g., SharePoint), they are quickly realizing that they need to implement more robust compliance data management solutions to integrate and manage compliance data in the long term. Further, companies are recognizing the challenges of optimizing the voluminous data in an effort to proactively monitor potential risks.

Interpreting the Requirements

Various stakeholders that implement and monitor the compliance requirements throughout an organization may interpret the CIP standards differently, resulting in inconsistent design, implementation, and performance of compliance activities. For example, stakeholders may have differing understanding of key terms[11] such as (1) "monthly," (2) "significant change," and (3) "exception." The resulting inconsistent application may result in inefficiencies in implementing the requirements or, in a worst-case scenario, a program that ineffectively identifies threats to the organization's cybersecurity.

Various stakeholders that implement and monitor the compliance requirements throughout an organization may interpret the CIP standards differently, resulting in inconsistent design, implementation, and performance of compliance activities.

Resources

Responsible entities often have inadequate staffing to properly implement and support compliance, audit, and security activities. Therefore, operational teams maintaining cyber assets typically have had the additional responsibility of performing NERC CIP compliance. In many instances, these individuals lack the qualifications and training to properly meet the demands of these responsibilities and, to further complicate matters, there is often a lack of clarity regarding the roles and responsibilities of those involved in this process.

Such resource issues often culminate in a rushed, last-minute effort by organizations to meet compliance requirements that is inefficient and ineffective. In extreme cases, those assigned may not understand the evaluation criteria for the program performance and those charged with managing the responsible entity's overall compliance program may find it difficult to track costs and understand the level of effort needed to successfully meet the compliance requirements.

[11] NERC has developed Compliance Application Notices (CANs) to clarify and provide guidance on some key terms included in the CIP standards, although the CANs do not fully clarify all aspects of the CIP standards.

Overcoming Potential Challenges

With the effective date of Version 4 a little more than a year away and the approval of the "next generation" NERC CIP Version 5 expected in the near term, affected responsible entities should start working toward meeting the expanded requirements by:

- Establishing an **asset management database** that contains information about asset, usage, relationship and risk profiles, and link compliance processes.
- Using **an integrated governance, risk, and compliance (GRC) tool** to distribute policies and map them to regulations and internal policies.
- Developing a repeatable, yet flexible, **process for personnel risk management**, including integrated role-based training for key performers.
- Integrating **enterprise identity and access management solutions** into the responsible entity's operations to (1) increase efficiency in access provisioning and de-provisioning and (2) streamline the periodic access review processes.
- Establishing **security monitoring throughout the responsible entity's operations** and related IT environment by considering the impact of emerging remote access solutions designed to address Version 5 standards.
- Building **an integrated control and monitoring solution** to consolidate various security systems within the responsible entity, allowing for a single view.
- **Monitor and enforce compliance procedures** by implementing a GRC tool as a single framework that integrates all applications.
- Designing an **incident reporting tool** to manage the processes for security incidents with a well-documented and repeatable workflow.
- Establishing thorough scenarios to **build and test a resilient enterprise** and promote quicker recovery time during failures.

To alleviate the pressures of complying with multiple federal and state regulatory requirements, organizations should consider leveraging existing general corporate compliance processes and developing an integrated compliance risk management program.

Integrating NERC CIP Compliance Requirements Into an Overall Compliance Program

To alleviate the pressures of complying with multiple federal and state regulatory requirements, organizations should consider leveraging existing general corporate compliance processes and developing an integrated compliance risk management program. Under this approach, a company would consider its regulatory, industry, and internal compliance requirements as a whole, allowing more efficient use of the company's people, processes, tools, and technology.

Thinking Ahead

The Deloitte Power & Utilities industry team will continue to monitor current and future activity related to NERC CIP requirements. As warranted, we will provide periodic updates (e.g., live industry seminars, *Dbriefs* webcasts, industry spotlights) on this activity, detailing its potential effect on your business or the industry as a whole. Also see Deloitte's *Power & Utilities: Financial Reporting, and Tax Update (January 2013)*.[12]

In addition, certain Deloitte professionals continually monitor both NERC CIP standard-setting activity and the NERC CIP program as a whole. Feel free to contact any of the following individuals for additional information:

- Sharon Chand (shchand@deloitte.com).
- Dmitriy Borovik (dborovik@deloitte.com).
- Paul Campbell (paulcampbell@deloitte.com).

[12] Previously titled *Energy & Resources: Accounting, Financial Reporting, and Tax Update.*

Appendix A — Evolution of Critical Infrastructure Protection

Background

The U.S. government's CIP program includes a standardized description of critical infrastructure that allows for consistent monitoring of, and preparation for, events that might disable the assets in a particular sector. Under this program, each private company in the industry sector must perform certain responsibilities related to protecting its assets, including:

- Assessing its vulnerability to both physical and cyber-related attacks.
- Establishing a plan to eliminate significant vulnerabilities.
- Developing systems to identify and prevent potential attacks to the infrastructure.
- Identifying, containing, and fighting back against known attacks.
- Rebuilding essential capabilities with the assistance of the Federal Emergency Management Agency after an attack.

In the context of energy and resources, more specifically the critical infrastructure related to power, the Department of Energy (DOE) is charged with overseeing the energy supply (e.g., electricity, oil, natural gas) aspect of the CIP program. Further, the DOE works with the Nuclear Regulatory Commission to help monitor and protect the critical infrastructure of nuclear power plants.

FERC is the U.S. federal agency charged with (1) overseeing the sale of interstate electricity, (2) regulating wholesale electric rates, (3) licensing hydroelectric plants, (4) regulating pricing for natural gas, and (5) regulating oil pipeline rates. FERC has certified NERC as the not-for-profit ERO responsible for developing and monitoring regulatory standards for power system operation, developing and providing educational and training resources to operators as part of an accreditation program, and assessing the adequacy of the power infrastructure. Further, NERC investigates any significant power system disruptions and analyzes the causes to help alleviate any future events.

An Evolution to Where We Are Today

To face potential risks of cyberterrorism against the North America power grid, NERC developed Version 1 of its CIP program. Version 1, which consisted of nine separate standards, addressed the potential risks associated with the cybersecurity of assets embedded in the power generation infrastructure in North America. This version served as the foundation for the current CIP reliability standards in the NERC CIP program and included the following standards:

- CIP-001, "Sabotage Reporting."
- CIP-002, "Cyber Security — Critical Cyber Asset Identification."
- CIP-003, "Cyber Security — Security Management Controls."
- CIP-004, "Cyber Security — Personnel & Training."
- CIP-005, "Cyber Security — Electronic Security Perimeter(s)."
- CIP-006, "Cyber Security — Physical Security of Cyber Assets."
- CIP-007, "Cyber Security — Systems Security Management."
- CIP-008, "Cyber Security — Incident Reporting and Response Planning."
- CIP-009, "Cyber Security — Recovery Plans for Critical Cyber-Assets."

On August 28, 2006, Version 1 of the NERC CIP reliability standards was submitted to FERC; it was subsequently approved by FERC on January 8, 2008. Version 1 was effective from July 1, 2008, through January 1, 2010, and was phased in.

On August 7, 2008, the NERC Standards Committee began Project 2008-06, "Cyber Security," and charged a standards development team (SDT) with reviewing each cybersecurity standard to (1) ensure that it conformed to the latest version of the electric reliability organization rules of procedure and (2) met the requirements and needs of industry stakeholders. In working toward this goal, the NERC SDT refined the language from certain standards while adding language to clarify the requirements and related guidance in others. Version 2 of the CIP program was filed with FERC on May 22, 2009; was subsequently approved by FERC on September 30, 2009; and became effective on April 1, 2010.

NERC continued to review, refine, and enhance its CIP reliability standards. Its efforts culminated with the filing of Version 3 with FERC on December 29, 2009, which was subsequently approved on March 31, 2010, and became effective on October 1, 2010. While each of the nine Version 3 standards was consistent with its counterpart in Version 2, there was one significant change: Version 3 revised the implementation considerations and requirements related to (1) newly identified critical cyber assets and (2) newly registered entities. Under the previous implementation guidance, responsible parties were required to immediately identify any new critical cyber assets and these assets were subject to audit requirements. This proved challenging for responsible entities since they were not given enough time to achieve this milestone. Under the revised implementation plan guidance, a responsible entity would be given a reasonable amount of time to meet the CIP program compliance requirements for newly identified critical cyber assets. The revised implementation plan also addresses the compliance requirements for newly identified critical cyber assets resulting from a merger with an entity or an acquisition made by an entity.

Appendix B — NERC Version 5 CIP Standards

The table below (1) lists the NERC Version 5 CIP cybersecurity standards, (2) gives a brief overview of the standards, and (3) discusses high-level differences between Version 5 and Version 4. This table is not all-inclusive and should be considered in conjunction with the current Version 5 draft on the NERC's Web site.

Standard	Purpose[13]	Differences Compared With Version 4
CIP-002-5, "Cyber Security — BES Cyber System Categorization"	"To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES."	• The terms "critical asset" and "cyber asset" are replaced with "BES cyber asset," and the impact of these assets on BES reliability services is discussed. • There is a shift from identifying critical cyber assets (prior versions) to identifying BES cyber systems. • How the rest of the standards are applied will be determined on the basis of the characterization of BES cyber assets and BES cyber systems within this standard.
CIP-003-5, "Cyber Security — Security Management Controls"	"To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES."	• Version 5 removes the requirement related to policy exceptions. • Requirements in Version 4 related to information protection are shifted to CIP-011-1. • Requirements in Version 4 related to change control and configuration management are moved to CIP-010-1.
CIP-004-5, "Cyber Security — Personnel & Training"	"To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems."	• Specific role training is added for (1) the visitor control program, (2) electronic interconnectivity supporting the operation and control of the BES cyber systems, and (3) storage media as part of the handling of BES cyber systems information. • References are changed from critical cyber assets to BES cyber systems. • Training requirement is changed from "annual" to "once every 15 calendar months." • Seven-year criminal history check is now required for all locations where an individual resided. • All access management requirements are relocated to this standard. • Requirement is included for immediate revocation of cyber asset physical and electronic access of an individual upon transfer, retirement, or termination.
CIP-005-5, "Cyber Security — Electronic Security Perimeter(s)"	"To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES."	• It is clarified that a BES cyber asset connected via routable protocol must be in an electronic security perimeter. • New requirements are provided for interactive remote access sessions, including (1) requirement to use intermediate system so that there is no direct access to cyber asset, (2) use of encryption that terminates at an intermediate system, and (3) need for multifactor authentication of all interactive remote access sessions.
CIP-006-5, "Cyber Security — Physical Security of BES Cyber Systems"	"To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES."	• "Six-wall" border concept is eliminated ("physical security perimeter" term is retired). • Implementation of one or more physical access controls is allowed under defined physical boundary concept. • Documentation of controls related to physical access is required. • One or more physical access controls are required for "medium" impact, and two or more different physical access controls are required for "high" impact.

[13] The "purpose" is excerpted directly from each respective standard from NERC CIP Version 5, released on October 26, 2012.

Standard	Purpose	Differences Compared With Version 4
CIP-007-5, "Cyber Security — Systems Security Management"	"To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES."	• Applicable only to high- and medium-impact systems. • In Version 5, there are enhanced requirements for (1) security management of physical input/output ports, (2) security patch management, (3) malicious code prevention, (4) security event monitoring, and (5) system access control.
CIP-008-5, "Cyber Security — Incident Reporting and Response Planning"	"To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements."	• In Version 5, activities required to maintain cybersecurity incident response plan are clearly specified. • Timeline and requirements are provided for (1) documenting lessons learned, (2) updating/modifying response plan, and (3) updating individuals on plan changes as a result of a test or actual cybersecurity incident response.
CIP-009-5, "Cyber Security — Recovering Plans for BES Cyber Systems"	"For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as 'Responsible Entities.' For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly."	• Applicable only to high- and medium-impact systems. • Requirement is established for one or more processes for the backup and storage of information supporting recovery of BES cyber system functionality. • Testing timing and requirements are established for information used to recover BES cyber system functionality.
CIP-010-1, "Cyber Security — Configuration Change Management and Vulnerability Assessments"	"To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES."	• CIP-010-1 did not exist in Version 4 (certain guidelines that were moved from other standards are incorporated). • Applicable only to high- and medium-impact systems. • Baseline configuration requirement that was not included in Version 4 is incorporated. • Authorization of changes from baseline is required. • "Specific test procedures" are removed but the point at which testing must occur is clarified. • Monitoring requirement is enhanced to include need to consider malicious actions and intentional changes. • Requirement is added to perform active vulnerability assessment for new cyber assets.
CIP-011-1, "Cyber Security — Information Protection"	"To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES."	• CIP-011-1 did not exist in Version 4 (certain guidelines that were moved from other standards are incorporated). • Applicable only to high- and medium-impact systems. • Methods for identifying BES cyber information are required. • Procedures are required for protecting BES cyber system information, including the storage, transit, and use of such information.

Contacts

If you have questions about this publication, please contact the following Deloitte industry professionals:

Bill Graf
U.S. AERS Sector Leader,
Power & Utilities
Industry Professional Practice
Director, Power & Utilities
Deloitte & Touche LLP
+1 312-486-2673
wgraf@deloitte.com

Paul Campbell
Energy Regulatory & Risk
Practice Leader
Deloitte & Touche LLP
+1 713 982 4156
paulcampbell@deloitte.com

Sharon Chand
Security and Privacy Services
Deloitte & Touche LLP
+1 773 294 6430
shchand@deloitte.com

Dmitriy Borovik
Enterprise Risk and
Compliance Management
Services
Deloitte & Touche LLP
+1 212 436 4109
dborovik@deloitte.com

Subscriptions

Don't miss an issue! Register to receive Spotlight and other Deloitte publications by going to www.deloitte.com/us/subscriptions, choosing the Industry Interests category, and checking the boxes next to your particular interests. Publications pertaining to your selected industry (or industries), along with any other Deloitte publications or webcast invitations you choose, will be sent to you by e-mail.

Dbriefs for Financial Executives

We invite you to participate in *Dbriefs*, Deloitte's webcast series that delivers practical strategies you need to stay on top of important issues. Gain access to valuable ideas and critical information from webcasts in the "Financial Executives" series on the following topics:

- Business strategy & tax.
- Corporate governance.
- Driving enterprise value.
- Financial reporting.
- Financial reporting for taxes.
- Risk intelligence.
- Sustainability.
- Technology.
- Transactions & business events.

Dbriefs also provides a convenient and flexible way to earn CPE credit — right at your desk. Join *Dbriefs* to receive notifications about future webcasts at www.deloitte.com/us/dbriefs.

Registration is available for this upcoming *Dbriefs* webcast. Use the link below to register:

- The Responsible Enterprise: At the Intersection of Commerce and Corporate Citizenship (May 7, 2 p.m. (EDT)).

Technical Library: The Deloitte Accounting Research Tool

Deloitte makes available, on a subscription basis, access to its online library of accounting and financial disclosure literature. Called Technical Library: The Deloitte Accounting Research Tool, the library includes material from the FASB, the EITF, the AICPA, the PCAOB, the IASB, and the SEC, in addition to Deloitte's own accounting and SEC manuals and other interpretive accounting and SEC guidance.

Updated every business day, Technical Library has an intuitive design and navigation system that, together with its powerful search features, enable users to quickly locate information anytime, from any computer. Technical Library subscribers also receive *Technically Speaking*, the weekly publication that highlights recent additions to the library.

In addition, Technical Library subscribers have access to Deloitte Accounting Journal entries, which briefly summarize the newest developments in accounting standard setting.

For more information, including subscription details and an online demonstration, visit www.deloitte.com/us/techlibrary.

The Spotlight series is prepared by the National Office Accounting Standards and Communications Group of Deloitte. New issues in the series are released as developments warrant. This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.