Critical Infrastructure Protection Required on Electric Grid Continually Changing

David W. Hilt

The supply of electricity since the days of Thomas Edison and George Westinghouse has been an ever-changing and rapid-growth environment. One of the most significant changes came in 1964, when seven separate systems were connected to ultimately form what is known today as the Eastern Interconnection. In it, all of the generators, transmission lines, and loads operate as one very large system. The interconnections—Eastern, Western, Texas, and Quebec—operate with all generators in synchronization, making them essentially one very large machine (**Exhibit 1**).

Electricity is recognized as a critical infrastructure by the US Department of Homeland Security in that it is an enabling infrastructure for all other critical infrastructures.

As utilities interconnected the system to improve the overall reliability of the system, consumers took confidence in the supply of electric energy in the United States. Today, the electric supply system in North America has become part of our everyday life in so many ways that it is hard to think of any aspect of modern life that is not impacted by the supply, or, more correctly, the lack of supply, of electricity. We obviously would have trouble heating and cooling our homes, but so many other areas would be impacted. These include our telecommunications, medical services, and transportation, due to pumping of fuels, food delivery, and even our ability to purchase items in the local grocery store. Indeed, the supply of energy including electricity is recognized as a critical infrastructure by the US Department of Homeland Security in that it is an enabling infrastructure for all other critical infrastructures.

Exhibit 2 shows the growth in electric energy usage since World War II. That growth has leveled off since 2009 due to improvements in energy efficiency and lower overall demand, but the criticality of the electric supply remains.

STANDARDS DEVELOPED AFTER 9/11

Recognizing this critical nature and responding to threats against the United States following the September 11, 2001, attacks; cyberevents at the time, such as the SQL Slammer Worm that directly impacted the electric utility industry; and a 2003 federal advisory regarding foreign attack scenarios, the North American Electric Reliability Corporation (NERC) had initially developed a set of Critical Infrastructure Protection (CIP) standards in 2003. These standards, the Urgent Action 1200 standards, were the first such industry-based standards for cybersecurity. These initial reliability standards were voluntary, and the first enforceable CIP standards were approved by the Federal Energy Regulatory Commission (FERC) on January 18, 2006, in FERC Order 706.

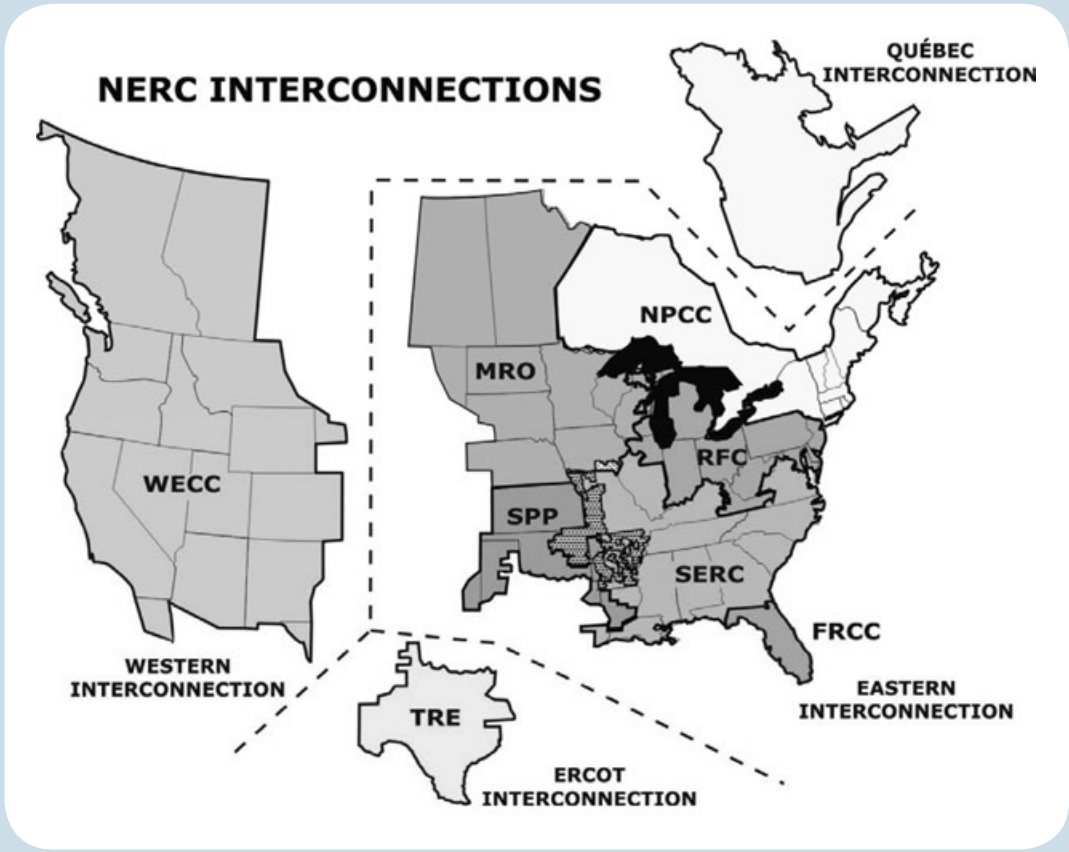
In February 2003, the president's Critical Infrastructure Protection Board said the following:

> A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption of our

David W. Hilt, P.E. (dhilt@gridreliabilityllc.com), is president of Grid Reliability Consulting LLC.

DOI 10.1002/gas.22040

Exhibit 1. NERC Interconnections



Nation's critical infrastructures, economy, or national security.

This concern has not changed since then.

The initial concepts for cybersecurity and critical infrastructure protection from those early NERC Urgent Action standards have not changed. While much more detail has been added to the standards since then, the original concepts remain in the standards today and included the following:

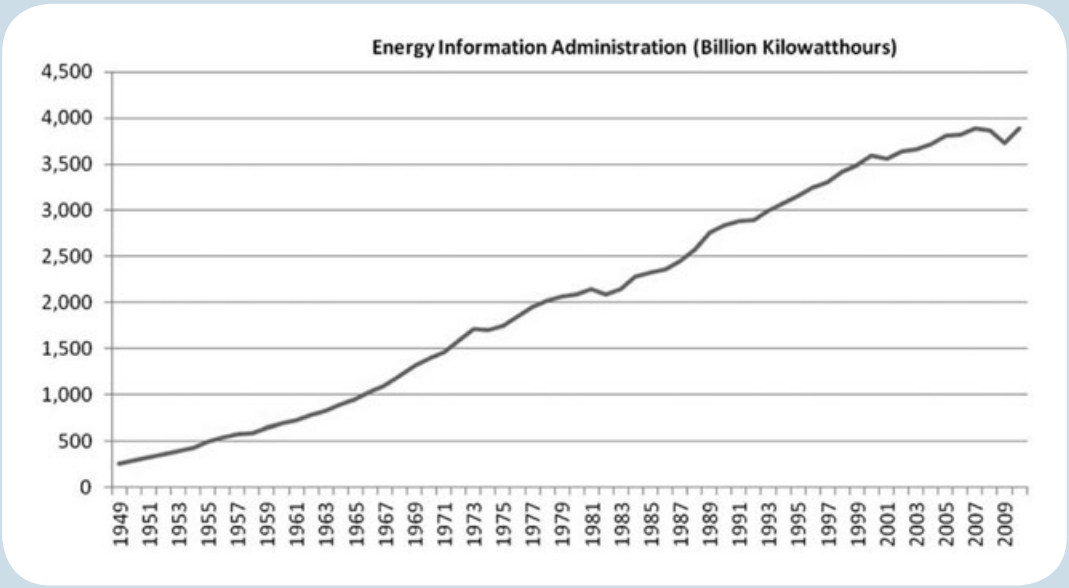
- Establishing a cybersecurity program including
  - Policy and procedures
  - Identifying accountable management
- Identifying/documenting critical cyberassets
- Defining/implementing electronic:
  - Security perimeters
  - Access controls
  - Monitoring controls
- Defining/implementing physical:
  - Security perimeters
  - Access controls
  - Monitoring controls
- Defining/implementing personnel authorization controls
- Security awareness training
- Information protection controls
- Cybersystem management controls
- Cybersystem test procedures
- Incident response and reporting for cyber and physical security incidents
- Recovery planning

These concepts were very fundamental and are the foundations of a good cybersecurity program.

Since the original standards were put in place, the cyberworld has not become any friendlier, and attacks on utilities have continued. In 2007, the Department of Energy conducted a test on a generator demonstrating that a cyberattack could destroy the generator. This event was followed by congressional hearings in October 2007 and May 2008. Utilities have been the target of ransomware where they were required to pay a ransom to gain control of some computer

  / DOI 10.1002/gas

Exhibit 2. US Electric Consumption



system back from the attacker. Most notably, in December 2015 and again in December 2016, cyberattacks resulted in power outages in the Ukraine. All of this activity and other activity related to industrial control systems continue to place a great deal of attention on cybersecurity for the electric power systems.

Physical security of the electric grid came to the forefront in April 2013 when, in a sophisticated attack including communication systems, gunmen fired on the Metcalf Transmission Substation near San Jose, California, damaging a number of large power transformers. The attack resulted in over $15 million in damage to that substation. While there are substantial rewards offered (total $500,000), no one has been identified as responsible for the attack. In response, FERC directed NERC to develop a standard to identify and physical protect such facilities.

While there are substantial rewards offered (total $500,000), no one has been identified as responsible for the attack.

That standard, CIP-014, was approved by FERC on November 20, 2014, and the standard became effective on October 1, 2015.

CRITICAL INFRASTRUCTURE CHALLENGES

One of the most significant challenges in developing and managing a program for critical infrastructure protection is the need to bring a number of functional areas together to effectively implement the program. The NERC CIP standards do a good job of laying out the fundamentals of a program, but the implementation and tracking are challenging.

Implementation and tracking are challenging.

First, the areas within a company that must be involved include management, system operations, information technology/management, human resources, training, and physical security. All of these areas must work in unison to have an effective program. In some cases, companies have established a corporate security function, either as a stand-alone group or as a virtual group, to manage the cyber and physical security of physical, electronic, information, and employees.

The NERC CIP standards are among the most frequently violated standards on an ongoing basis. Much of this is due to the challenges posed by ensuring that background checks and training are

DOI 10.1002/gas

up-to-date for everyone with unescorted physical and electronic access to bulk electric system (BES) cybersystems and assets as well as monitoring and revoking access based on these factors and need due to employees leaving or transferring and no longer having a need for access.

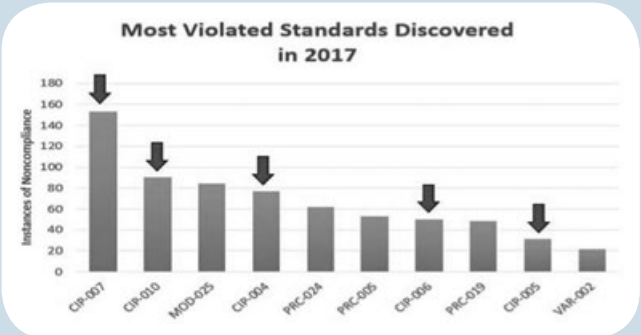
The NERC CIP standards are among the most frequently violated standards on an ongoing basis.

Exhibit 3 shows the most violated standards discovered by NERC in 2017 (not full-year reporting) to be CIP-007 (System Security Management) and CIP-010 (Change Management and Vulnerability Assessments). CIP-004 (Personnel and Training) is also on the list, as well as CIP-006 (Physical Security of BES Cyber Systems) and CIP-005 (Electronic Security Perimeters). The arrows highlight CIP standards.

NERC made a major modification to the CIP standards with the adoption of the "Version 5" (V5) reliability standards. The previously approved Version 3 CIP standards allowed entities to implement their Risk-Based Analysis Methodology to identify the transmission assets that were critical and then to identify any cyberassets associated with those transmission assets. According to NERC,

> CIP Version 5 represents a significant improvement—and change—over the currently-effective CIP Version 3, as it adopts new cyber security controls and extends the scope of systems that are protected by the CIP Reliability Standards.

Exhibit 3. NERC Summary of Most Frequently Violated Standards 2017—NERC BOTCC



The standards were indeed significant in that all risks throughout the BES were categorized as high, medium, or low impact based on the categorization provided by NERC in CIP-002, specifically Attachment 1 to that standard.

The result was more electric utilities would become involved and more groups and personnel in companies that had assets under Version 3 would become involved. Medium- and low-impact facilities and their BES cyberassets now needed to be addressed.

The V5 standards were approved on November 22, 2013, with implementation across all high-, medium-, and low-impact BES cybersystems on April 1, 2017. The industry did a good job of implementing the standards as reported by NERC. **Exhibit 4** shows the number of violations per year through the transition period (2017 data is not yet complete).

The industry did a good job of implementing the standards as reported by NERC.

STANDARD-BY-STANDARD CHALLENGES

CIP-002—BES Cyber System Categorization

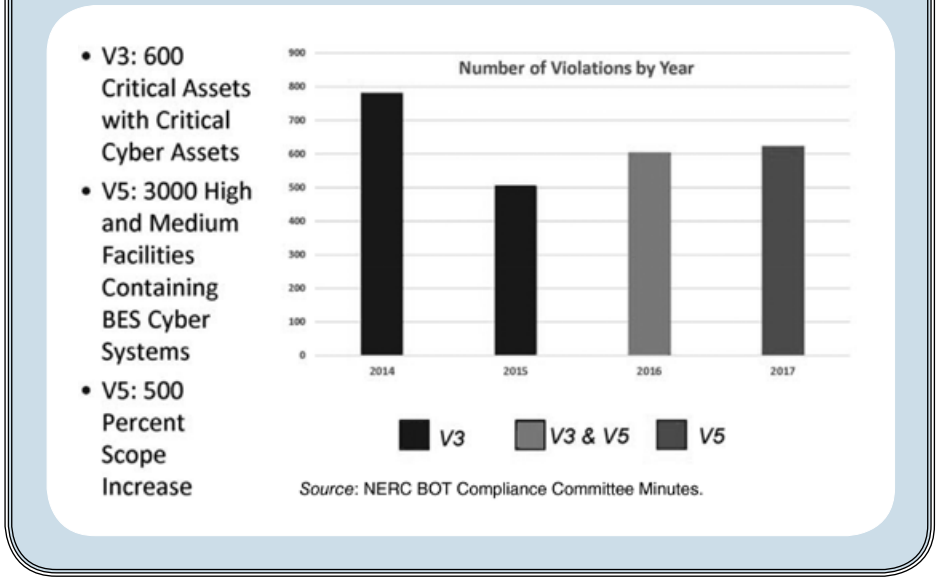
NERC made a significant change in CIP-002 V5 to include BES cybersystems rather than just BES cyberassets. In the new standard, several critical cyberassets may comprise a single BES cybersystem. This change allowed for management of systems that can be categorized based on the function they perform, the type of device, the manufacturer, and other factors, allowing for potentially easier management of large numbers of assets when software or firmware changes.

However, the standard requires the categorization of all BES cyberassets based on the definitions in Attachment 1 to the standard. With the standard being applied to the full lists of facilities in Attachment 1, some clarity was added to what constituted a BES cybersystem in that if the system did not impact the BES within 15 minutes or less, it was not a BES cybersystem. This standard allowed for the recognition that some systems, such as a fuel-handling system at a coal-fired power plant, allow sufficient time for operations processes to respond to avoid sudden BES disturbances.

In general, high-impact are control centers and backup control centers for reliability co-

  / DOI 10.1002/gas

Exhibit 4 CIP Reliability Standard Violations by Year



Source: NERC BOT Compliance Committee Minutes.

ordinators and balancing authorities with generation over 3,000 megawatts and transmission operators and generator operators that control medium-impact assets. Medium-impact are generating plants that exceed 1,500 megawatts in aggregate (generators can be segmented depending on configuration and controls), transmission facilities operating at 500 kilovolts and above, control centers not included as high impact that control in excess of 1,500 megawatts, and transmission facilities operating below 500 kilovolts based on a scoring index (less than 200 kilovolts are not applicable to the scoring). Low-impact are everything else associated with the BES, including other control centers, substations, generating resources, and other facilities. There has been some confusion surrounding the medium-impact control centers for transmission operators, and NERC is working to provide clarity in Version 6 of CIP-002, currently under development.

High-impact are control centers and backup control centers for reliability coordinators and balancing authorities with generation over 3,000 megawatts and transmission operators and generator operators that control medium-impact assets.

The biggest challenge with CIP-002 is identifying and categorizing all BES cybersystems and associated cyberassets and maintaining up-to-date inventories.

CIP-003—Security Management Controls

This standard requires the development of documented policies for cybersecurity management of BES cybersystems. The latest version, Version 6, included some requirements for low-impact BES cybersystems at the direction of FERC. It is worth noting that the requirements for low impact were added to this standard.

Tracking physical keys, dealing with lost keys, and multiple padlocks for joint ownership and contractors to gain access can be challenges for ensuring compliance.

There will likely be challenges with some of the provisions. For example, many utilities have low-impact facilities and can use existing programs for cybersecurity awareness (every 15 months) and incident response plans. However, physical security controls and electronic access controls may be more challenging. For example, an electronic access point may need to be added for BES cybersystems. Further, many utilities allow access to low-impact facilities with padlocks and physical keys. A program will need to be documented and in place for such a program.

DOI 10.1002/gas / © 2018 Wiley Periodicals, Inc.

Where there may be a program, tracking physical keys, dealing with lost keys, and multiple padlocks for joint ownership and contractors to gain access can be challenges for ensuring compliance with the requirements of the standard.

CIP-004—Personnel and Training

Ensuring that all personnel with electronic access and unescorted physical access have proper seven-year personnel risk assessments and have completed all required training required for high- and medium-impact assets is often the reason this standard is violated. Revocation of access for termination within 24 hours (not a business day) and the next calendar day for reassignment or transfer is also required. With the increased pool of high- and medium-impact assets under the V5 reliability standard, tracking of employee and contractor training, personnel risk assessment, and terminations and reassignments is the most challenging aspect.

Establishing links across the organization is critical. Operations must provide the lists of personnel and contractors with a business need to access the BES cybersystems. Training must design and provide the required training, and Human Resources must ensure that the personnel risk assessments are completed as required. Each group must make the necessary notifications to revoke access. Information Technology and Physical Security must revoke access as required.

Software systems to track those with access for these requirements must be applied across the organization for a successful implementation.

CIP-005—Electronic Security Perimeters and CIP-006—Physical Security of BES Cyber Systems

These two standards together ensure the security of high- and medium-impact BES cybersystems from both unauthorized electronic and physical access.

Methods of detecting known or suspected malicious communication and controls for remote access must be in place. Again, with the expansion of the standards under V5, new organizations and facilities may now be required to meet these requirements. Fortunately, technology is readily available, but there are likely costs for the additional facilities and tracking is necessary.

Remote access continues to be an issue, and FERC directed that NERC conduct a study of remote access issues. NERC filed that report on June 30, 2017, and more on the issue is expected in future standard modifications.

CIP-007—System Security Management and CIP-010—Configuration Change Management

Until NERC developed the V5 CIP standards, much of what is in these two standards was combined under CIP-007.

CIP-010 was a new standard with the V5 update for high- and medium-impact BES cybersystems. Many of the challenges from these standards come from managing of ports and services, security patch management, configuration change management, shared-password management, and configuration changes. For effective management, each of these processes should be handled through systems that require appropriate approvals before any changes are made and, in the case of high-impact assets, tested in a nonproduction environment.

Transient cyberassets and removable media were addressed in the second version of CIP-010 as required by FERC. Companies with high- and medium-impact BES cyberassets are required to have plans for each that are detailed in Attachment 1 to that standard to ensure detection and mitigation of malicious code on transient cyberassets and removable media used by employees or contractors.

Other CIP Standards

CIP-008, CIP-009, and CIP-011

CIP-008, Incident Reporting and Response Planning, and CIP-009, Recovery Plans for BES Cyber Systems, were two fundamental requirements included in the original CIP standards developed in 2003. These standards require drills and updates to the plans following the drill or actual incident within a defined timeframe. CIP-011, Information Protection, while not a new concept in the CIP standards, was separated out in a new standard under V5. This standard requires the identification and protection of BES cybersystem information, including storage, transit, and use of the information. It

  / DOI 10.1002/gas

also contains requirements related to the release, reuse, and disposal of cyberassets that contain BES cyberinformation.

CIP-014—Physical Security

This standard was developed following several events that could be classified as a physical attack on the BES from a physical versus a cyber perspective, including the Metcalf attack.

The standard requires that for BES elements, the company conduct a risk assessment of the impact to the BES if the facility (entire substation, control center, or other installation) is rendered inoperable or damaged as a result of a physical attack. If there is the possibility of cascading, instability, or uncontrolled separation of the BES within an interconnection, then the facility must have a physical security plan developed and implemented. The risk assessment and physical security plan must be reviewed by an independent third party.

While NERC cannot develop regulations beyond the scope of the BES, utilities should consider the impact of their systems on other critical infrastructures. While physical security cannot be required by the standard, physical security of remote electric facilities serving critical loads should be considered even if the impact is not significant to the BES. Energy, and electricity in particular, is an enabling infrastructure for all other infrastructures.

If there is a significant impact to another infrastructure, the utility may be held accountable in the public eye.

If there is a significant impact to another infrastructure, the utility may be held accountable in the public eye.

EMERGING ISSUES

NERC has stated that

> the supply chains for information and communications technology and industrial control systems present significant risk to [BES] security providing various opportunities for adversaries to initiate cyberattacks.

Such attacks have already happened to industrial control systems and on utility systems elsewhere in the world. However, NERC has no authority over the suppliers of systems to the electric utility industry. Given the level of concern at the federal level, FERC directed NERC to develop forward-looking, objective-based standards that address these risks.

In response, NERC developed CIP-013, Supply Chain Risk Management and made modifications to CIP-005 and CIP-010 to address supply-chain issues. These standards were filed with FERC in September 2017 and are awaiting approval. The proposed standards will apply to high- and medium-impact BES cybersystems and will require specific procurement processes to identify and assess cybersecurity risk from procuring and installing vendor equipment and software including transitions from one vendor to another.

The update to CIP-005 will require methods to determine active vendor remote-access sessions (including system-to-system) and the ability to disable those sessions. CIP-010 will require for operating systems, firmware where no independent operating system exists, commercially available or open-source software installed, and any security patches applied that utilities verify the identity of the software source and verify the integrity of the software obtained prior to installation.

NERC is also working on standards related to virtualization in the CIP environment. NERC is currently developing a revised definition of a cyberasset to include virtual assets.

A MOVING TARGET

Cybersecurity is an ever-changing environment.

Cybersecurity is an ever-changing environment.

The reliability standards developed to protect one of our most critical infrastructures from cyber (and physical) attack will continually be changed and updated to address changes in technology, application, and the approach of potential cyberattack scenarios. The NERC Standards are a moving target and have become more aligned with the National Institute of Standards and Technology (NIST) approaches.

The NIST website provides a wealth of information regarding cybersecurity and response planning.

DOI 10.1002/gas