



# Information Bulletin

## *Public Policy Division*

### *Impact of NIST Guidelines for Cybersecurity*

Prepared by

UTC Staff



# Information Bulletin

1. Introduction .....	3
2. Cybersecurity Landscape .....	3
3. One Likely Scenario .....	5
4. Draft NISTIR 7628, Guidelines for Smart Grid Cyber Security .....	6
5. What This Means to Utilities .....	9
6. Next Steps .....	10
7. Summary .....	11
Appendix A - Summary of NERC CIP Standards .....	13
Appendix B – Links .....	15

## NIST Cybersecurity Guidelines – Practical Impacts

---

### 1. Introduction

The release of *Guidelines for Smart Grid Cyber Security*<sup>1</sup>, draft version one, points to the pivotal role cybersecurity will play in the deployment and protection of the smart grid. The document draws from several years of effort by National Institute of Standard and Technology (NIST) staff and other efforts to secure Information Technology systems, and has been adapted for the smart grid by the Smart Grid Interoperability Panel Cyber Security Working Group (SGIP-CSWG). Version one is scheduled for publication on August 31, 2010. Security practices continue to evolve and the Guidelines document, like NIST's *Smart Grid Interoperability Roadmap*<sup>2</sup>, are considered "living documents". They will be updated as the industry matures and best practices are identified and refined.

The role of cybersecurity, and security in general, is well known in the industry; essentially we know "why" we need to protect our critical infrastructure from terrorists, hackers, disgruntled or poorly trained employees, and natural disasters. Unfortunately the regulatory structure to provide clear mandates in order to achieve the best protection possible is not so clear. Smart grid technology, along with standards and policies needed to ensure interoperability and resiliency, is still being developed. Utilities are missing clear "how to" guidelines that will protect their existing and next generation systems, meet developing state regulations in order to recover the costs of their investments, and provide confidence that smart grid deployments will provide the benefits to consumers and shareholders alike. And there are potential fines associated with non-compliance.

NIST Interagency Report (NISTIR) 7628 is intended to serve as a guide for utilities to prepare for cybersecurity issues related to the smart grid. Following a brief discussion of the current regulatory landscape, we examine the 400+ page NISTIR to extract a few high level recommendations to assist utilities in planning for their specific security needs in order to ensure future regulatory compliance.

### 2. Cybersecurity Landscape

The next generation of the electric grid challenges existing regulatory structure with incredibly innovative technology and equally advanced business models. Regulators struggle to keep up

---

<sup>1</sup> Draft available at <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTIR7628v1July2010>

<sup>2</sup> Available at [http://www.nist.gov/public\\_affairs/releases/upload/smartgrid\\_interoperability\\_final.pdf](http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf)

## NIST Cybersecurity Guidelines – Practical Impacts

---

with technologies as they continue to protect consumer's rights and privileges. With respect to cybersecurity, a high level review of entities seeking to influence and mandate standards will shed light on how utilities should handle this complex issue.

a. **North American Electric Reliability Corporation**

The North American Electric Reliability Corporation (NERC) jurisdiction extends to the bulk power system, not the distribution network. NERC has mandatory reliability standards related to the bulk power system, including the Critical Infrastructure Protection (CIP) standards. NERC-CIP is a suite of regulatory requirements for security numbered 002-009 that depend on the definition of critical assets. The appendix provides a breakdown of the topics addressed in these standards. NERC CIP 002 deals specifically with the definition of critical cyber assets. Engineers, cyber experts and policy analysts seek to release a version 4 of this NERC suite of standards as soon as possible, but several factors have delayed the process.

The NERC process has been severely criticized on Capitol Hill. As engineers struggle to complete the long overdue next version of NERC CIP, Congress remains critical over the final product and if NERC CIP 2, version 4, is deemed insufficiently rigorous to protect the grid, NERC's authority over this part of the grid could shift to Federal Energy Regulatory Commission.

b. **Federal Energy Regulatory Commission**

The Federal Energy Regulatory Commission (FERC) is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil. FERC has authority over anything that could impact the reliability of the bulk power system (including distribution companies). In 2008, FERC approved eight new mandatory CIP reliability standards to protect the nation's bulk power system against potential disruptions from cybersecurity breaches<sup>3</sup>.

Currently, FERC has limited ability to mandate standards for use in the bulk power grid. However, if the NERC CIP 2 version 4 standards, assuming they are approved, are inadequately stringent, in the view of Congress, it serves up the issue to the House and Senate on a silver platter to enact additional authority to FERC to mandate standards

---

<sup>3</sup> See <http://www.ferc.gov/media/news-releases/2008/2008-1/01-17-08-E-2.asp>

## NIST Cybersecurity Guidelines – Practical Impacts

---

directly. Several bills circulating through Congress, including the Grid Act, are proposing to do just that.

There are other organizations weighing in as well. The United States Department of Energy (DOE), in cooperation with Howard Schmidt, the White House Cybersecurity Coordinator, has drawn up a set of cybersecurity principles for the electric industry and smart grid. Department of Homeland Security (DHS) Secretary Janet Napolitano included cybersecurity as one of the top five missions of the department, and is seriously toughening its cybersecurity division. Each of the 19 DHS critical infrastructure sectors is designing its own security “roadmaps” specific to its area of responsibility. The first step in planning for compliant smart grid deployments is to understand this regulatory regime and its dynamic nature.

### 3. One Likely Scenario

The point of the regulatory discussion above is that there is no clear path yet to regulatory certainty. Waiting for regulatory certainty puts utilities at a disadvantage when the administration and the Department of Energy are handing out stimulus grants. Those that choose a path, right or wrong, are the ones getting the money because that is a requirement for receiving the grant. In the ecosystem of smart grid cybersecurity regulatory oversight, there are two major contenders: NERC and FERC. NERC will come out on top if the revised NERC CIP mandates are adopted quickly and will win Congressional support if Congress considers them sufficiently stringent. Some of the main Congressional criticisms of the NERC process appear close to resolution. NERC CIP may incorporate portions of the NISTIR that make sense.

Many believe the top contender is FERC. If Congress has its way, the agency will receive authority to mandate standards, over NERC’s existing authority and the cyber security mandates will be pushed down to those parts of the distribution system which could potentially impact the reliability of the bulk power system. And now, it appears that the likely source of FERC cybersecurity mandates will be some edited form of the NISTIR. The NIST staff point person and former chair of the CSWG, security veteran Annabelle Lee, has elected to leave NIST for a position at FERC. We let the reader draw their own conclusions from this move. But, if some form of the NISTIR is likely to be mandated by FERC, it would benefit utilities to understand the document and guidelines it lays out.

## NIST Cybersecurity Guidelines – Practical Impacts

---

### 4. Draft NISTIR 7628, Guidelines for Smart Grid Cyber Security

The NISTIR is intended to be a tool that allows utilities to conduct their own high level risk assessment of their smart grid deployment, identifying cyber security vulnerabilities. The information included in this document is **baseline guidance** for organizations. NIST is not prescribing particular solutions through the guidance contained in this document. Each organization must develop its own cybersecurity strategy (including a risk assessment methodology) for the Smart Grid.<sup>4</sup>

The security requirements and the supporting analysis included in this NIST report may be used by implementers of the Smart Grid (e.g., utilities, equipment manufacturers, regulators) as input to their risk assessment and mitigation processes. The information serves as baseline guidance to the various organizations for assessing risk and selecting appropriate security requirements. NIST is not prescribing particular solutions to cyber security issues through the guidance contained in this document. Each organization must develop its own cyber security strategy for the Smart Grid recognizing the unique situations presented by its current platform and its target architecture<sup>5</sup>.

The NISTIR simplifies the “what” in cybersecurity at a very high level to be five steps:

1. Selection of use cases with cybersecurity concern or potential impact.
2. Performance of a risk assessment.
3. Specification of high level security requirements.
4. Development of a logical reference model/Standards Assessment.
5. Conformity Analysis.

To consider the NISTIR a tool, utilities and vendors will apply the same processes the NIST team used to develop the guidelines with their own smart grid implementations.

The common theme in smart grid implementation is to divide this complex entity into manageable chunks. Each chunk is reviewed for security and functionality, and then the connections between the chunks are evaluated to create a functional, secure smart grid. The NISTIR includes diagram that could assist in the process:

---

<sup>4</sup> Draft NISTIR 7628, Executive Summary, July 2010

<sup>5</sup> Draft NISTIR 7628, Chapter One, July 2010



## NIST Cybersecurity Guidelines – Practical Impacts

---

specific tasks within this strategy.

**Chapter 2 – *Logical Architecture*** includes a high level diagram that depicts a composite high level view of the actors within each of the Smart Grid domains and includes an overall logical reference model of the Smart Grid, including all the major domains. The chapter also includes individual diagrams for each of the 22 logical interface categories. This architecture focuses on a short-term view (1–3 years) of the Smart Grid.

**Chapter 3 – *High Level Security Requirements*** specifies the high level security requirements for the Smart Grid for each of the 22 logical interface categories included in Chapter 2.

**Chapter 4 – *Cryptography and Key Management*** identifies technical cryptographic and key management issues across the scope of systems and devices found in the Smart Grid along with potential alternatives.

**Appendix A – *Crosswalk of Cyber Security Documents***

**Appendix B – *Example Security Technologies and Procedures to Meet the High Level Security Requirements***

### **Volume 2 – Privacy and the Smart Grid**

**Chapter 5 – *Privacy and the Smart Grid*** includes a privacy impact assessment for the Smart Grid with a discussion of mitigating factors. The chapter also identifies potential privacy issues that may occur as new capabilities are included in the Smart Grid.

**Appendix C – *State Laws – Smart Grid and Electricity Delivery***

**Appendix D – *Privacy Use Cases***

**Appendix E – *Privacy Related Definitions***

### **Volume 3 – Supportive Analyses and References**

**Chapter 6 – *Vulnerability Classes*** includes classes of potential vulnerabilities for the Smart Grid. Individual vulnerabilities are classified by category.

**Chapter 7 – *Bottom-Up Security Analysis of the Smart Grid*** identifies a number of specific security problems in the Smart Grid. Currently, these security problems do not have specific solutions.

**Chapter 8 – *Research and Development Themes for Cyber Security in the Smart Grid*** includes R&D themes that identify where the state of the art falls short of meeting the envisioned functional, reliability, and scalability requirements of the Smart Grid.

**Chapter 9 – *Overview of the Standards Review*** includes an overview of the process that is being used to assess standards against the high level security requirements included in this report.

**Chapter 10 – *Key Power System Use Cases for Security Requirements*** identifies key use cases that are architecturally significant with respect to security requirements for the Smart Grid.

**Appendix F – *Logical Architecture and Interfaces of the Smart Grid***

**Appendix G – *Analysis Matrix of Interface Categories***

## NIST Cybersecurity Guidelines – Practical Impacts

---

### **Appendix H – Mappings to the High Level Security Requirements**

### **Appendix I – Glossary and Acronyms**

### **Appendix J – SGIP-CSWG Membership**

As a tool, the NISTIR is valuable in two ways. First, the document embraces a methodology that can be applied to any smart grid solution, large or small. Because the document specifically is not intended to provide the “how” for specific cybersecurity issues, as long as the process used to define problems and recommend solutions, compliance with any resulting regulations can be demonstrated. Second, the document provides sufficient recommendations for existing, known vulnerabilities that allow vendors to create compliant solutions. Utilities that purchase smart grid systems have criteria that can be used to measure a vendor’s solution against the base metric of the NISTIR recommendations.

Specific areas of concern identified in the document include a lengthy discussion of customer data privacy, with specific recommendations on what needs to be done to protect customer data. Another area of concern is encryption and the resources needed to allow device to device authentication within the grid. The resulting security key management could be massive; this is also recommended as an area of further research. Finally, software development practices are cited as the source of many vulnerabilities and specific attention is paid to defining vulnerabilities such as hidden back door access to systems, hard coded and weak passwords, and open debugging ports.

## **5. What This Means to Utilities**

The NISTIR provides a far more granular definition of “what” needs to be done to protect the smart grid from cyber and system failure threats, but provides little, if any “how to” guidelines. As a practical matter, if one makes a few relatively logical conclusions, we can interpret the impact of the NISTIR and cybersecurity regulation on utilities seeking to deploy compliant smart grid solutions.

The assumption we make is that cybersecurity regulations will be imposed on the overall smart grid and will extend from generation to the metering systems and home energy networks that interact with consumers. Either NERC or FERC will have the authority to mandate the cybersecurity protections with the likely winner being FERC. FERC will likely adopt portions of the NISTIR as its cybersecurity roadmap, hopefully with a comment period to allow interested parties to weigh in. The states may also have jurisdictional authority over the distribution networks.

What makes this scenario troubling is that the NISTIR defines a process, not necessarily a solution. It defines “what” but not “how”. There are baseline security practices that utilities should have been using years ago, but the biggest question is how this process will be converted

## NIST Cybersecurity Guidelines – Practical Impacts

---

to regulation, with specific, defined procedures for compliance. Utilities will demand this clarity of oversight if millions of dollars in upgrades as well as millions of dollars in fines are at stake.

Utility impact can be sorted into categories of “present” and “future”. The immediate impact, the present, necessitates utilities to review existing generation, transmission and distribution systems for known vulnerabilities using the “bottom up” analysis in chapters seven and eight of the NISTIR. As the systems are identified and categorized, risk assessment is applied to the configuration and potential solutions are identified and implemented.

For the future, the key to compliance is a unified vision of the smart grid deployment, a process to ensure metrics are met and an ongoing conformance program. The vision of the smart grid should be constructed using the conceptual models available in the industry today and include close cooperation between communications, power and information technology personnel. The conceptual model has become a common language in the smart grid industry and drawing on this resource allows utilities to communicate their needs to vendors that must provide compliant solutions.

### 6. Next Steps

Given the amount of regulatory uncertainty surrounding smart grid cybersecurity protection, utilities ask themselves what they can do to prepare. Some things utilities can do immediately are<sup>7</sup>:

- a. **Create a living definition of the utility’s smart grid vision** and specifically define which components of the Smart Grid Reference Architecture that will be implemented. If the utility has no generation and transmission functions, for example, these aspects of the reference model need not be addressed.
- b. **Develop a security architecture** leveraging industry reference architectures for a holistic solution
- c. **Create a clear customer data privacy vision** that can be used early in the process. This will define some of the IT security controls needed in the implementation.

---

<sup>7</sup> See UTC Webinar dated July 29, 2010: Understanding the New Draft Guidelines for Smart Grid Cyber Security from the National Institute of Standards and Technology, presented by David Dalva of Cisco, Inc.

## NIST Cybersecurity Guidelines – Practical Impacts

---

- d. **Establish corporate governance of the smart grid projects** to act as a central source for design, planning and implementation. Include all necessary departments to create a team. Ensure that all new capital projects be coordinated through the smart grid team in order to promote interoperability.
- e. **Initiate risk assessment analysis on existing grid deployments.** Fixing existing problems should be considered at the same time new technologies are being evaluated.
- f. **Define appropriate remediation** (people, process, technology) to address the assessment gaps
- g. **Create a template for equipment procurement** that specifically addresses cybersecurity issues, including software development procedures and other known vulnerabilities.
- h. If necessary, hire a consultant to assist in developing a security posture
- i. **Establish/extend a cross-functional Cyber Network Operations Center** to manage the operations of converged energy & information and communication technology grid assets
- j. **Engage in standards development**, industry information exchanges and best practice sharing

### 7. Summary

The NISTIR is a powerful tool in ensuring the security and resiliency of the smart grid. Combined with the NERC CIP documents, utilities have a relatively clear definition of what to do. Some utilities will use the NISTIR directly to create request for proposals that specifically identify requirements and mandate that vendors define their solutions.

But for utilities that do not have the resources to create their own RFPs, consultants will develop templates for this purpose and assist utilities in choosing solutions that will meet regulations and ensure rate recovery. Vendors, some of whom had a hand in creating the NISTIR, will develop products with guidance from the NISTIR.

The impact of the NISTIR is clear: cybersecurity is a cross cutting issue that must be considered



## NIST Cybersecurity Guidelines – Practical Impacts

---

in all aspects of smart grid design and deployment. Cybersecurity cannot be ignored in specifying new products and services for the grid and failure to do so will likely cause denial of rate recovery. Utilities need to create a vision, then create a plan, and then constantly recheck the assumptions in the plan to make sure they remain valid.

Compliance is a process.

## NIST Cybersecurity Guidelines – Practical Impacts

### Appendix A - Summary of NERC CIP Standards

Number	Title/Summary	Date	
CIP-001-1	<a href="#"><u>Sabotage Reporting</u></a>	11.01.2006	<a href="#"><u>pdf</u></a>
CIP-001-1a	<a href="#"><u>Sabotage Reporting</u></a>	02.16.2010	<a href="#"><u>pdf</u></a>
CIP-002-1	<a href="#"><u>Critical Cyber Asset Identification</u></a> NERC Standards CIP-002 through CIP-009 provides a cybersecurity framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.	05.02.2006	<a href="#"><u>pdf</u></a>
CIP-002-2	<a href="#"><u>Cyber Security - Critical Cyber Asset Identification</u></a>	05.06.2009	<a href="#"><u>pdf</u></a>
CIP-002-3	<a href="#"><u>Cyber Security - Critical Cyber Asset Identification</u></a>	12.16.2009	<a href="#"><u>pdf</u></a>
CIP-003-1	<a href="#"><u>Security Management Controls</u></a>	05.02.2006	<a href="#"><u>pdf</u></a>
CIP-003-2	<a href="#"><u>Cyber Security - Security Management Controls</u></a>	05.06.2009	<a href="#"><u>pdf</u></a>
CIP-003-3	<a href="#"><u>Cyber Security - Security Management Controls</u></a>	12.16.2009	<a href="#"><u>pdf</u></a>
CIP-004-1	<a href="#"><u>Personnel &amp; Training</u></a>	05.02.2006	<a href="#"><u>pdf</u></a>
CIP-004-2	<a href="#"><u>Cyber Security - Personnel &amp; Training</u></a>	05.06.2009	<a href="#"><u>pdf</u></a>
CIP-004-3	<a href="#"><u>Cyber Security - Personnel &amp; Training</u></a>	12.16.2009	<a href="#"><u>pdf</u></a>
CIP-005-1	<a href="#"><u>Electronic Security Perimeter(s)</u></a>	05.02.2006	<a href="#"><u>pdf</u></a>
CIP-005-1a	<a href="#"><u>Electronic Security Perimeter(s)</u></a>	02.16.2010	<a href="#"><u>pdf</u></a>
CIP-005-2	<a href="#"><u>Cyber Security - Electronic Security Perimeter(s)</u></a>	05.06.2009	<a href="#"><u>pdf</u></a>
CIP-005-2a	<a href="#"><u>Cyber Security - Electronic Security Perimeter(s)</u></a>	02.16.2010	<a href="#"><u>pdf</u></a>
CIP-005-3	<a href="#"><u>Cyber Security - Electronic Security Perimeter(s)</u></a>	12.16.2009	<a href="#"><u>pdf</u></a>
CIP-006-1	<a href="#"><u>Physical Security of Critical Cyber Assets</u></a>	05.02.2006	<a href="#"><u>pdf</u></a>
CIP-006-1a	<a href="#"><u>Physical Security of Critical Cyber Assets</u></a>	02.12.2008	<a href="#"><u>pdf</u></a>
CIP-006-1b	<a href="#"><u>Physical Security of Critical Cyber Assets</u></a>	08.05.2009	<a href="#"><u>pdf</u></a>
CIP-006-1c	<a href="#"><u>Physical Security of Critical Cyber Assets</u></a>	02.16.2010	<a href="#"><u>pdf</u></a>
CIP-006-2	<a href="#"><u>Cyber Security - Physical Security of Critical Cyber Assets</u></a>	05.06.2009	<a href="#"><u>pdf</u></a>
CIP-006-2c	<a href="#"><u>Cyber Security - Physical Security of Critical Cyber Assets</u></a>	02.16.2010	<a href="#"><u>pdf</u></a>
CIP-006-3	<a href="#"><u>Cyber Security - Physical Security of Critical Cyber Assets</u></a>	12.16.2009	<a href="#"><u>pdf</u></a>



## NIST Cybersecurity Guidelines – Practical Impacts

---

CIP-007-1	<a href="#"><u>Systems Security Management</u></a>	05.02.2006	<a href="#"><u>pdf</u></a>
CIP-007-2a	<a href="#"><u>Cyber Security - Systems Security Management</u></a>	11.05.2009	<a href="#"><u>pdf</u></a>
CIP-007-3	<a href="#"><u>Cyber Security - Systems Security Management</u></a>	12.16.2009	<a href="#"><u>pdf</u></a>
CIP-008-1	<a href="#"><u>Incident Reporting and Response Planning</u></a>	05.02.2006	<a href="#"><u>pdf</u></a>
CIP-008-2	<a href="#"><u>Cyber Security - Incident Reporting and Response Planning</u></a>	05.06.2009	<a href="#"><u>pdf</u></a>
CIP-008-3	<a href="#"><u>Cyber Security - Incident Reporting and Response Planning</u></a>	12.16.2009	<a href="#"><u>pdf</u></a>
CIP-009-1	<a href="#"><u>Recovery Plans for Critical Cyber Assets</u></a>	05.02.2006	<a href="#"><u>pdf</u></a>
CIP-009-2	<a href="#"><u>Cyber Security - Recovery Plans for Critical Cyber Assets</u></a>	05.06.2009	<a href="#"><u>pdf</u></a>
CIP-009-3	<a href="#"><u>Cyber Security - Recovery Plans for Critical Cyber Assets</u></a>	12.16.2009	<a href="#"><u>pdf</u></a>



## NIST Cybersecurity Guidelines – Practical Impacts

---

### Appendix B – Links

NISTIR 7628 Guideline for Smart Grid Cybersecurity Document:

[http://www.nist.gov/public\\_affairs/releases/smartgrid\\_interoperability\\_final.pdf](http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf)

NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009: [http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final\\_updated-errata\\_05-01-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf)

Catalog of Control Systems Security: Recommendations for Standards Developers, Department of Homeland Security, March 2010: [http://www.us-cert.gov/control\\_systems/pdf/Catalog\\_of\\_Control\\_Systems\\_Security\\_Recommendations.pdf](http://www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf)

Federal Energy Regulatory Commission, Smart Grid Policy:

<http://www.ferc.gov/industries/electric/indus-act/smart-grid.asp>

NIST SP 800-39, DRAFT Managing Risk from Information Systems: An Organizational Perspective, April 2008; <http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-39>

NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, NIST, March 2006:

<http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, NIST, February 2004: <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment, North American Electric Reliability Corporation (NERC), 2002:

<http://www.esisac.com/publicdocs/Guides/V1-SensitiveData.pdf>

The National Infrastructure Protection Plan, Partnering to enhance protection and resiliency, Department of Homeland Security, 2009: [http://www.dhs.gov/files/programs/editorial\\_0827.shtm](http://www.dhs.gov/files/programs/editorial_0827.shtm)

[ANSI/ISA-99.00.01-2007](#), *Security for Industrial Automation and Control Systems: Concepts, Terminology and Models*, International Society of Automation (ISA), 2007;



Information Bulletin  
Date: August 25, 2010

## NIST Cybersecurity Guidelines – Practical Impacts

---

[ANSI/ISA-99.02.01-2009](#), *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*, ISA, January 2009.

The IT, telecommunications, and energy sector-specific plans (SSPs), initially published in 2007 and updated annually: [http://www.dhs.gov/files/programs/gc\\_1179866197607.shtm](http://www.dhs.gov/files/programs/gc_1179866197607.shtm)

SECURITY PROFILE FOR ADVANCED METERING INFRASTRUCTURE (UCA AMI-Sec):

[http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/AMI%20Security%20Profile%20\(ASA-P-SG\)/AMI%20Security%20Profile%20-%20v2\\_0.pdf](http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/AMI%20Security%20Profile%20(ASA-P-SG)/AMI%20Security%20Profile%20-%20v2_0.pdf)

Electronic Communications Privacy Act; 18 U.S.C. § 2510. See

[http://www.law.cornell.edu/uscode/18/usc\\_sup\\_01\\_18\\_10\\_I\\_20\\_119.html](http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I_20_119.html)

OECD “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” at

[http://www.oecd.org/document/20/0,3343,en\\_2649\\_34255\\_15589524\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html)