Metric #18: Cyber Security

M.18.1.0 Introduction and Background

The interconnected North American grid is arguably the world's largest and most complex machine. It has achieved and sustained an enviable record of reliability through application of numerous technological and operational efficiencies, and strong regulatory oversight. The grid's complexity and interconnected nature, however, also pose a significant drawback; under the right circumstances, problems occurring in one area have the potential to cascade out of control and affect large geographical regions.

Economic forces and technology development are making the power system more dependent on information systems and external communications networks. The interconnected nature of the communications systems that support regional and interregional grid control, and the need to continue supporting older legacy systems in parallel with newer generations of control systems, further compound these security challenges. Additionally, with the advent of inexpensive microcontrollers and smart-grid implementation, there is a growing trend for increased intelligence and capabilities in field equipment installed in substations, within the distribution network, and even at the customer's premises. This increased control capability, while vastly increasing the flexibility and functionality to achieve better economies, also introduces new cyber-vulnerabilities that have not previously existed.

M.18.2.0 Description of Metric

An understanding of component and associated system vulnerabilities will be necessary to quantify cyber-security issues inherent in smart-grid deployments, particularly when these elements can be used to control or influence the behavior of the system. Assessments will be needed, both in controlled laboratory or test-bed environments and in actual deployed field conditions, to explore and understand the implications of various cyber-attack scenarios, the resilience of existing security measures, and the robustness of proposed countermeasures. Vendor adoption of these countermeasures will be critical to broadly influence the installed base of future deployments. The asset-owner utilities will remain responsible for legacy systems.

(Metric 18): the electric power industry's compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards (Table M.18.1).

Designed to maintain the integrity of North America's interconnected electrical systems, the NERC CIP standards establish minimum requirements for cyber-security programs protecting electric control and transmission functions. On January 17, 2008, the Federal Energy Regulatory Commission (FERC) directed NERC to further tighten the standards to provide for external oversight of classification of critical cyber assets and removal of language allowing variable implementation of the standards. One of the areas that will likely be changed in the next revision of the standards is the removal of "reasonable business judgment" in the context of technical feasibility.

Table M.18.1. Summary of the NERC Critical Infrastructure Protection Standards[1]

NERC Standard	*Subject Area*
CIP-001-1	Sabotage Reporting
CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

M.18.3.0 Deployment Trends and Projections

The interviews with 21 service providers in Annex B of this report provides initial data with regard to industry compliance with these cyber-security standards, including the percentage of utilities that have conducted assessments at various frequencies for NERC CIP Standards 002 through 009. The interviews found that 5% of the utility respondents have indicated they have never conducted an assessment. It's not clear whether this is because they are not large enough to have an impact on the bulk electric power system or because they are still in the process of phasing in their compliance. As the timeline for mandatory compliance of all entities associated with the bulk electric system becomes fully implemented, and NERC establishes procedures for more formally tracking compliance with these standards, it will become increasingly easier to gather data and assess trends for this metric.

Table M.18.2. Sample Security Question from Interviews

Have you deployed the following security features? *(Select all that apply)*	**Responses**
a. Intrusion detection	65.0%
b. Key management systems	50.0%
c. Encrypted communications	70.0%
d. Firewalls	95.0%
e. Others (Please describe)	30.0%

While compliance with mandatory security standards is an important step toward achieving security, it is in itself not a complete measure of security. Generally, these security standards are more focused on compliance requirements, and increased compliance may not necessarily equate to increased security. Furthermore, standards can take years to develop and implement and may lag behind the cutting edge of technology deployment, particularly when the industry is in transition, as is the case with smart-grid technologies. Therefore, these metrics may be more of a lagging rather than leading indicator of the security posture of the smart grid.

[1]See Critical Infrastructure Protection Standards at www.nerc.com.

Additionally, the interview form includes a question about specific security measures that utilities are implementing. The sample results are shown in Table M.18.2. While this represents useful information and can be valuable for trending, the questions themselves are too vague to ascertain what precisely is the security posture of the smart-grid technologies vis-à-vis more broad "enterprise-wide" security measures that are employed by the utility. Clarification may also be needed about the definitions and some additional detail regarding the effeteness of these security measures (for example, the presence of a firewall does not ensure that its rules are properly implemented).

Control systems evolved in an environment of implicit trust. A properly formatted command is carried out without question by the automatic controller. In this environment, security relies on isolation. Over the years, the electric utility industry built and operated its own private communications infrastructure to control the electric power grid, using systems and protocols unique to the industry. Noise, interference, and equipment reliability were primary issues to overcome. This isolation resulted in inherent security, but was expensive to implement and maintain. Because of this, the trend has been shifting toward the use of shared communication with public networks, open and commonly used protocols, and general-purpose operating systems whose many security weaknesses are more widely known. Economic forces and technology development are making the power system more dependent on information systems and associated communications networks, particularly in the context of smart-grid systems and their inclusion of demand-side resources. The interconnected nature of these communications systems and the need to continue supporting older legacy systems in parallel with newer generations of control systems further compound the complexity and challenges of addressing this problem.

In addition, data exchange interactions between businesses result in handing off data security responsibility at the interface between the interacting parties. Ensuring that information privacy is protected and that cyber-security vulnerabilities are addressed on either side of an interface requires a coordination of business processes, particularly when the data may transition to different technologies and protocols. Designed-in security approaches are only now emerging.

Unlike the threats from component failures, extreme weather, or natural disasters that are mitigated by highly effective and well-developed contingency and restoration practices, the cyber-threat landscape is only beginning to be effectively addressed through common industry standards and best practices.

M.18.3.1 Associated Stakeholders

- End users: Cyber-security breaches can greatly affect consumers, not only from disruptions when the electric infrastructure is compromised, but also because a smart grid incorporates participation by consumers' automation systems. Electricity-related information-technology connectivity may provide a new path for a cyber attack that might affect a facility's operation or obtain private information. Each consumer group needs to assess its vulnerability and develop an appropriate security posture.
- Electric service retailers and wholesale electricity traders: These entities connect to customer systems, market operators, and infrastructure system operators with greater linkages as smart grid trends progress. Security issues must be assessed across their operations with cooperation between all transacting business systems.

- Distribution and transmission service providers, balancing authorities, and reliability coordinators: The protection of the infrastructure is a national concern. The NERC CIP requirements, while modest, are being refined, with recognition for the importance of security.
- Products and services suppliers: Information technology, business systems, and engineering vendors have shown interest in developing or updating product offerings to address security needs. However, real change occurs when customers specify security features as requirements for their purchases.
- Energy policymakers and advocates: The idea that the electric infrastructure could be crippled by a cyber security breech is disconcerting to those protecting the public interest. Policymakers are searching for ways to ensure that cyber-security issues are addressed. For example, FERC is pushing NERC to strengthen the CIP standards, as the balance between cost, risk, and effective measures continues to mature.

M.18.3.2 Regional Influences

Approaches to cyber security should not vary greatly across nations. State-specific issues may arise because of different laws relating to transparency of information associated with Freedom of Information Act issues. For example, in California, a state-sponsored organization such as the California Independent System Operator may find it difficult to protect sensitive information from being disclosed because of state sunshine laws. There will also continue to be international and national standards in the cyber-security area that may compete in technology and policy approaches.

M.18.4.0 Challenges to Deployment

M.18.4.1 Technical Challenges

The electric system of the future could become much more vulnerable to disruption by skilled electronic intrusion originating either internally or externally. Compounding the problem, security is often neglected or introduced as an afterthought rather than being incorporated as a core component in the development and deployment of these new technologies and applications.

Because cyber security is largely a defensive practice when applied to protecting against a steady flow of active exploits, the threat to computer and control systems is never completely ameliorated. A vital need in the electricity industry is the development of new approaches for inherent security: components and systems with built-in security capabilities. Coordination is also needed between these approaches and techniques appearing in other industrial, commercial building, and residential systems that interact with the electric system.

Complexities and interdependencies are poorly understood. These include internal and external issues with the electricity infrastructure. Examples of internal interdependencies are market-based systems for buying, selling, and wheeling power throughout the network – while they are not directly connected to the control systems providing real-time operation of the grid, there are sometimes subtle dependencies that could cause reliability implications if security in these systems were compromised. An example of an external interdependency is reliance on other infrastructures, such as communication, that is vital to the operation of the electricity infrastructure. Systemic failures that propagate among these dependency seams can create failure modes that are difficult to predict and mitigate.

Finally, it is not clear whether there is general consensus among the industry stakeholders regarding the threat, which leads to inconsistent views regarding the appropriate level of attention and investment needed to achieve appropriate levels of security.

M.18.4.2 Business and Financial Challenges

The key challenge will be to maintain reliability in a vastly more "connected" electric industry under threats that could involve multiple, distributed, and simultaneous or cascading incidents – whether accidental or deliberate. Steps should be taken to enhance the security of real-time control systems using sound information security practices. In the future, all control systems for critical applications should be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.

All stakeholders share a common interest in deterrence, intrusion detection, security countermeasures, graceful degradation and emergency backup and rapid recovery. While the NERC CIP-002 through CIP-009 standards are an effective start to begin addressing cyber security and are achieving increased awareness and action within the electric utility industry, there is growing recognition that they have not yet achieved their ultimate purpose – defining uniform standards that if implemented can provide adequate security against cyber threats to the electric infrastructure. Problems with the standards include provisions for entities to self-define what they will protect and how they will protect it; this has resulted in a patchwork of mitigation measures that is more focused on compliance than security. In addition, there is concern that the standards have loopholes associated with communications and certain types of control systems. There is an urgent need to quickly address these issues with the adoption of new versions of these standards, but the standards development and approval process is literally measured in years. More work to transition the industry mindset from a culture of compliance to a culture of security needs to be done.

Another issue is inconsistent regulatory support that electric utilities have associated with cost recovery for necessary security enhancements. The electricity regulatory landscape is complex with multiple stakeholders at the federal, state, and local levels. Not all regulatory jurisdictions have recognized security as a recoverable cost, and other utilities are constrained in implementing security because it would cause preexisting rate cases to be reopened at great expense and risk to the company.

M.18.5.0 Recommendations for Future Measurement

A more mature evaluation of cyber security will evolve toward self-assessment tools to provide enduring capabilities for vendors, system integrators, and asset owners to afford appropriate security commensurate with the risk associated with the application. This will empower industry to be responsible for making reasoned and informed tradeoffs.

Fundamentally, systems will be required that are inherently secure and robust. Research and development will be needed to develop these systems. Metrics to measure their effectiveness will need to be defined.

PNNL, with ANL and INL, has been tasked by DOE to prepare a report for Congress with answers to the questions posed in Section 1309 of Title XIII of the Energy Independence and Security Act of 2007:

1. How can smart-grid systems help make the nation's electricity system less vulnerable to disruptions caused by intentional acts against the system?
2. How can smart-grid systems help restore the integrity of the nation's electricity system subsequent to disruptions?
3. How can smart-grid systems facilitate nationwide, interoperable emergency communications and control of the nation's electricity system during times of localized, regional, or nationwide emergency?
4. What risks must be taken into account because smart-grid systems may, if not carefully created and managed, create vulnerability to security threats of any sort, and how such risks may be mitigated?

This report will be prepared with industry input through the first half of Fiscal Year 2009, and will help provide greater clarity around cyber-security issues associated with smart-grid technologies with suggested metrics that should be useful for future reports of this nature.