

The Challenge of Implementing NERC's Cyber Standard

How to develop, implement, and operate a security program.

BY RON BLUME, P.E.

On May 2, 2006, the North American Electric Reliability Council (NERC) board of trustees adopted the Critical Infrastructure Protection (CIP) Cyber Security Standard. The comprehensive standard—which addresses asset identification, security management controls, personnel and training, perimeter security, systems security, incident reporting and response planning, and recovery plans—is intended to “ensure that all entities responsible¹ for the reliability of the bulk electric systems² in North America identify and protect critical cyber assets³ that control or could impact the reliability of the bulk electric systems.”

On July 20, 2006, the Federal Energy Regulatory Commission (FERC) certified NERC as the Electric Reliability Organization (ERO) charged with the responsibility to develop and enforce bulk-power system⁴ reliability standards. The forthcoming mandatory enforcement provisions of the standard raise a number of burning questions for electric utilities:

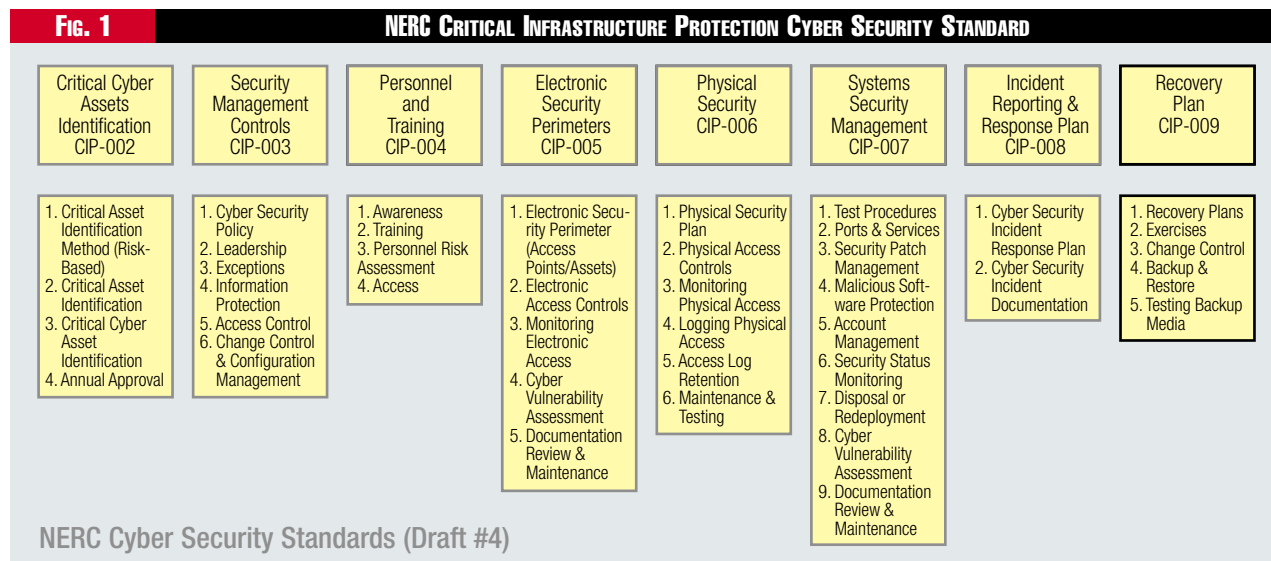
- How much of an effort will it take in terms of cost and time to develop, implement, and sustain a compliant security program?
- How do the provisions of the standard relate to existing security programs?

- What additional processes, procedures, policies, organizational resources, and additional information support infrastructures (software or hardware) will be required?
- Other than complying with the standard, are there any real benefits that can be realized with implementation of the standard?
- To what type of issues will implementation of the standards give rise?

This article provides some answers to these questions in the form of security program development, implementation, and operation.

Requirements

While the standard is designed specifically to protect only the critical cyber assets, the implications of the requirements reach far beyond the boundaries of the defined critical cyber assets from a cyber, physical, and managerial perspective. As illustrated in Fig. 1, the standard includes eight major topics and 41 specific requirements. As can be observed, the standard complements the premise that security is more than just technical solutions and procedures: It addresses processes, policies, physical security, and management issues. »



XEROX

Security Program

Development Strategy

Fifteen different functional program areas, illustrated in Fig. 2, have been identified⁵ as relevant to the implementation of a responsive and comprehensive standard-compliant security program. The critical factor within the functional program area definitions is the development of specific interrelationships between the functional program areas that are consistent with the operational characteristics of the entity. This functional program model provides the framework for an organized and logical approach to develop the required policies, procedures, documentation, and subsequent training and security awareness program curriculums. In addition, technical requirements, including supporting software tools such as document control systems, identity management strategies, and network management tools, can be developed in a controlled and consistent manner through this framework. Last, a viable program implementation work plan can be developed from the functional program area perspective.

Organizational Relationships

Multiple organizations will need to be involved in the development of the security program. The responsibility for many of the functional program areas delineated above falls outside the operations groups typically responsible for critical cyber assets—*i.e.*, transmission, engineering, generation, energy delivery.

Fig. 3 illustrates the security program relationships between functional program areas and organizations within a typical integrated electric utility entity. As an example, the human resource organizations most likely will be involved in the access-control function with regard to the relevant physical and cyber assets. Likewise, most organi-

zations will have a stake in the issues surrounding the information classification and handling function.

The unique organizational relationships also are relevant in terms of the governance requirements for the security program. In this regard, leadership for the security program needs to originate at a level within the organization where visibility for all relevant organizations is resident and responsibility can be committed and delegated accordingly. This approach also will address the need for consistency in the application of policies and procedures across all organizations and functions.

In many cases, these organizational issues are compounded by recent separations of generation and transmission organizations, as well as the sensitivities among the traditional business information systems, engineering, and operation organizations. To ensure an optimized security program, the design, development, implementation, and ongoing operations of the security program require an entity-wide perspective.

Finally, recognizing that the security program reaches beyond the operations organizations of the entity, it may be prudent to address other cyber and physical security and auditing standards⁶ in setting the objectives and scope of the security program.

Critical Cyber Asset Identification

Identifying critical assets and critical cyber assets are very important tasks. The standard requires that critical assets be identified using a risk-based assessment methodology with specific consideration for a specific list of assets.⁷ An appropriate risk-based methodology will need to be developed that quantifies the impact that assets can have on the reliability of the bulk electric system.

Although NERC is interested only

in the reliability of the bulk electric system, a load-serving entity may wish to consider including assets that affect the reliability of serving specific critical loads. In any regard, identification of critical assets is a key task in the security program implementation process and significantly can affect the scope and maintenance of the ongoing processes. Subsequently, a list of critical cyber assets, *i.e.*, cyber assets essential to the operation of critical assets, can be defined.

The standard requirements are quite extensive. As the list of critical cyber assets grows, the operational implications of the security program can expand exponentially. Accordingly, the identification of critical cyber assets must be controlled to minimize this potential impact. Strategically, the following activities are beneficial:

- Optimize the electronic and physical security perimeters⁸ through appropriate design of the underlying network infrastructures;⁹ and
- Recognize and understand the impact of employing routable protocol or dial-up communications with cyber assets.

The standard addresses the physical security of critical cyber assets but does not address the physical security of critical assets that do not contain critical cyber assets. However, given that critical assets by definition affect the reliability of the bulk electric system, it is recommended that each entity evaluate the need to protect, from a physical security perspective, those critical assets that fall into this category.

Technical Issues

In the development of a security program work plan, technical solutions (hardware and software) that can support the compliance sustainability of the program with the standard also may be

FIG. 2 FIFTEEN FUNCTIONAL PROGRAM AREAS RELEVANT TO A STANDARD-COMPLIANT SECURITY PROGRAM

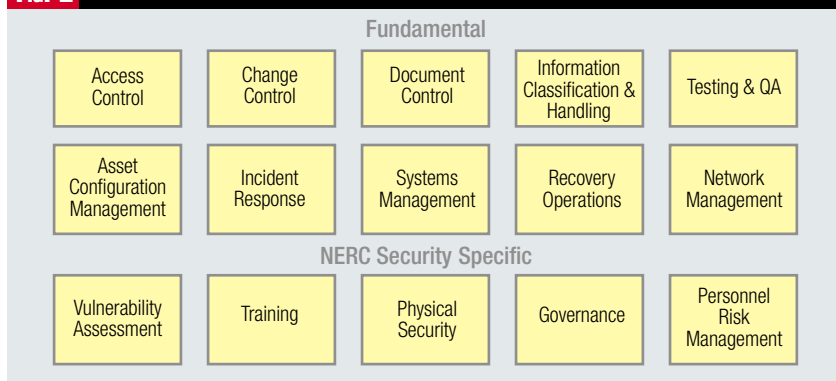


FIG. 3 FUNCTION VS. ORGANIZATION MATRIX

Functional Control Areas	IT Management Services	Physical Facilities Services	Grid Operations	Substation Engineering	Energy Supply	Human Resources	Internal Audit Services	General Counsel/Contracts	Corp Communications
Access Control	x	x	x	x	x				
Change Management	x		x	x	x				
Document Control	x	x	x	x	x			x	
Info Classification and Handling	x	x	x	x	x	x	x	x	x
Testing & Q/A			x	x	x				
Asset Inventory Management		x	x	x	x				
Vulnerability Assessment	x	x	x	x	x				
Incident Response	x	x	x	x	x		x		
Systems Management	x		x	x	x			x	x
Training	x	x	x	x	x	x			x
Physical Security		x	x	x	x				
Recovery Operations	x	x	x	x	x				x
Governance	x	x	x	x	x	x	x	x	x
Personnel Risk Management		x	x	x	x	x		x	
Network Management	x		x	x	x				

needed. Typical considerations follow:

- Managing configuration control of the assets through an appropriate change control process may require new information support systems;
- New requirements for access control and authentication for application systems, servers, routers, firewall, and physical facilities can be a difficult and expensive process to manage and may require new user management and provisioning solutions to efficiently maintain compliance; and
- Document control is an integral component of managing security-related documents that may require new systems.

Tactical Directions

One of the first steps in moving forward with the implementation of a NERC-compliant security program is to conduct a gap analysis inclusive of the following tasks:

- Identify the critical assets, critical cyber assets, the electronic security perimeter, and the physical security perimeter;
- Conduct a security vulnerability assessment of the network infrastructures included within the physical security perimeter and the electronic security perimeter.¹⁰ Include an assessment of both the cyber and physical security provisions. (Note: If the logical network infrastructure design contains critical vulnerabilities, or the

physical security measures are ineffective, policies and procedures, while compliant with the standard, will not ensure that the critical cyber assets are secure.);

- Understand and document the gaps between the existing policies and procedures, and the requirements of the security standard; and
- Use the results of the gap analysis to provide the basis for developing a detailed work plan to implement a NERC compliant security program.


Level of Effort

The level of effort required to develop and implement a NERC-compliant security program can vary significantly by organization and depends on a number of factors, including the:

- Functional responsibility of the entity;¹¹
- Size and complexity of the entity's organization;
- Number of critical assets and critical cyber assets within the organization;
- Experience of the implementation team (internal and consultants);
- Current level of compliance of the existing policies and procedures; and
- Current cyber and physical security of the network infrastructures that protect the critical cyber assets.

Recognizing these factors for a typical entity, an organization can expect a level of effort projected to require from 30 to 60 man months, excluding the potential need for advanced technical solutions or enhanced information support systems. The resultant work schedule can range from 12 to 18 months for a typical implementation plan.

Benefits Summary

These types of projects, driven by mandatory standards, typically are viewed as a necessary expense. However, recognizing that the reliability of the bulk electric system is a critical success factor for most entities, and that the focus of the standard is increased reliability of these assets, significant operational benefits can be achieved through a well-designed security program. As succinctly stated in a recent publication, “an improvement in the overall resiliency of the entity through a viable security program is a goal that is realistic.”¹² 

Ron Blume is vice president and energy practice director for DYONYX. Contact him at (214) 280-8925 or ron.blume@dyonyx.com.

Endnotes

1. A “responsibility entity” is an organization that is (and has registered with the NERC to be) responsible for performing one or more functions as defined in the NERC reliability functional model. In terms of CIP-002, the standard specifically mentions the following entities: Reliability Coordinator, Balancing Authority, Interchange Authority,

Transmission Service Provider, Transmission Owner, Transmission Operator, Generation Owner, Generator Operator, Load-Serving Entity, and Regional Reliability Organizations. Nuclear power organizations are exempt from the standard as well as cyber assets associated with communications networks and data communication links between discrete electronic security perimeters.

2. Bulk electric systems are the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source generally are not included in this definition.
3. Critical cyber assets are those cyber assets essential to the reliable operation of critical assets. Critical assets are defined as those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system.
4. The definition of “bulk power system” by FERC is more comprehensive than the NERC defined “bulk electric system” (see endnote 2). Most likely, in terms of the standard, these differences will be resolved by the ERO or delegated accordingly specific to each entity’s infrastructures.
5. There certainly can be variations from this model as functional definitions are specific to the mission and responsibilities of the underlying entity.
6. For example, ISO 17799, SAS 70, API 1164, and NIST standards may need to be incorporated in the work scope.
7. The assets to be considered as critical assets include control centers, transmission substations, strategic generation resources, restoration facilities, load-shedding facilities, and special protection systems, all of which support the reliable operation of the bulk electric system.
8. NERC defines the electronic security perimeter as the logical border surrounding a network in which critical cyber assets are connected and for which access is controlled. Physical security perimeters are defined by the NERC as the six-wall border surrounding computer rooms, telecommunication rooms, operation centers, and other locations in which critical cyber assets are housed and for which access is controlled.
9. For example, workstations that have direct access to the critical cyber assets should be contained within the same electronic and physical perimeters as other critical cyber assets. Special provisions for remote access will be required.
10. The assurance that a secure network design is in place and is prudent before detailed security procedures are developed as a significant change in the network design can impact the procedure development effort, *e.g.*, re-writes, disjointed procedures, ineffective procedures, and configuration management.
11. The functional program areas defined in this document should not be confused with the functions defined by the NERC reliability functional model. For example, an entity involved in both the generation operations function and the transmission operations function will have significant critical cyber assets compared with an entity serving only as a distribution function, the latter of which may not have any critical cyber assets.
12. *Managing for Enterprise Security*, Richard Caralli, Carnegie Mellon University, December 2004.