Asia-Pacific
Economic Cooperation

Cyber-Energy Nexus Study

Best Practices, Opportunities, and Challenges for Smart Energy Technology

Energy Working Group

July 2016

APEC Project No: EWG 02 2014S

Cyber-Energy Nexus Study
Best Practices, Opportunities, and Challenges for Smart Energy Technology

Report prepared for the APEC Energy Working Group by:

Luis A. Mendoza
Cyber Physical Security
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0757

Michael Mylrea
Electricity Infrastructure - Cybersecurity
Pacific Northwest National Laboratory
Michael.Mylrea@pnnl.gov
902 Battelle Boulevard
Richland, WA 99352

Caitriona Helena Heinl
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Blk S4, Level B4
Nanyang Avenue, Singapore 639798

For
APEC Secretariat
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 68919 600 Fax: (65) 68919 690
Email: info@apec.org Website: www.apec.org

APEC# 216-RE-01.14

Cyber-Energy Nexus Study

Best Practices, Opportunities, and Challenges for Smart Energy Technology

Luis A. Mendoza
Cyber Physical Security
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0757

Michael Mylrea
Electricity Infrastructure
Cybersecurity & Resilience
Pacific Northwest National Laboratory
902 Battelle Boulevard
Richland, WA 99352

Caitriona Helena Heinl
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Avenue, Singapore 639798

Abstract

Smart energy technology and networked control systems are becoming integral parts of the energy value chain globally. These critical energy infrastructure assets are vulnerable to cyber and physical attacks and lack secure interoperability policies and standards. The U.S. Department of Energy, together with Singapore Energy Market Authority, led the first Asia-Pacific Economic Cooperation (APEC) study exploring smart energy technology cyber security trends, policies and standards in the region. The study was conducted as part of the Energy Smart Communities' Initiative (ESCI) smart grid pillar with six primary goals: (1) define the cyber-energy nexus landscape, (2) identify relevant standards and current policy gaps in standards development, (3) share best policy practices, (4) identify related opportunities and challenges, (5) provide guidance to help APEC economies implement cyber-energy nexus plans in ways that optimize shared security and interoperability goals, and (6) add to the ESCI Knowledge Sharing Platform's resource links and case studies.

This page intentionally left blank.

Acknowledgments

We would like to thank a number of energy and cyber experts that made this report possible: Dr Phyllis Yoshida, Deputy Assistant Secretary, Office of International Affairs, U.S. Department of Energy and Tom Cutler, CEO, Cutler International LLC, for giving impetus to the study's launch; Elena Thomas-Kerr, the U.S. APEC Lead, for providing valuable guidance throughout the study; and Dr Carol Hawk, Director for Research & Development, Office of Electricity, U.S. Department of Energy for her support in bolstering the cyber defenses of our Nation's energy infrastructure and systems. Lastly, Dr Cary Bloyd, Senior Staff Scientist with the Electricity Infrastructure and Buildings Division of Pacific Northwest National Laboratory for sharing his valuable technical expertise and deep insight into APEC's energy landscape.

This page intentionally left blank.

Contents

Figures

Tables

This page intentionally left blank.

Executive Summary

The cyber-energy nexus landscape is rapidly evolving in the Asia Pacific Region as smart energy technology continues to be networked and incorporated into Asia-Pacific Economic Cooperation (APEC) Member Economies' energy infrastructure. If APEC Member Economies are to optimize energy infrastructure through increased interconnectivity, energy efficiency, conservation and renewable energy integration, they need to adopt additional standards to increase smart grid interoperability and security. APEC Member Economies could help overcome these standards gaps through a wider adoption of cyber security and interoperability policies.

The cyber energy nexus presents many energy security opportunities as well as challenges. If security is prioritized in the development, implementation and maintenance of the grid, smart energy technology opportunities such as increased use of renewable energy, increased reliability, visualization and conservation will vastly outweigh the cyber security challenge.

The future of smart energy technology, however, is not yet a foregone conclusion and many challenges remain. This study's results are intended to help APEC economies better understand interoperability opportunities and related cyber challenges in order to realize shared energy security, trade and economic goals. This report covers the following topics:

- Opportunities for Cooperation
- Industry Standards and Best Practices
- Cybersecurity Programs and Organizations
- Framework Implementation Guidance
- Asia-Pacific Economic Cooperation Member Economies
- Challenges
- Recommendations
- Additional Resources

This study is an initial effort to identify relevant standards and current cyber-energy security policies to help begin to address gaps in standards development and their application. This effort sets the stage for a potentially much larger effort involving industry partners, more extensive communication among APEC entities, and discussion of technical mitigations plans.

Several general observations and findings include:

1) The cyber threat to energy systems and infrastructure in APEC continues to increase, threatening economic and national security.

2) Increased situational awareness of the cyber threat and mitigation solutions would be facilitated by increased public information sharing by government and industry on

relevant policies. This study finds that, in some instances, it is unclear what cybersecurity policies and initiatives are in place to secure critical energy infrastructure. Public messaging on the importance of securing the cyber-energy nexus is imperative. Japan has specifically noted, for example, that no vulnerabilities is in the interest of all given the cascading effects on others when damage occurs in one economy, including the impacts on the supply chain. In particular, in terms of the energy sector, it is worth reemphasizing the interdependence of the global economy.

3) The APEC Member Economy reports highlight several examples of cybersecurity efforts that seem successful and could be adopted by others as best practice policy and models. They can be adapted to suit specific economy requirements as necessary. In addition, the issue is evolving and there is much space for developing initiatives even further. Examples include, amongst others, the SmartGrid Canada (SGC) Canadian Smart Grid Repository; the Ontario Information & Privacy Commissioner's 2011 report titled "Operationalizing Privacy by Design: The Ontario Smart Grid Case Study"; Japan's "Basic Policy of Critical Information Infrastructure Protection (3rd Edition)" published in May 2014; and, the recently established New Zealand Smart Grid Forum (NZSGF) which will report to the Minister every six months and provide recommendations. The NZGF believes there is a considerable advantage in using a broad representative model from across the power sector. In addition, APEC Member Economies could learn and copy its first highly useful deliverable of a "stock take of smart grid activity". Finally, the 2015 U.S. DOE Office of Electricity Delivery and Energy Reliability "Energy Sector Cybersecurity Framework Implementation Guidance" as well as the 2014 U.S. National Institute of Standards and Technology Cybersecurity Framework offer insights and lessons.

4) This study finds a number of APEC Member Economies are adopting different aspects of some international cybersecurity risk management processes including International Organization for Standardization (ISO) 31000:2009, ISO/IEC 27005:2011, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39 and the *Electricity Subsector Cybersecurity Risk Management Process* (RMP) guideline. APEC Member Economies should consider increasing their adoption of, and build upon, these standards, guidelines, and practices in securing critical energy infrastructure from cyber threats.

5) This study finds that the 2014 "Forging a Common Understanding for Critical Infrastructure" document, which outlines the shared views of the Critical 5 members (Australia, Canada, New Zealand, the United Kingdom, and the United States), provides a high-level overview of the meaning and importance of critical infrastructure, including the energy sector. It is a good practice model that outlines an approach to find common understanding of critical infrastructure. This work could provide a good first step to then assist in developing peacetime norms that place critical infrastructure off limits for cyber attacks as called for in February 2015 by Australia's Foreign Minister Julie Bishop. In

addition, the study finds that Japan is a particularly interesting case since smart grids and smart cities are specifically cited in its national cybersecurity strategy.

This study further finds that the threat to critical energy infrastructure posed by cyber threats is a common concern for all APEC Member Economies that should incentivize cooperation. The study specifically outlines several related measures already being undertaken within several regional forums.

6) This study finds that regularly updated, national-level repositories that are made public or regular stocktakes that are then published would be a useful addition of open source documents to the ESCI Knowledge Sharing Platform. However, it will also be important to keep the information up to date as developments relating to cybersecurity initiatives and cybersecurity measures in APEC are occurring increasingly frequently.

7) This study finds that the lack of skills both in the domain of cybersecurity and smart grids seems to be common to the vast majority of APEC members.

8) While many initiatives are in the pilot or test phase, cybersecurity measures such as security and data privacy by design should be put in place as early as possible while also ensuring that innovation or the introduction of new technologies is not disproportionately suppressed. For instance, such energy technology may be commercially attractive, especially for those Member Economies with visions of exporting related energy and smart grid technologies. However, for long-term commercial attractiveness, cybersecurity and data privacy/data protection concerns should be fully addressed.

9) A follow up study would provide considerable value in conducting a deeper dive examining APEC's cyber-energy nexus landscape and could: 1) describe the current cybersecurity posture; 2) describe their target state for cybersecurity; 3) identify and prioritize opportunities for improvement within the context of a continuous and repeatable process; 4) assess progress toward the target state; and, 5) communicate to both internal and external stakeholders about cybersecurity risk.

This page intentionally left blank.

Nomenclature

ANSI	American National Standards Institute
APEC	Asia-Pacific Economic Cooperation
C2M2	Cybersecurity Capability Maturity Model
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIKR	Critical Infrastructure and Key Resources
CIP	Critical Infrastructure Protection
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off the Shelf
CSSWG	U.S. Cyber Systems Security Working Group
DCS	Distribution Control Systems
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
DSM	Demand Side Management
ECP	Entry Control Point
EEI	Edison Electric Institute
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
EMS	Energy Management System
ERO	Electric Reliability Organization
ES	Electricity Subsector
ESCI	Energy Smart Communities Initiative
ESCC	U.S. Electricity Subsector Coordinating Council
EV	Electric Vehicle
EWG	APEC Energy Working Group

FERC	U.S. Federal Energy Commission
FIPS	Federal Information Processing Standards
ICS	Industrial Control System
ICT	Information and Communication Technology
IEC	International Electro Technical Commission
IEEE	Institute of Electrical and Electronics Engineers
INPO	Institute of Nuclear Power Operations
IP	Internet Protocol
ISMO	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
JSARs	Joint Security Awareness Reports
LAN	Local Area Network
MMS	Manufacturing Message Specification
NATF	North American Transmission Forum
NCCIC	U.S. National Cybersecurity and Communication Integration Center
NERC	North American Electric Reliability Corporation
NIAC	U.S. National Infrastructure Advisory Council
NIST	U.S. National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NNCEIP	Non-Nuclear Critical Energy Infrastructure Protection
ONG SCC	U.S. Oil & Natural Gas Subsector Coordinating Council
OSCE	Organization for Security and Co-operation in Europe
PACRAT	Physical and Cyber Risk Analysis Tool
PLC	Programmable Logic Controller
PV	Photovoltaic

R&D	Research and Development
RMP	Risk Management Process
SC	Subcommittee
SCADA	Supervisory Control and Data Acquisition
SGCC	Smart Grid Cybersecurity Committee
SGIP	Smart Grid Interoperability Panel
SGTCC	Smart Grid Testing and Certification Committee
SHA	Security Hash Algorithm
SMB	Standardization Management Board
SNL	Sandia National Laboratories
T&D	Transmission and Distribution
TC	Technical Committee
TCP/IP	Transmission Control Protocol / Internet Protocol
UML	Unified Modeling Language
WG	Working Group
XML	Extensible Markup Language

This page intentionally left blank.

1 Introduction

Smart energy technology and networked control systems from smart grid systems to building controls are becoming integral parts of the energy value chain.[1] These critical energy infrastructure assets are vulnerable to cyber and physical attacks. They also lack fully optimized and secure interoperability policies and standards. The United States, together with Singapore and Canada, are leading the effort under the Asia-Pacific Economic Cooperation (APEC) Energy Smart Communities' Initiative (ESCI) smart grid pillar to study international policies and standards. The results are intended to help APEC Member Economies understand interoperability opportunities and related cyber challenges in order to realize APEC's shared energy security, trade and economic goals.

1.1 Project Goals

The study has six primary goals:

1. Define the cyber-energy nexus landscape.
2. Identify relevant standards and current policy gaps in standards development.
3. Share best policy practices.
4. Identify related opportunities and challenges.
5. Provide guidance to help APEC economies implement cyber-energy nexus plans in ways that optimize shared security and interoperability goals.
6. Build the ESCI Knowledge Sharing Platform's resource links and case studies to promote increased understanding of cyber-energy nexus issues.

1.2 Project Scope

This study seeks to identify relevant standards and current policy in cyber-energy security to help address gaps in standards development and their application in the 21 APEC Member Economies. It is intended to provide best policy practices and guidance to identify related opportunities and challenges, and suggest an initial framework for how the APEC Member Economies can work together to improve their security posture and awareness as well as increase their understanding of cyber-energy nexus issues. This study sets the stage in anticipation of a potential larger effort involving industry partners, extensive communication among APEC entities, and discussion of technical mitigation plans.

1.3 Project Methodology

The methodology used to accomplish each of the goals is described below.

[1] For this project, networked control systems will be defined generally as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) as defined by NIST SP 800-82: Accessed at **http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf**

1. Define the cyber-energy nexus landscape.

- Collect, aggregate and analyze open source research defining energy-cyber nexus landscape.
- Develop a survey form and/or collect open source related information and documents highlighting the energy-cyber nexus landscape in the 21 APEC Member Economies.
- Determine gaps in the available research, request survey feedback from the APEC Energy Working Group (EWG), and collect data to fill in the gaps.
- Determine how APEC Member Economies define cybersecurity, critical infrastructure protection, and critical energy assets.

2. Identify relevant standards and current gaps in standards development.

- Analyze open source data and responses, and fill in critical energy-cyber asset lists based on NERC (North American Electric Reliability Corporation)-Critical Infrastructure Protection (CIP) and National Institute of Standards and Technology (NIST) guidelines; define critical energy-cyber assets.
- Determine some of the interoperability protocols and standards, such as smart grid communications standards.
- Determine what the most popular interoperability standards are in the Asia Pacific region. What are ongoing and future plans for networked energy infrastructure in the Asia Pacific region?
- Analyze open source data and responses, and fill in critical cyber-energy standards lists.
- Determine the major standards guiding energy-cyber nexus in APEC Member Economies. Where are the gaps? What standards can be shared that will help an energy infrastructure be more secure?
- List publicly reported cyber-energy nexus incidents in each Member Economy: have there been any documented physical or cyber-attacks on energy infrastructure? If so, document and site sources.

3. Share best policy practices.

- List best policy practices for cyber-energy nexus globally, including industrial control systems, smart grid, and security.
- The United States can share document resources with APEC Member Economies to help secure their cyber-energy nexus assets as well as make them more interoperable and efficient as an example and first step.

4. Identify related opportunities and challenges

- List cyber-energy nexus opportunities and challenges in each APEC Member Economy.

- Determine trade opportunities for networked or smart energy infrastructure in the Asia-Pacific region.
- Develop best practice technical guidance based on survey feedback, current standards, existing best practice data, and other research.
- Develop an initial cyber-energy nexus framework to help APEC optimize shared security, efficiency and interoperability goals.

5. Provide guidance to help APEC Member Economies implement cyber-energy nexus plans in ways that optimize shared security, efficiency and interoperability goals.

- Recommend ways to make the cyber-energy nexus secure, efficient and interoperable.
- Analyze the trade, investment, and economic opportunities. What is the estimated smart grid investments needed in the Asia-Pacific region to 2020? Who are the leaders and laggards? How are interconnected and networked grids being secured?

6. Build the ESCI Knowledge Sharing Platform's resource links and case studies to promote increased understanding of cyber-energy nexus issues.

- Collect and share resource links, Microsoft® PowerPoint files, and PDF files through the online data bank.

2 Opportunities for Cooperation on Cybersecurity in the Energy Sector

This section describes activities to improve cybersecurity that are supported by the U.S. Department of Energy (DOE) both for the U.S. and international energy sectors as an initial example from which APEC can learn.

2.1 Background on DOE's Activities to Improve Cybersecurity in U.S. Energy Sector

The DOE carries out a range of activities to improve cybersecurity in the electricity subsector and the oil and natural gas subsector, including:

- Facilitating **government-industry partnerships** to accelerate cybersecurity efforts for the grid of the 21st century.
- Funding **research and development** (R&D) of advanced technology to create a secure and resilient energy infrastructure.
- Supporting the development of **cybersecurity guidelines** to provide a baseline to protect against known vulnerabilities.
- Facilitating timely sharing of actionable and relevant threat information.
- Advancing **risk management strategies** to improve decision-making.
- Supporting sector incident management and response.
- Enhancing and augmenting the **cybersecurity workforce** within the energy sector.

2.2 DOE Tools to Strengthen Cybersecurity Capabilities

Building on DOE’s work with U.S. industry and federal partners, the DOE has developed the following tools. These tools, along with others developed elsewhere, can help other APEC Member Economies build their own capacity to address cybersecurity threats in the electricity, oil, and natural gas sectors:

- The DOE, in partnership with U.S. industry, developed an Electric Subsector **Cybersecurity Capability Maturity Model** (ES-C2M2). It is developing an Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model. The ES-C2M2 outlines ten domains, such as risk management and incident response, in which utilities should seek to improve capabilities. This tool can facilitate self-assessments by energy sector entities.

- The DOE supports the R&D of **advanced technologies** uniquely designed to protect energy systems from cybersecurity threats, some of which are commercially available and in current use.

- Under the U.S. National Response Framework, the DOE is the lead federal agency for coordinating the reestablishment of damaged energy systems and components in

response to disasters and emergencies. To that end, DOE has developed a robust incident management capability to respond to natural disasters and emergencies involving energy infrastructure. As a complement, DOE is developing a sector-wide **cybersecurity incident management capability**.

Other potential opportunities for cooperation that would require external funding include:

- The DOE can develop a tailored **Graded Security Protection framework** and conduct **cyber-physical security vulnerability assessments** of energy systems in cooperation with host Member Economies. DOE national laboratories—such as Sandia National Laboratories (SNL) —are involved in design and implementation of cyber and physical security infrastructures. Software tools are also available. One tool that is available for use is Pacific Northwest National Laboratory's (PNNL) Physical and Cyber Risk Analysis Tool (PACRAT), a next-generation assessment tool that blends methods of evaluating physical security and cyber systems to identify potential vulnerabilities in today's modern integrated security systems.

- The DOE develops **new capabilities in R&D and testing**. The DOE could share information on how to develop a cyber research lab, which could provide a foundation for strengthening cybersecurity and developing new technology. Drawing on its own experience in creating the National SCADA Test Bed, the DOE could provide information on establishing a reliability test bed and cybersecurity simulator for researching, developing, and deploying technologies to better manage and control grid operations, as well as for providing a platform for training cybersecurity specialists in electric power operations.

- The DOE is identifying the job skills required to perform cybersecurity functions in daily operations of the modernized grid. Identifying those skills enables a more informed discussion power industry needs as well as the education and training required to meet those needs. The DOE can share the results from its Secure Power Systems Professional project, and develop and conduct energy cyber-physical security training for host Member Economies.

3 Industry Standards and Best Practices

This chapter contains information about organizations and structures at the international and regional level as well as, as an example at the Member Economy level, the relevant U.S. entities that work on standards and best practices for addressing the cyber-energy nexus.

A challenge for standards is that the cyber threat is complex, non-linear and rapidly evolving. It can take years to develop an effective standard to protect against a threat but that may look very different by the time the standard is implemented. Meanwhile, the number of smart sensors and networked devices that are collecting and sending information back into energy infrastructure is rapidly increasing. Indeed, the modern grid is quickly becoming part of the Internet of Things (IoT) and APEC Member Economies need to be prepared to realize the opportunities as well as overcome the cyber security challenges that this energy evolution will entail. It is essential that APEC Member Economies continue to improve, adapt and adopt their own cyber security standards to help ensure the energy security and reliability of energy supply in the region.

3.1 Industrial Control Systems (ICS) Computer Emergency Response Team (CERT)

The North American Electric Reliability Corporation (NERC) develops mandatory federal critical infrastructure protection (CIP) standards that are then approved by the Federal Energy Regulatory Commission (FERC). On November 22, 2013, FERC approved Version 5 of the critical infrastructure protection cybersecurity standards (CIP Version 5), which covers critical cyber asset identification, security management controls, personnel and training, electronic security, physical security, systems security, incident reporting and response planning, and recovery plans. These standards have been valuable in fostering situational awareness among a wide spectrum of power sectors stakeholders. However, U.S. standards only cover part of what can be considered a critical cyber asset. Currently, there are standards gaps at the distribution level.

The Industrial Control Systems (ICS) Computer Emergency Response Team (CERT) is part of the U.S. Department of Homeland Security's (DHS) National Cybersecurity and Communication Integration Center (NCCIC). Its mission is to provide interrelated guidance between government and industry to improve cybersecurity of control systems within the nation's critical infrastructure, and to work to reduce risks within and across all critical infrastructure sectors. The partnership includes law enforcement agencies and the intelligence community in addition to cybersecurity and control systems communities. ICS-CERT provides assistance to control system vendors and energy critical asset owners/operators to identify cybersecurity vulnerabilities as well as develop mitigating strategies to strengthen their cybersecurity posture and reduce risk.

ICS-CERT has established the Control Systems Security Working Group (CSSWG) provides a forum for federal level stakeholders to improve control systems' cybersecurity in critical

infrastructure. The CSSWG encourages and provides the framework for interaction and collaboration among federal departments and agencies pertinent to control system cybersecurity initiatives. The range of critical infrastructure sectors can include chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactor/material/waste, transportation systems, water systems, and wastewater systems. Because of the wide range of sectors, team members come from various departments and agencies with a common role and a responsibility for securing relevant ICSs. Although the sectors may vary, many cybersecurity challenges are similar from sector to sector. Thus, this collaborative effort provides benefits by promoting and leveraging existing work while maximizing efficient resource use.

ICS-CERT also collaborates with members of the control systems community to help develop and vet recommended practices, and provide guidance in incident response capability. It participates in leadership workshops to ensure the community's cybersecurity-related concerns are considered in future development of products and deliverables. Finally, ICS-CERT takes part in discussions within the control systems community to establish a relationship that leads to a collaborative environment in which to address common control system cyber-security issues. ICS-CERT is developing a suite of tools that can be used to provide asset owners/operators the ability to measure the security posture of their control systems environment and help identify appropriate mitigation measures to address issues and risks. [1]

The ICS-CERT provides a location for the Control Systems Advisories and Report bulletin, which includes the following sections:

- **Alerts** – The alerts section provides a list of notifications to critical infrastructure owners and operators in a timely manner in relation to any threats to critical infrastructure networks.

- **Advisories** – The advisories section provides information to the community in a timely manner in relation to current security issues, vulnerabilities, and exploits of critical infrastructure networks.

- **ICS-CERT Monitor** – In the monitor section, a newsletter is provided to the owners, operators, or other personnel who are responsible for the protection of their critical infrastructure assets.

- **Joint Security Awareness Reports (JSARs)** – The JSAR Advisory is available to the community and provides awareness and/or feedback information from critical infrastructure owners, operators, integrators, and industry-related peers. The information pertains to ongoing cyber events and potential threats that affect the critical infrastructure computing networks.

- **Other Reports** – This section provides access to other reports, technical papers, annual reports, and other products that ICS-CERT believes could be of interest both to the control systems community and to those who protect industry control systems.

In addition, ICS-CERT provides general announcements, newsletters, relevant resources and published work available for download, and an archive for past advisories and reports. All information is shared and available to the control systems community to further deliver a collaborative workspace and help each individual owner/operator further enhance their controls systems to increase their security posture. ICS-CERT encourages owners and operators to join the Control Systems secure portal. [1]

3.2 International Electrotechnical Commission (IEC)

The International Electrotechnical Commission (IEC) is the world's leading not-for-profit, non-governmental organization that prepares and publishes international standards for all electrical, electronic, and other related technologies. IEC, established in 1906, provides companies, industries, and governments a platform to meet, discuss, and develop international standards. Devices that contain electronics and use or produce electricity rely on the International Standards and Conformity Assessment Systems (put together by IEC) to properly perform, fit, and work safely together.

The IEC International Standards represent the needs of key stakeholders from every participating nation around the world. Approximately 10,000 subject matter experts in the industry worldwide participate in the technical work of the IEC. Every country member has one vote and cooperates in approving the information that becomes part of the IEC International Standards. IEC promotes world trade and economic growth, and encourages development of new products, systems, and services that are safe, efficient, and environmentally friendly. [2]

3.2.1 IEC TC57

The Technical Committee (TC) 57 is one of 174 TCs and Subcommittees (SC) that carry out the standards work of the IEC. These working committees are composed of subject matter experts in electrotechnology from around the world. These subject matter experts, who are from industry, commerce, government, R&D laboratories, academia, and consumer groups, contribute and take an active part in the work. The TC groups report to the authorizing Standardization Management Board (SMB). The Full Member National Committee is the approving board for areas of activity for preparation and publication of technical documents on specific subjects within each TC or SC's respective scope. The Full Member National Committee conduct votes to approve submissions and assign them as International Standards. [2]

TC 57 is the power system management and associated information exchange working committee. TC 57, established in 1964, addresses the need to produce international standards in the field of communication between the equipment and systems for the electrical power process, including telecontrol, teleprotection, and all other telecommunications to control the electric

power system. TC 57 has recently evolved to include critical subset of standards relevant to smart grid technology. [2]

The scope of TC 57 is to prepare international standards for power systems control equipment and systems including Energy Management Systems (EMS), Supervisory Control and Data Acquisition (SCADA), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information used in planning, operation, and maintenance stages of power systems. [2]

3.2.2 IEC TC57 WG15 IEC 62351

Under the IEC TC 57 structure, Subcommittees and/or Working Groups (WG) are further broken down to more specific subject areas. Within IEC TC 57 are twelve Working Groups, two Joint Working Groups, and one ad-Hoc Group. All relate to the protocols, automation, and communication (of distribution, interfacing monitoring and control, and carrier systems). IEC 62351 exists under the WG15. [2]

IEC 62351, under the WG15, is the security standard for the power system information infrastructure. The scope and purpose is:

> *Undertake the development of standards for security of the communication protocols defined by the IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series and the IEC 61968 series.*
>
> *Undertake the development of standards and/or technical reports on end-to-end security issues.* [2]

The five accepted communications standards that IEC TC 57 has developed are:

1. **IEC 60870-5:** This series is widely used in Europe and many other countries for SCADA system to RTU data communication. It is used in serial links (Part 1) and over networks (Part 104). [2] [3]
2. **IEC 60870-6:** This series is used internationally for communications between control centers and often for communications between SCADA systems and other engineering systems within control centers. [2] [3]
3. **IEC 61850:** This series is used for interactions with field equipment, including protective relaying substation automation distribution automation, power quality, distributed energy resources, substation to control center, and other power industry operational functions. It also includes profiles to meet the ultra-fast response time of protecting relaying and for the sampling of measured values. [2] [3]
4. **IEC 61968 and IEC 61970:** These series are used for application–to-application interactions, primarily within utility operations centers. The series consist of a UML abstract model of the power system and includes information models and messaging for

application-level information exchanges for transmission, distribution, and market functions. [2] [3]

5. **IEC62351** security standards and the IEC TC 57 communications standards do not have a one-to-one correlation because many of the communication standards rely on the same standards at different layers in the security standards. [2] [3]

The power industry is becoming more reliant on information to operate power systems so the power system and infrastructures must be managed together. As automation increasingly replaces manual operations, the management of power system infrastructure becomes more reliant on the information infrastructure.

Figure 1and Figure 2 illustrate the methods of manufacturing dual infrastructure:

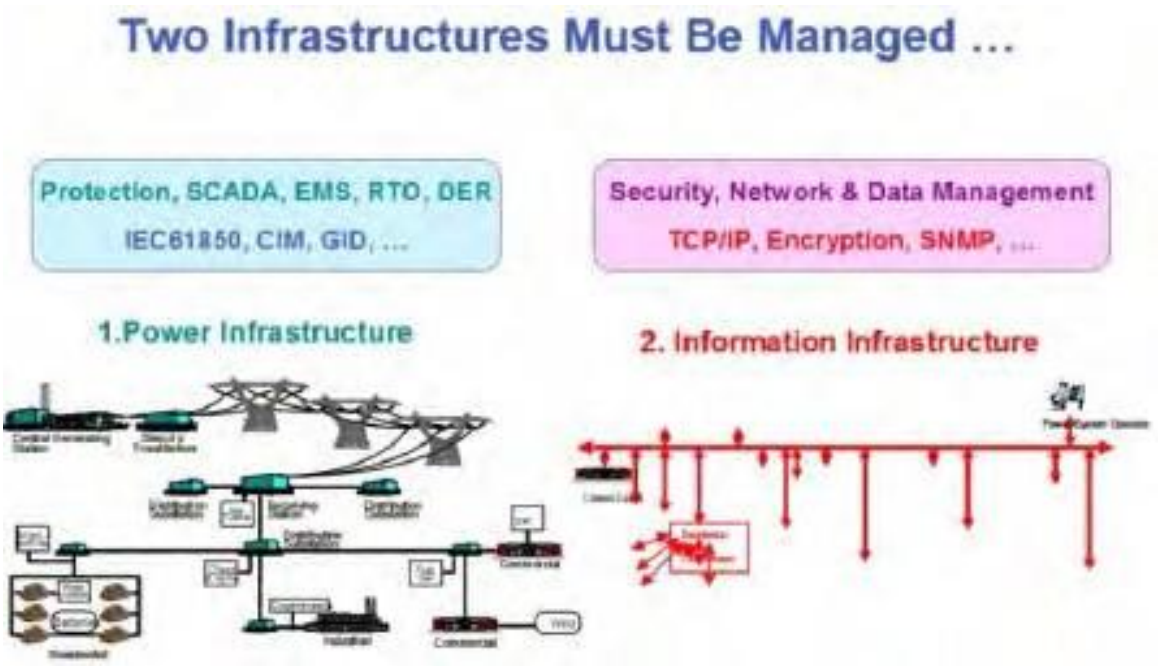

Figure 1. Managing Two Separate Infrastructures [3]

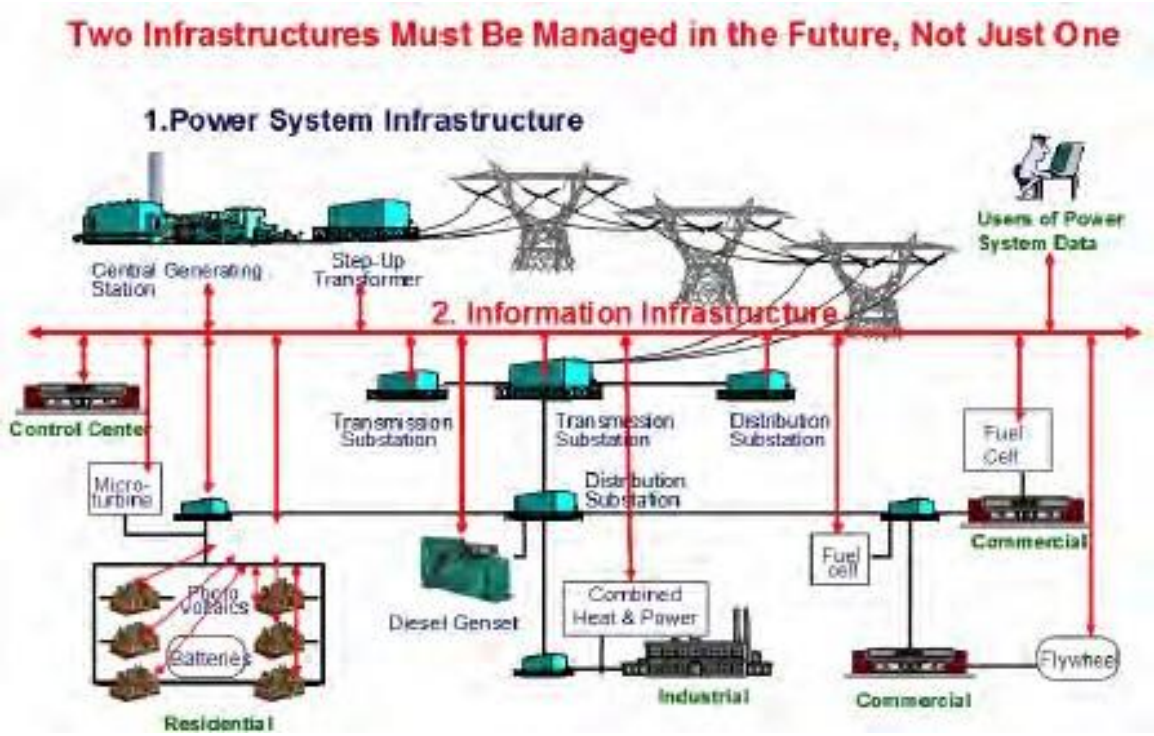

Figure 2. Managing Two Dependent Infrastructures [3]

Just as physical security protects a critical infrastructure from the defined threats on physical attacks, cybersecurity can be used to protect against cyber-attacks. A cyber-attack can use communication protocols to manipulate or negatively impact power system operations. In addition, an adversary can incorporate industrial espionage threats in an attack to seek out information to use in their favor to have an advantage over a specific facility or industry. Energy critical infrastructures exist in worldwide and, therefore, they are an attractive target for cyber-attacks. The IEC 62351 security standards provide guidelines for security on TCP/IP, Manufacturing Message Specification (MMS), architecture, XML files, and on IEC 69870-5 and IEC 61850 derivatives and profiles. [3]

3.3 National Institute of Standards and Technology (NIST) Standards

NIST is a U.S. federal technology agency within the U.S. Department of Commerce that works with industry to develop and apply technology, measurements, and standards. In relation to smart electric power grids, the electronics records, atomic clocks, advanced nanomaterials, and services rely on the standards developed and provided by NIST. Founded in 1901, NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology to enhance economic security and improve quality of life. NIST is responsible to developing standards, guidelines, and minimum requirements for all agency operation and asset facilities to provide adequate information security. [5]

3.3.1 NIST SP 800-53

The NIST SP 800-53 is a guideline that covers Risk Management Framework in relation to security controls for federal information security in the Federal Information Processing Standards (FIPS) 200. The security controls are those actions related to management, operational, and technical safeguards or countermeasures applied to an information system effectively to protect a system and its information. NIST SP 800-53 defines and recommends security controls for use by organizations to implement protection of their information as well as implementing those protection elements as part of a well-defined information security program. The NIST SP 800-53 guideline describes the assessment procedures for 17 security controls, which are: [10]

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Certification, Accreditation, and Security Assessments
5. Configuration Management; Contingency Planning
6. Identification Authentication
7. Incident Response
8. Maintenance
9. Media Protection
10. Physical and Environmental Protection
11. Planning; Personnel Security
12. Risk Assessment
13. System and Services Acquisition
14. System and Communications Protection
15. System and Information Integrity

The NIST SP 800-53 describes what an effective information security program should include. The guidelines in this document help the organization's responsible individuals understand the risk factors and their effects on the operations and assets. An understanding of security program and security controls—along with the guidelines in this document—will help the responsible individuals make informed decisions and investments to mitigate risks to an appreciable level. The objective is to provide guidance for organizations to meet their missions and provide adequate security against unauthorized access, use, disclosure, disruption, modification, or destruction of information. [10]

The publications of NIST SP 800-53 also include a description of fundamental concepts for security control selection and specification (i.e., structural components, common use of security controls, baseline controls, effectiveness assurance of security controls, and commitment to maintain the security controls up to date and current). They also include a description of selection and specification process of security controls for an information system, and, reference

appendices with detailed information on the selection and specification of security control systems.[10]

3.3.2 NIST SP 800-82

This document was developed to provide guidelines for ICS security, including SCADA, Distribution Control Systems (DCS), and other control system configurations like Programmable Logic Controllers (PLC). The document provides an overview of ICS and other typical system infrastructure, identifies common threats and vulnerabilities, and provides recommended security countermeasures to mitigate associated risks. [5] [6]

This document provides overview information for each of the SCADA, DCS, and PLC systems as well as giving details of their key components and typical modes of operations. General system layout and architecture for each system also provides examples for basic understanding of the topology. Key components identified within each type of system describe how each component is implemented and integrated in the system. [5] [6]

Currently in today's industries, ICS systems are no longer isolated from outside networks as they once were. They now require secure communication capabilities for interconnected systems. ICS systems were at one time considered isolated systems running proprietary control protocols with specialized hardware and software, but now low cost Internet Protocol (IP) devices are replacing proprietary solutions. With that change comes an increase of the possibility of cybersecurity vulnerabilities and incidents, as well as ICS systems that resemble IT systems. Although ICS and IT systems resemble one another, security solutions designed and used to address typical IT security issues may not apply to an ICS system environment. When these IT security solutions are applied to ICS systems, special precautions must be taken to ensure they apply. In some cases, new security solutions need to be specifically tailored for the ICS environment. The NIST SP 800-82 characterizes an ICS and an IT system to document the differences between the two environments. The document also identifies the threats and vulnerabilities at different levels within an ICS. Possible incident scenarios include in the documentation outline and characterize which sources of incidents and consequences associated with each scenario. [6]

NIST SP 800-82 provides guidelines for ICS security program development and deployment for an ICS. The guidelines discuss what an ICS should protect against and how to prioritize the threats, potential consequences, mitigations, training, management's role, and other elements that should be considered when developing and deploying an ICS security program. Furthermore, this document includes standards and guidelines involving the network architecture and critical components and elements to consider when designing the network structure for an ICS. Finally, this document covers security control, which involves the management, operational, and technical controls (i.e., safeguards or countermeasures) for an informational system to protect the confidentiality, integrity, and availability of the system and its information. [6]

3.3.3 NISTIR 7268

The National Institute of Standards and Technology Interagency Report (NISTIR) describes research conducted of a technical nature and of interest within a specific area and for a specialized audience. NIST generates the final reports from its work performed for outside sponsors and stakeholders, both of whom may be government or non-government agencies. The NISTIR 7268 is a three-volume guideline publication widely recognized and applicable to utilities, vendors, and regulators. Developed from the framework and roadmap of NIST, the NISTIR 7268 guideline describes an analytic framework that organizations can use to develop effective cybersecurity strategies designed for different combinations of smart grid characteristics, risks, and vulnerabilities. The variety of different stakeholders and industries can use this guideline's methodologies and information to identify and assess risk, along with applying appropriate security requirements. [11]

The volume structure and content of the NISTIR 7268 is as follows:

- **Volume 1.** Describes the strategy approach for a smart grid cybersecurity architecture and infrastructure along with associated requirements, management methodology, and relevant examples. This volume presents high-level architecture interfaces and components and describes the associated security requirements.

- **Volume 2.** Describes the privacy topics related to the smart grid cybersecurity infrastructure as well as associated state laws and privacy use cases. This volume provides awareness and discussion topics of evolving smart grid technologies. New types of information relate to individuals, groups, and their behavior. Furthermore, this volume discusses how the new information may present privacy risks and challenges. This volume discusses risks and mitigation recommendations based on widely accepted privacy principles for entities that participate within the smart grid.

- **Volume 3.** Describes different analysis types for smart grid cybersecurity, the different level of vulnerability classification (including potential vulnerabilities), security analysis, R&D topics for cybersecurity, standards review and security requirements related to the smart grid. [11]

3.4 North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards

The North American Electric Reliability Corporation (NERC), originally formed in June 1968, is a non-profit international regulatory authority; its successor formed in March 2006. NERC's mission is to promote the reliability and adequacy of the bulk power system of North America. NERC's major responsibilities include development and enforcement of reliability standards, assessments of seasonal and long-term reliability, monitoring the bulk power system through system awareness, and providing education and training resources through an accreditation program to ensure industry power system operators are qualified and proficient. NERC regional

responsibility oversees eight regional entities of all the interconnected power systems in the United States, Canada, and the northern portions of Baja California, Mexico. The Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada oversee the NERC electric reliability organization. The NERC community includes more than 334 million personnel from industry who are users, owners, and operators of the bulk power system. [7]

3.4.1 NERC CIP Standards

The NERC Critical Infrastructure Protection (CIP) standards 001 through 009 are mandatory Reliability Standards in the United States for cybersecurity standards of critical infrastructures. The FERC designated NERC with the ERO in accordance with Section 215 of the Federal Power Act, legislated by the Energy Policy Act of 2005. The CIP standards address the security of cyber assets and components vital to the operations of the electric grid. Subject matter industry experts develop standards that are approved by FERC, which oversees NERC's enforcement of them. [7] [8]

NERC CIP Standards include nine mandatory standards under the following areas:

- CIP-001: Addresses sabotage reporting of a critical infrastructure.
- CIP-002: Addresses the requirements of identification and documentation of critical cyber assets associated with the Critical Assets that support the reliability of the bulk electric system operations.
- CIP-003: Addresses the requirements the critical infrastructure entity must have in place for minimum-security management control to protect the critical cyber assets.
- CIP-004: Addresses the requirements authorized personnel with access to critical cyber assets must have, including an appropriate level of personnel risk assessment, training, and security awareness.
- CIP-005: Addresses the requirements of identification and protection of the electronic security perimeters where all critical cyber assets reside, including all Entry Control Points (ECP) of the perimeter.
- CIP-006: Addresses the requirements of implementation of a physical security program for the protection of the critical cyber assets.
- CIP-007: Addresses the requirements of the responsible Critical Infrastructure entity to define methods, processes, and procedures for securing systems identified as Critical Cyber Assets, including other non-critical cyber assets within the electronic security perimeter (Protected Area).
- CIP-008: Addresses the requirements to ensure the identification, classification, response, and reporting of cybersecurity incidents related to critical cyber assets.
- CIP-009: Addresses the requirements to ensure recovery plans are developed and implemented for critical cyber assets and to ensure the recovery plans coincide with existing business policies and disaster recovery techniques and practices. [7] [8] [9] [19]

3.5 International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is an organization composed of recognized representatives and members from various countries who are the national standards bodies around the world. ISO initially began in 1926 as the International Federation of the National Standardizing Associations (ISA). In 1946, delegates from ISA and the United Nations Standard Coordinating Committee (UNSCC) formed ISO. It began operating in 1947. Today, ISO is a well-known independent, non-governmental membership organization and is the world's largest developer of voluntary international standards. The group has published over 19,500 international standards related to technology and manufacturing. [12] [13]

ISO consists of 165 member countries and 3,368 technical bodies with a Central Secretariat based in Geneva, Switzerland. The Technical Management Board is responsible for the 250-plus technical committees that develop the standards. ISO's main product is international standards, but ISO also publishes technical reports, technical specifications, publicly available specifications, technical corrigenda, and guides. ISO has also formed joint committees with IEC to develop standards and terminology in the areas of electrical, electronic, and other related technologies. The joint committees are composed of the ISO/IEC JTC 1 (Information Technology) and ISO/IEC JTC 2 (Joint Project Committee – Energy Efficient and Renewable Energy Sources – Common Terminology). ISO has several families of standards in different topic areas. For this report, this section covers the industry-specific family of standards relevant to cybersecurity and smart grids. [12] [13]

3.5.1 ISO/IEC 27000 Family of Standards Series

ISO/IEC joint committees make the ISO/IEC 27000 family of standards series of information security standards, which ISO and IEC publish jointly. This family of standards series provides best practices and recommendations on information security management and risks and controls within an Information Security Management System (ISMS). The scope of this family of standards series is broad in that it covers topics beyond privacy, confidentiality, and IT/technical security issues. These standards are applicable to a broad number of different organizations regardless of their type or size. The ISO/IEC 27000 family of standard series encourages organizations to assess their information security risks, and then apply guidance and suggestions to implement appropriate information security control based on the identified risks. The overall objective of using and aligning to the ISO/IEC family of standard series (Figure 3) is so an organization is able to:

- Secure its critical asset.
- Effectively manage risks.
- Improve and maintain customer confidence.
- Demonstrate conformance to international best practice.
- Avoid brand damage, loss of earning, or potential regulatory fines.
- Evolve information security posture alongside technological developments. [14]

Currently, 23 standards in the series are published and available, and several others are under development. [15]

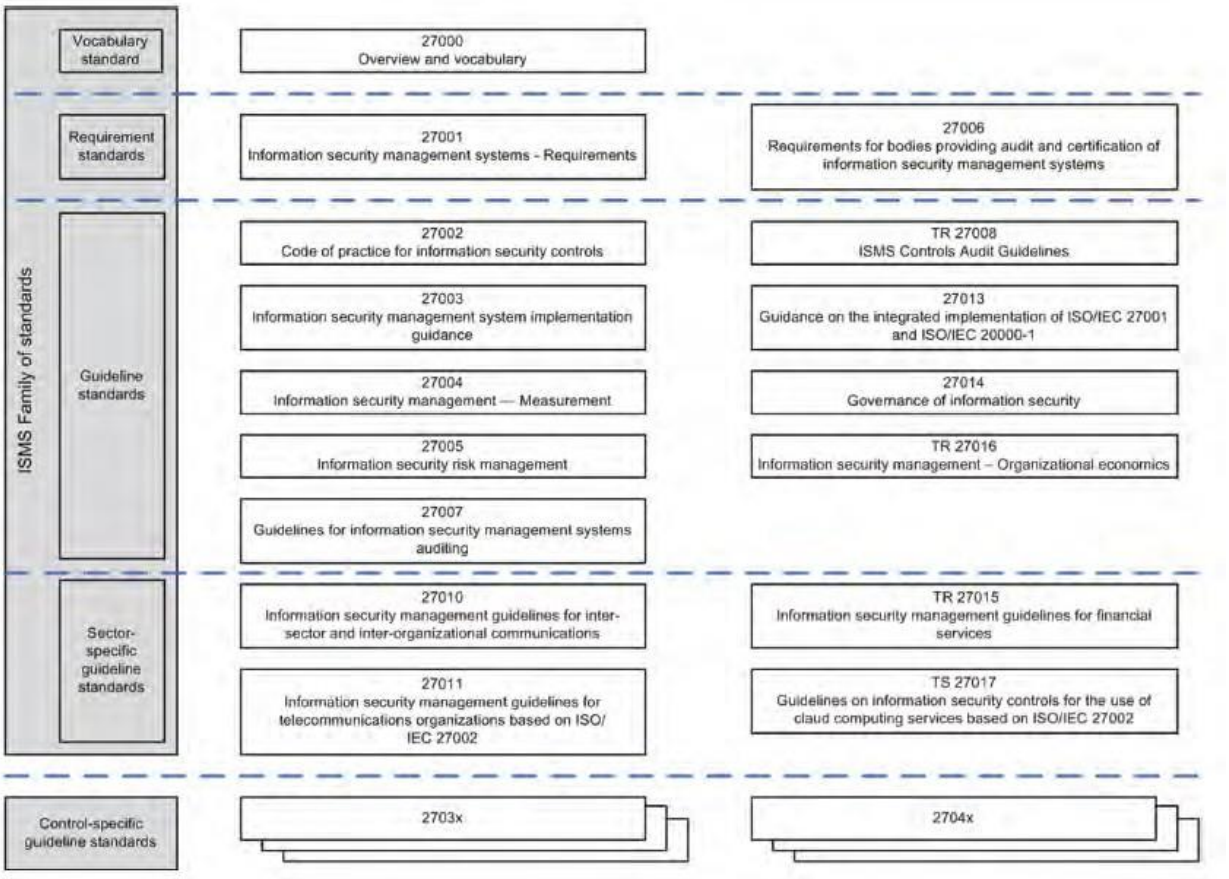

Figure 3. ISO/IEC Family Standards Sections and Relationships [14]

3.5.2 ISO/IEC 27002 Standard

The ISO/IEC 740027002 standard is a code of practice for information security controls. This international standard provides a list of industry-accepted control objectives and best practice controls during the selection and implementation of control systems in an organization's information security infrastructure [14]. Furthermore, experts use this standard to develop industry- and organization-specific information security management guidelines, keeping in mind their own specific information security risk environments. This standard is also designed to help organizations implement commonly accepted information security control and to develop their own information security management guidelines. [16]

The ISO/IEC 27002 standard covers 14 different security control topics relating to a total of 35 main security categories and 114 controls. Each security control may have one or multiple security categories, but it is up to the organization to determine which security control and category is applicable and relevant to their organization; therefore, the organization must identify applicable controls and prioritize the level of importance based on the organization's business processes. Note: The security control and category listed in this standard does not imply significance or importance. It is the responsibility of the organization to establish the order for its own business environment.

3.5.3 ISO/IEC 27005 Standard

The ISO/IEC 27005 standard provides guidelines for information security management in an organization. This standard specifically addresses the requirements of an ISMS, but does not include any specific method for information security risk management. Each organization's individual(s) are responsible for defining the organization's specific methods and approach to risk management. ISO/IEC 27005 lists a number of existing methodologies to use to meet the requirements of ISMS. The ISO/IEC 27005 standard supports the general concepts specified in ISO/IEC 27001 and assists in the satisfactory implementation of information security. [17]

3.5.4 ISO 31000 Family of Standards Series

The ISO 31000 family of standards series provides principles and generic guidelines for the design, implementation, and maintenance of risk management throughout an organization. This family of standards series is not for any particular industry group, management system or subject matter expert; instead, it provides best practices and guidance for operations concerned with risk management. This family of standards series can be applied at any time within an organization to a broad range of activities, strategies and decisions, operations, processes, functions, projects, products, services, and assets. In addition, practitioners can apply this family of standards series to any type of risk, regardless of whether an outcome may produce positive or negative consequences. [18]

ISO/IEC Guide 73 is a revised version of the terminology under the ISO 31000 family of standards series.

Figure 4 summarizes the relationships among the principles, framework, and processes of the ISO 31000 family of standards. [18]

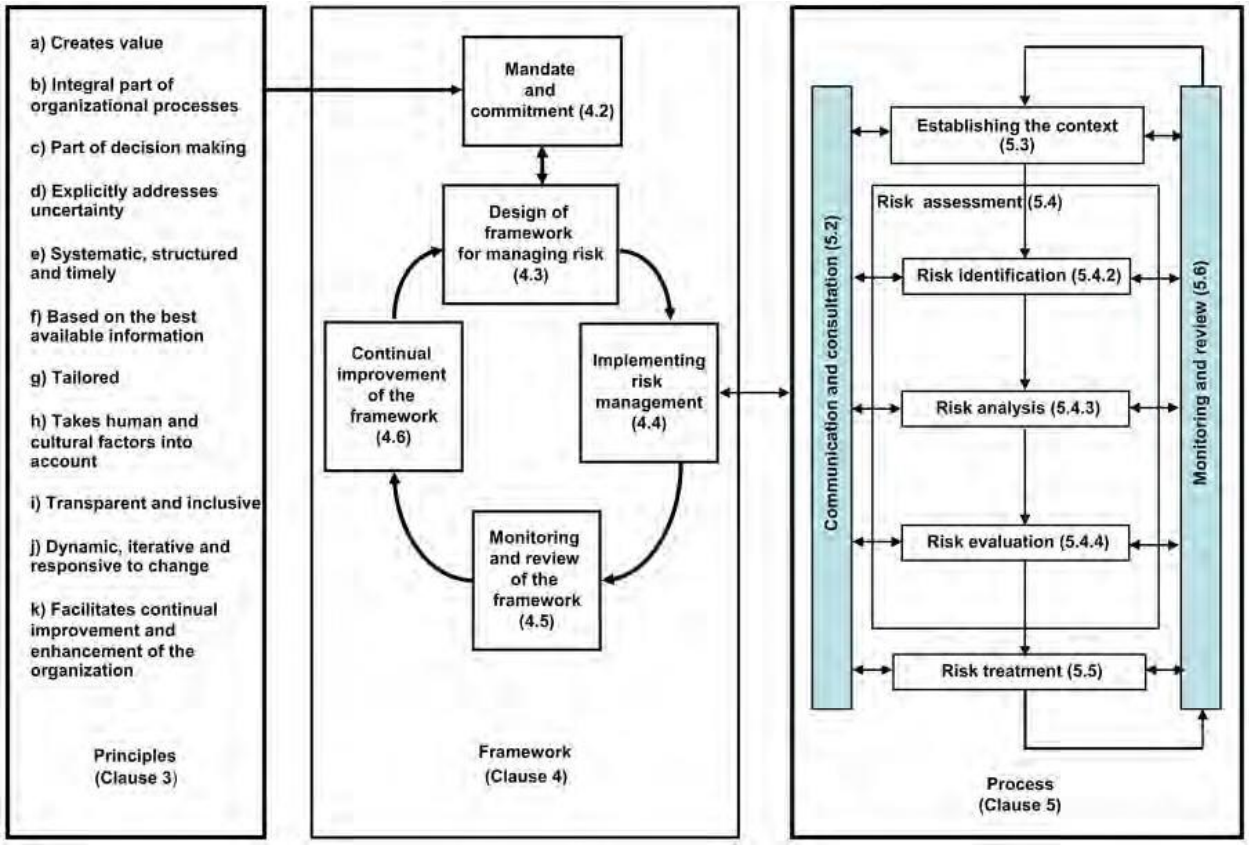

Figure 4. ISO 31000 Family Standards Sections and Relationships [18]

3.6 Federal Information Processing Standard (FIPS)

The U.S. Government publically announces standards it has developed for use by government and non-military government contractors in their computer systems to protect sensitive data in Federal Information Processing Standards (FIPS) publications, issued by NIST. FIPS standards describe the documentation process, encryption algorithms, and other information technology standards. The FIPS mission is to ensure that all U.S. Federal Government agencies adhere to the same security, communication, and data privacy requirements. FIPS addresses the compatibility of different systems, the portability of data and software, cost-effective computer security, and the privacy of sensitive information in U.S. federal computer systems. Most of the statements made in the FIPS are modified versions of the standards used in the technical community, such as the American National Standards Institute (ANSI), the Institute of Electrical and Electronic Engineers (IEEE), and ISO. [5] [20]

FIPS 140-2 is one of 15 listed standards in the FIPS. FIPS 140-2 contains the security requirements for cryptographic modules that provide four qualitative levels (Levels 1 through 4)

intended to cover a wide range of potential applications and environments. These areas, related to the secure design and implementation of cryptographic models, include specifications, ports and interfaces, roles, services, authentication, finite state model, physical security, operations environment, cryptographic key management, electromagnetic interference/electromagnetic compatibility (EMI/EMC), self-testing, design assurance, and mitigation of other attacks. [20]

The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to the FIPS 140-2 standards. NIST and the Communications Security Establishment of the Government of Canada jointly established the CMVP. Federal agencies of both economies accept these validated products for the protection of sensitive information (United States) or Designated Information (Canada). [20]

FIPS 140-2, which is follow-on to FIPS 140-1, incorporates changes in applicable standards and technology based on comments received from vendors, laboratory personnel, and users who are part of the technical committee. The operator of an organization is responsible for ensuring the proper cryptographic module provides security to the users and is acceptable to the owner of the protected information. Practitioners must determine an overall security level of a cryptographic module to provide an acceptable level of security appropriate for the security requirements of the application and the environment in which the module is used. FIPS 140-2 describes the different security levels and their protection characteristics along with the security requirements. The document contains examples to illustrate how requirements might be met. [20]

3.7 Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers (IEEE) is the largest technical professional association with more than 425,000 members worldwide (in approximately 160 countries). Its core objectives are educational and technical advancement in innovation and excellence of electrical and electronic engineering, telecommunications, computer engineering, and other related disciplines. The related disciplines include computer science, software development, information technology, physics, and medicine. [21] [22]

IEEE provides members with services. It has 38 established technical societies and communities. IEEE also provides a wide range of quality publications and standards. The publications allow the exchange of technical knowledge and information among technology professionals. IEEE produces over 30 percent of the world's literature in the electrical and electronics engineering and computer science fields. The standards provide technical expertise and innovation concepts, drive global participation, and pursue ongoing advancement and promotion of new concepts. IEEE is the leading standards development organization for development of industrial standards in a broad range of disciplines. [21] [22]

The IEEE 1402 standard is a guide for physical and electronic security of electrical power substations, which provides minimum requirements and practices for physical security of electric power stations. The purpose of this standard is to provide defined engineering practices to enhance the physical protection of a substation to protect against a number of threats. Substations

are typically unmanned so the practices help in mitigation risks related to vulnerabilities in unauthorized access, theft, and vandalism. The IEEE standard defines requirements that cover the authorized access control, monitoring of facilities, and delay/deterrent features, to implement to mitigate defined threats/risks for an organization/facility. This standard also defines the levels of physical protection measures to consider for implementation at electric power substations. The responsible substation owner of an organization determines the level of protection by conducting a threat assessment based on the characteristics and attractiveness levels of their facility/facilities. This standard in itself does not establish requirements based on the specific characteristics or criticality of a substation. Beyond the scope of this standard are attack scenarios on a substation that include natural disasters or an adversary's main objective of destroying or disabling the operation of a substation by the use of explosives, projectiles, and/or vehicles. [23]

3.8 Regional Challenges and Standards Development Gaps

The APEC community faces challenges similar to those in other communities in addressing and preventing cyber-related incidents, and in increasing the level of effort to facilitate national and international cooperation. For example, the APEC community is facing issues similar to those of the Association of Southeast Asian Nations (ASEAN), whose membership overlaps and has been slow to adopt national and regional comprehensive cybersecurity strategies and standards. A desire exists among regional communities to increase the level of collaboration on cyber-related challenges through the adoption of new structures, standards, and methods of conducting business consistent with national initiatives and international efforts. [24]

The challenge is becoming greater as the number of internet users continues to increase, especially now that the number of users in developing economies is becoming equal to or greater than the number of users in developed economies. Of the 2.1 billion internet users worldwide, most (922.2 million) are located in Asia. China alone has 485 million users (Figure 5). Some areas in Asia do not have adequate access to information communication technology. This situation will change, with the number of users forecasted to increase. In addition, recent indicators also forecast a higher population growth rate in the ASEAN member states, which raises the probability of an increase in information communication technology demand. Demand for cooperation among the developing and developed economies to adopt processes, structures, and standards is likely continue to increase along with the population growth rate. Measures for consideration include a permanent coordination method, improved computer emergency response team among community members, additional training and proficiency building, supply chain surety, and defense building cooperation efforts. [24]

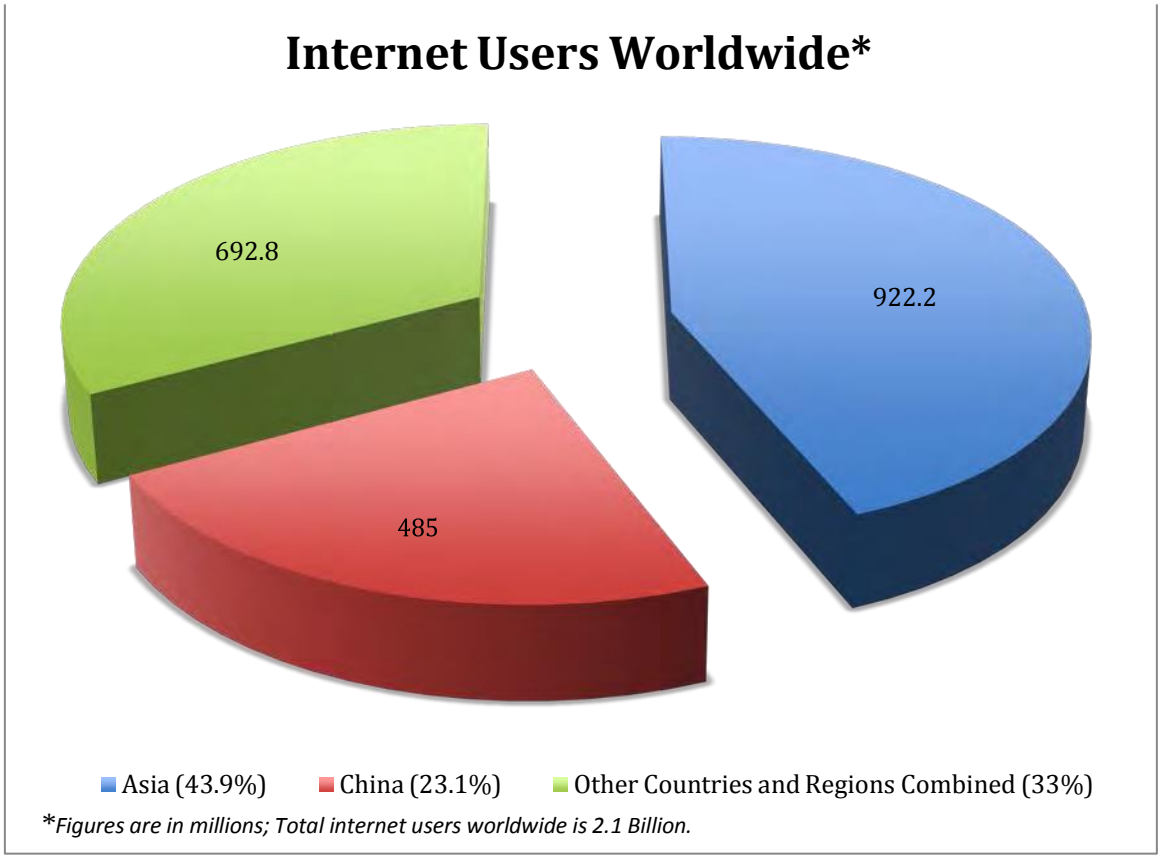

Figure 5. Internet Subscribers or Users Worldwide [24]

Within the ASEAN region, the average number of internet users increased by almost 150 percent between 2008 and 2011. The average number of internet users in 2011 is 101.6 users per 1,000 persons; the average mobile phone density in 2011 is 1,009 units per 1,000 persons. Note the rapidly growing number of mobile phones per capita, which highlights a potential increase in the number of mobile-enabled threats.

Figure 6 and Figure 7 each represent the number of average internet subscribers/users per 1,000 persons and the average number of cellular/mobile phone units per 1,000 persons respectively. When measuring internet use in terms of subscribed capacity compared to the number of subscriptions, the average number is greater, meaning there is a wider gap in internet use today versus the number of internet users in the near future. Viet Nam is a significant example; in June 2012, it was ranked 80th in the world in terms of internet use, while it was ranked eighth in Asia and third within the ASEAN community. Viet Nam has an estimated population of 31 million of which 10.5 million (35 percent of the population) are connected to or use the internet. Usage could increase to 45 percent to 50 percent of the population by 2020. Similarly, March 2013 reports stated Cambodia saw an increase in the number of internet users of 60 percent from the previous year that saw 2.7 million people online. The average mobile phone density reported previously for the ASEAN region (1,009 units per 1,000 persons) suggests that the member economies are at a saturation point or close to that, which assumes a narrowing gap between

present and future unit estimates. For example, in 2012 Viet Nam now has the greatest number of units per 1,000 persons with 1,560.7 units followed by Singapore, which has 1,517.8 units. Indonesia has nearly 63 million internet users, most of whom access the internet through their mobile devices. Myanmar had the lowest number of units per capita in the regional with only 62 mobile units per 1,000 persons; however, the number of units per capita is set to change with two new telecommunication licenses awarded in June 2013, which should increase the number of users in Myanmar. [24] [25]

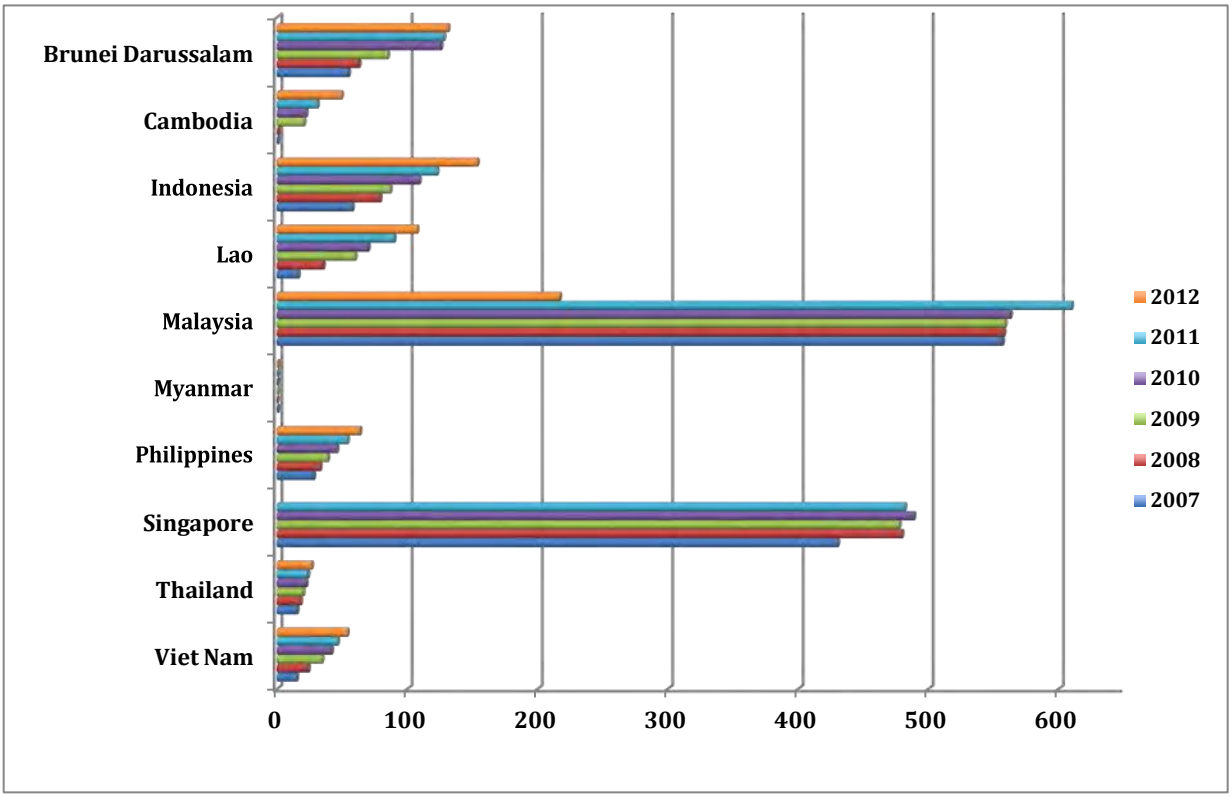

Figure 6. Internet Subscribers/Users per 1000 persons [25]

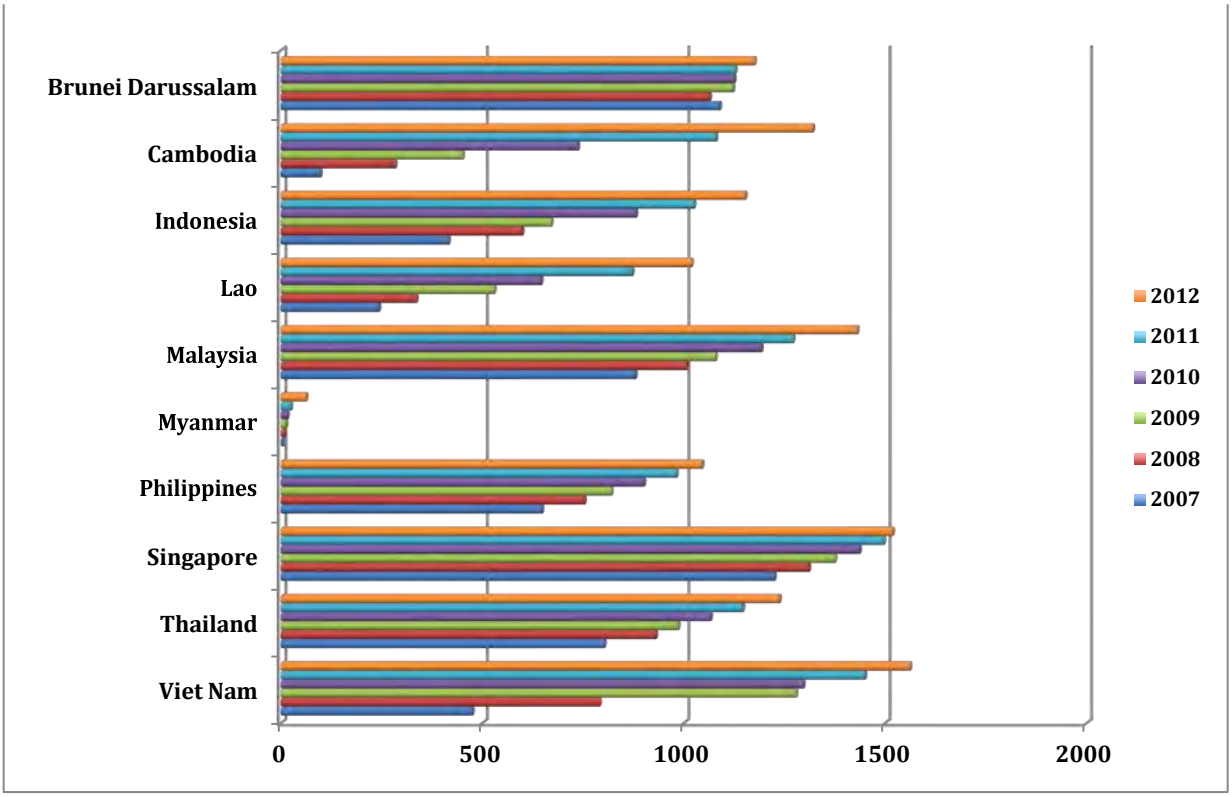

Figure 7. Cellular/Mobile Phone Density (number of units per 1000 persons) [25]

With these growing figures of internet users and mobile phone densities, it is important to implement and publish cybersecurity strategies in those economies that have not yet developed or implemented an appropriate framework to address cybersecurity issues. Economies that lack the necessary expertise, capabilities, and budgets can consult with other neighboring economies within the region as well as use open source resources (as defined in Section 4 of this report). Economies could also consider negotiating agreements for technical assistance, information sharing, technical training, and nontechnical expertise to help build effective and robust cybersecurity architecture. The objective is to work toward closing the digital divide and to support global training and capability building of technical personnel, law enforcement, policies, and organizations. A useful training and technical assistance program could build cybersecurity capability for crisis management in all APEC Member Economies.

A number of international and regional organizations, bodies, and forums are working towards addressing cybersecurity challenges and gaps. Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Viet Nam all have been working to adopt both national and comprehensive regional frameworks for cybersecurity, but the process has been slow and in stages. Ten Asian states are developing cyber capabilities and "are wrestling with how to adjust their policies and practices to new technology." [24]

The ASEAN Community has called for development of a common framework for cyber/network security and the establishment of minimum standards of network security to ensure preparedness and integrity of networks. Implementation of a status-screening program has also been called for, as well as development of best-practices models for business continuity and disaster recovery, and a multi-stakeholder network to promote CERT cooperation and sharing of knowledge and expertise. As the ASEAN Community continues to make progress in implementing these activities, albeit at a slower pace, it is necessary to make headway in addressing evolving cyber threats across multiple member states. Just as the ASEAN Community has done, the APEC Community should consider its goals and implement a number of measures, which include:

- Promoting international and regional collaboration to enhance the security of information infrastructures.
- Working towards a "conducive, safe, secure, and trusted environment and harmonized information communication technology rules and regulations that will promote trade, investment, and entrepreneurship".
- Provide safe and secured fixed and mobile broadband.
- Cooperating in building and promotion of secure online environments to enhance cybersecurity and counteract online threats within and among its member economies.
- Face-lifting "robust and resilient information infrastructure" through developing and implementing national frameworks on submarine cable connectivity protection and risk mitigation.
- Further enhancing the development of a policy framework and the sharing of best practices on the protection of data and information infrastructure in order to safeguard the network between member economies.
- Continuing to collaborate among regional CERTs to enhance incident investigation and coordination in support of community activities. [24]

To further expand on and build a more resilient cybersecurity regime, the APEC community could develop and implement a comprehensive, forward-looking, and multipronged framework to coordinate regional cooperation on common global cybersecurity challenges. This approach would not only benefit the APEC Member Economies, but also other regional and international communities. APEC could share developed and implemented frameworks among these communities to increase transparency for cooperatively agreed measures. The community members could also continue to strengthen relations with other regional dialogue partners and the international community on cybersecurity issues. One option could be to establish working groups to deal with cross-broader cyber challenges and common concerns. Additional measures that could be possible to expand elements of a wider comprehensive framework include:

- Establishing a permanent mechanism for regional coordination and information sharing.

- Establishing a robust regional community CERT and strengthening operational cooperation and information sharing among national CERTs.
- Creating a global cybersecurity hub of excellence for training and capacity building.
- Developing a secure supply chain and regional harmonization of international standards.
- Enhancing defense cooperation for cyber-related threats. [24]

In establishing cybersecurity initiatives, it is also important to recognize the many differences between information technology and operational technology (IT and OT). While increasingly IT and OT, cyber and physical systems are integrated and networked there are different threats, vulnerabilities and mitigation requirements for IT and OT. Moreover, the risk management policies, processes and governance for IT are very different from OT. So too are the necessary skills and tools to respond to cyber threats. IT and OT systems converge in buildings and "smart" energy infrastructures so it is important to establish new policies, processes and security paradigms to mitigate related threats.

APEC's critical infrastructure community includes a wide range of public and private stakeholders involved in securing infrastructure. Members of each critical infrastructure sector perform functions supported by information technology (IT) and industrial control systems (ICS). This reliance on technology, communication, and the interconnectivity of IT and ICS has changed and expanded the potential vulnerabilities and increased potential risk to operations. For example, as ICS and the data produced in ICS operations are increasingly used to deliver critical services and support business decisions to assess the potential impacts of a cybersecurity incident on an organization's business, assets, health and safety of individuals. One key take-away from the NIST's Framework for Improving Critical Infrastructure Cybersecurity is that to manage cybersecurity risks, a clear understanding of the organization's business drivers and security considerations specific to its use of IT and ICS is required. Because each organization's risk is unique, along with its use of IT and ICS, the tools and methods used to achieve the outcomes described will vary.

This page intentionally left blank.

4 Cybersecurity Programs and Organizations

4.1 U.S. Smart Grid Interoperability Panel (SGIP)

Initiated in December 2009 by the NIST, the Smart Grid Interoperability Panel (SGIP) is a public-private partnership to support in fulfilling NIST's responsibility, under the Energy Independence and Security Act of 2007, to coordinate and collaborate standards development for the smart grid with stakeholders. SGIP's mission is to accelerate the implementation of interoperable smart grid devices and systems. The SGIP seeks out input and cooperation from private and public sector stakeholders in developing the smart grid standards framework. The stakeholders include collaborators from the utilities, manufacturing, and consumer and regulator industries. [26] [27]

The SGIP is a non-profit private-public partnership organization, supported by industry stakeholder funding and funding provided through a cooperative agreement with NIST. NIST continues to play an active role in the SGIP. SGIP, through collaborated standards and advance interoperability, helps to develop the roadmap for innovation and more reliable, secure, and efficient energy systems globally. SGIP provides a platform for over 20 industry segments to voice their input, representing every domain in the power industry. The domain categories are as follows:

1. Appliance and consumer electronic providers
2. Commercial and industrial equipment manufacturers and automation vendors
3. Consumers – residential, commercial, and industrial
4. Electric transportation
5. Electric utility companies – investor-owned utilities and federal and state power authorities
6. Electric utility companies – municipal and investor owned
7. Electric utility companies – rural electric association
8. Electricity and financial market traders
9. Independent power producers
10. Information and communication technologies infrastructure and service providers
11. Information technology application developers and integrators
12. Power equipment manufacturers and vendors
13. Professional societies, users groups, trade associations and industry consortia
14. Research and development organizations and academia
15. Relevant government entities
16. Renewable power producers
17. Retail service providers
18. Standards and specification development organizations
19. State and local regulators
20. Testing and certification vendors
21. Transmission operators and independent system operators

22. Venture capital [26] [27]

The SGIP also supports other efforts aligned to address its mission in areas including: Doman Expert Working Groups, Priority Action Plans, Events (Workshops), Publications, Smart Grid Interoperability Panel Newsletter, and Catalog of Standards. The Catalog of Standards is a useful resource of information regarding smart grid standards that serves as a compendium of standards, practices, and guidelines relevant for development and deployment of a robust and interoperable smart grid. [26] [27] [28]

The SGIP coordinates and collaborates with stakeholders to further smart grid interoperability by:

- Developing reference architectures and implementation guidelines.
- Facilitating and harmonizing standards development.
- Identifying testing, certification, and security requirements.
- Informing and educating stakeholders.
- Conducting outreach to establish interoperability alignment. [26] [27] [28]

4.2 U.S. Smart Grid Cybersecurity Committee (SGCC)

Given the complex nature of the SGIP and the urgency of its mission, the SGIP has established several priority-specific committees and working groups. One of these working groups is the Smart Grid Cybersecurity Committee (SGCC), previously called the Cybersecurity Working Group (CSWG). SGCC identifies and analyzes security requirements, and develops risk mitigation strategies to ensure the security and integrity of the smart grid. SGCC established the following objectives:

1. Assess Smart Grid Interoperability Panel (SGIP)-identified standards within an overall risk assessment framework that focuses on cybersecurity within the smart grid.
2. Develop a set of recommended security requirements strategists, designers, implementers, and operators of the smart grid (e.g., utilities, equipment manufacturers, regulators) can use as input to their risk assessment process and other tasks in the security lifecycle of a smart grid information system.
3. Identify problems and issues specific to the smart grid that currently do not have solutions.
4. Create a logical reference model for the smart grid, which will enable further work towards the creation of logical and security architecture.
5. Identify inherent privacy risk areas and feasible ways in which those risks may be mitigated, while simultaneously supporting and maintaining the value and benefits of the smart grid.
6. Develop a conformity assessment program for security requirements in coordination with activities of the SGIP Smart Grid Testing and Certification Committee (SGTCC). [33]

Staffed by volunteer members, the SGCC currently has six active and several dormant subgroups, each charged with a different focus on specific issues. Below is a list of the current working groups and a brief description of each of their focus areas and/or projects:

1. **Architecture Subgroup** – Continue the refinement of smart grid cybersecurity architecture in coordination with the SGIP SGCC on the European Union architecture harmonization effort.

2. **Cloud Computing in Smart Grid** – Identify and address the unique cybersecurity issues of using and managing smart grid applications that utilize cloud computing.

3. **High-Level Requirements (HLR) Subgroup** – Maintain the high-level security requirements outlined in the NISTIR 7628, and develop mappings and other analyses between NISTIR 7628 and other documents, standards, and/or guidelines.

4. **Privacy Subgroup –** Identify and describe privacy risks and concerns within developed or emerging interoperability standards for the smart grid, and thereby identify the most appropriate and feasible practices for mitigating the identified risks.

5. **Risk Management Process (RMP) Case Study Subgroup** – Complete a case-study narrative to accompany the DOE's Cybersecurity RMP guideline.

6. **Standards Subgroup** – Assess cybersecurity requirements associated with SGIP-identified smart grid standards and other industry cybersecurity documents. The Standards Subgroup is responsible for examining candidate standards and prepares recommendations regarding cybersecurity issues such as security management, security architecture, encryption, etc. [33]

4.3 U.S. Roadmap to Achieve Energy Delivery Systems Cybersecurity

The Roadmap to Achieve Energy Delivery Systems Cybersecurity, released in 2011 by the DOE, seeks to enhance the security and reliability of the nation's energy infrastructure. The Energy Sector Control Systems Working Group developed the 2011 Roadmap to signify a continued effort through public and private stakeholder collaboration to identify steps to build, deploy, and improve cybersecurity systems of computer-based systems that manage processes in the electric, oil, and natural gas industries. The 2011 Roadmap is a follow on and an update to the 2006 Roadmap to Secure Control Systems in the Energy Sector report. The 2006 Roadmap outlined a strategic framework for designing, installing, operating, and maintaining a resilient energy delivery system capable of surviving a cyber-attack over the next decade for the various industry, vendors, academia, and government stakeholders in the control systems community. The 2006 Roadmap was the beginning of a national and international collaborative public-private partnership for increasing cybersecurity in the energy sector. [29] [30]

4.3.1 Roadmap Scope

The updated 2011 Roadmap scope included:

- Electricity, oil, and natural gas sectors
- Production, transmission, distribution, and delivery of energy to consumers
- 10-year timeframe segmented into near-, mid-, and long-term efforts
- Risk as a function of threat, vulnerability, and consequence
- Prevention, detection, response, and recovery efforts
- Cyber disruption caused by unintentional incidents, intentional cyber-attacks, and attacks against the cyber-physical interface

The update from the 2006 Roadmap to the 2011 Roadmap reflects cybersecurity and other technology advances and the evolving needs of the energy sector. The update also:

Changing Landscape – Addresses the issue of the constantly changing landscape such as the smart technologies (e.g., smart meters, pharos measurement units), new infrastructure components, use of mobile devices, and new applications that are being used to communicate information and control energy systems. The need for the update is to communicate new viable vulnerabilities along with mitigation migration methods to protect the consumer and the energy market information.

Building on Success and Addressing Gaps – Continues to build from the previous Roadmap in areas that include providing a solid foundation for public and private programs, R&D investments, interoperability and cybersecurity-related standard development and implementation, training, and product development. The update includes new priorities identified by the community participants: enhancing vulnerability disclosure, innovative partnership to optimize stakeholders' limited time and resources, effectively measuring progress of milestones, and addressing gaps to further advance today's technologies.

Advancing Threat Capabilities – Continues to recognize adversary cyber threats on energy delivery systems and that the threats are becoming increasingly innovative, complex, and sophisticated. Adversaries progressively seek innovative techniques to exploit flaws and vulnerabilities in system components, telecommunication methods, and operating systems to sabotage and create a security event.

Emphasizing a Culture of Security – Continues to recognize that a robust energy delivery system is more than compliance with standards, but also is focused on security. Beyond the framework of regulations and standards within industry and communities, it is important to train personnel to develop and implement security policies, procedures, and technologies tailored to the energy delivery system's operational environment.

4.3.2 Strategic Framework

Figure 8 outlines the overall strategies pursued to achieve the energy sector's vision of having designed, installed, operated, and maintained resilient energy delivery systems that will survive a cyber incident while also sustaining critical system functions. The challenges/barriers described in Figure 8 are not prioritized and do not include all of the challenges that must be overcome; each energy sector varies based on its vision. The five strategies (Build a Culture of Security, Assess and Monitor Risk, Develop and Implement New Protective Measures to Reduce Risk, Manage Incidents, and Sustain Security Improvements) form the core of the strategic framework associated with milestones and time frames. The framework coordinates efforts in both the public and private sectors for projects currently underway and new projects related to advancing energy delivery system security.

Build a Culture of Security – Figure 9 describes the culture of security strategy associated with the milestones and timeframe to achieve cybersecurity practices that are reflexive and expected among all energy sector stakeholders. By building a culture of security, citizens and stakeholders take part in a dialogue to define the meaning of security and the possible level of consequences of operating under a certain level of risk. When operating under reliable practices and with a culture of security, risk management practices are continuously reviewed and challenged against standards to ensure the energy delivery system is effective against emerging threats and risks.

Assess and Monitor Risk – Figure 10 describes the strategies for assessing and monitoring risk to achieve the security goal of wide adoption by energy asset owners and operators of continuous monitoring of the security state of all energy delivery system architecture levels and across cyber-physical domains. Assessing and monitoring risks enables a company to have a thorough understanding of its current security posture. This information supports a continuous assessment of cyber threats and vulnerabilities, risks, and responses to those risks. It identifies milestones and timeframes to achieve the intended goal, along with the associated barriers and priorities.

Vision	**By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.**				
Barriers	• **Cyber threats are unpredictable and evolve faster than the sector's ability to develop and deploy countermeasures** • **Security upgrades to legacy systems are limited by inherent limitations of the equipment and architectures** • **Performance/acceptance testing of new control and communication solutions is difficult without disrupting operations** • **Threat, vulnerability, incident, and mitigation information sharing is insufficient among government and industry** • **Weak business case for cybersecurity investment by industry** • **Regulatory uncertainty in energy sector cybersecurity**				
Strategies	**1. Build a Culture of Security**	**2. Assess and Monitor Risk**	**3. Develop and Implement New Protective Measures to Reduce Risk**	**4. Manage Incidents**	**5. Sustain Security Improvements**
Near-term Milestones (0–3 years) By 2013	1.1 Executive engagement and support of cyber resilience efforts 1.2 Industry-driven safe code development and software assurance awareness workforce training campaign launched	2.1 Common terms and measures specific to each energy subsector available for baselining security posture in operational settings	3.1 Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available	4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available 4.2 Tools to support and implement cyber attack response decision making for the human operator commercially available	5.1 Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders 5.2 Federal and state incentives available to accelerate investment in and adoption of resilient energy delivery systems
Mid-term Milestones (4–7 years) By 2017	1.3 Vendor systems and components using sophisticated secure coding and software assurance practices widely available 1.4 Field-proven best practices for energy delivery systems security widely employed 1.5 Compelling business case developed for investment in energy delivery systems security	2.2 Majority of asset owners baselining their security posture using energy subsector specific metrics	3.2 Scalable access control for all energy delivery system devices available 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented	4.3 Incident reporting guidelines accepted and implemented by each energy subsector 4.4 Real-time forensics capabilities commercially available 4.5 Cyber event detection tools that evolve with the dynamic threat landscape commercially available	5.3 Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners 5.4 Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining
Long-term Milestones (8–10 years) By 2020	1.6 Significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry	2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available	3.4 Self-configuring energy delivery system network architectures widely available 3.5 Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions 3.6 Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented	4.6 Lessons learned from cyber incidents shared and implemented throughout the energy sector 4.7 Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available	5.5 Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems 5.6 Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector
Goals	**Cybersecurity practices are reflexive and expected among all energy sector stakeholders**	**Continuous security state monitoring of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators**	**Next-generation energy delivery system architectures provide "defense in depth" and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident**	**Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment**	**Collaboration between industry, academia, and government maintains cybersecurity advances**

Figure 8. Strategies for Achieving Energy Delivery Systems Cybersecurity [30]

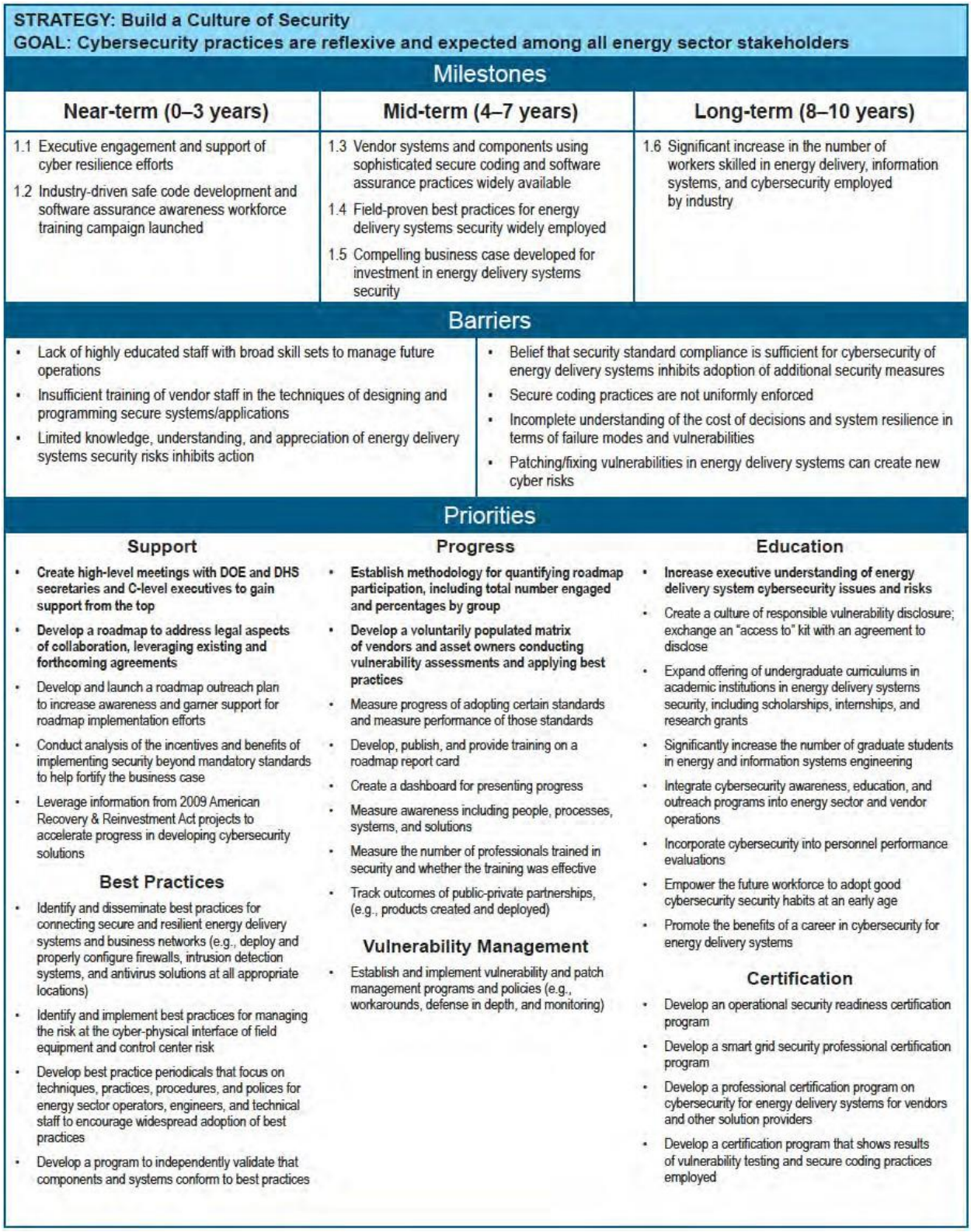

Figure 9. Building a Culture of Security Strategy [30]

STRATEGY: Assess and Monitor Risk

GOAL: Continuous security state monitoring of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators

Milestones

Near-term (0–3 years)	Mid-term (4–7 years)	Long-term (8–10 years)
2.1 Common terms and measures specific to each energy subsector available for baselining security posture in operational settings	2.2 Majority of asset owners baselining their security posture using subsector specific metrics	2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available

Barriers

- Risk factors (threat, vulnerability, and consequence) are not consistent and widely accepted by all energy sector stakeholders
- Baseline security postures of energy delivery systems in operational settings are not consistent and widely accepted by all energy sector stakeholders
- Threats, vulnerabilities, and consequences are uncertain and ambiguous factors of risk, which need to be addressed to manage risk
- Threats change with time and are hard to quantify, making it difficult to understand and properly categorize threat actors and timing of potential attacks
- Difficult to provide actionable and timely information and visualizations of security posture from vast quantities of disparate data from a variety of sources and levels of granularity
- Increasing complexity and interconnections with enterprise, telecommunications, environmental, safety, and smart networks can introduce the vulnerabilities of these systems to energy delivery systems

Priorities

Risk Factors and Levels

- **Develop key metrics to describe relative security posture before and after deployment of security solution**
- **Develop and achieve a consensus on scientifically defensible terms and measures for testing and baselining energy delivery systems security**
- Describe energy delivery system cyber risk levels according to current mitigation need
- Establish levels of risk for energy asset owners and develop a strategic implementation plan to gain widespread adoption
- Quantify trustworthiness and risk within a component, system, and "system of systems"
- Develop methods to better identify and characterize threats
- Develop appropriate threat actor models (expertise/motivation/attack vector)
- Develop deceptive reasoning algorithm(s) to counter plausibility, assertions, and threat hypotheses
- Characterize a set of threat scenarios and metrics for assessing energy delivery systems risk
- Develop industry attack surface metrics released annually with industry agreed upon parameters
- Define security and results in terms of prevent, detect, and respond

Risk Methodologies and Tools

- Employ resources for assessing energy delivery systems risk using consistent criteria within the context of each energy subsector
- Assess energy delivery systems risk using consistent criteria for the energy sector as a whole to help the sector and individual entities baseline their security posture
- Develop risk assessment tools that include methodologies for assessing vulnerabilities, frameworks for prioritizing control measures, and means for justifying costs
- Develop tool sets for asset owners to assess and benchmark energy delivery systems risk
- Develop methods to measure risk based on uncertain threats
- Create a risk-level matrix that balances threat, vulnerability, and consequence
- Develop engineering decision making tools for optimizing security
- Develop a distributed security state estimator that is tailored to multiple users and used by autonomous agents
- Develop time-to-deploy models for risk mitigations based on asset inventory
- Develop data driven ability to determine how and which vulnerabilities and threats should be addressed; track financial losses resulting from cyber incidents; and develop ability to trace vulnerabilities to financial losses

Security State Monitoring

- **Develop real-time security status visualization tools to baseline security states and compare security posture after implementation of new solutions**
- **Develop modeling and simulation tools that have dynamic automated capabilities to discover implication of complexities and inform risk management decisions**
- Develop real-time security state monitoring of energy delivery network support systems (uninterruptable power supply, environmental, emergency power, safety, and telecommunication systems)
- Develop real-time security state monitoring of new and legacy system applications
- Develop visualization technologies that integrate and correlate multiple data streams
- Create an upgradable dashboard for presenting security posture benchmarks of asset owner energy delivery system applications
- Develop methods to reduce data quantities to actionable levels
- Develop modeling and simulation tools for device management and control
- Develop network management/control at mesh-network (smart grid) scale (millions of devices)
- Develop tools for visualizing smart grid functions at transmission control centers
- Develop large-scale, high-resolution, multi-infrastructure modeling and simulation tools

Figure 10. Assess and Monitor Risk Strategy [30]

Develop and Implement New Protective Measures to Reduce Risk – Figure 11 describes the strategies for developing and implementing new protective measures to reduce risk to achieve the security goal of next-generation energy delivery system architectures that provide "defense-in-depth" and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident. New protective measures developed and implemented will reduce risk including against related vulnerabilities and their consequences, as well as emerging threats that are identified or anticipated. These new measures are built into next-generation energy delivery systems, and appropriate solutions are developed for legacy systems. The milestones and timeframes to achieve the intended goal are identified, along with the associated barriers and priorities.

Manage Incidents – Figure 12 describes the strategies for managing cyber-related incidents to achieve the security goal of enabling energy sector stakeholders to mitigate a cyber incident as it unfolds, quickly return to normal operations, and develop lessons learned from both incidents and changes in the energy delivery system environment. An emerging intentional cyber assault can be sophisticated and dynamic, making any system vulnerable, so absolute security is not always possible. Preventive and proactive measures can help to prevent a cyber incident, but when they do fail, the impact of the incident on the energy delivery system can be minimized through additional capabilities for detection, remediation, recovery, and restoration. A post-incident analysis and forensics capability is also imperative to enable energy sector stakeholders to learn and build from the incident. The milestones and timeframes to achieve the intended goal are identified, along with the associated barriers and priorities.

Sustain Security Improvements – Figure 13 describes the strategies for sustaining security improvements to achieve the goal of collaborating among industry, academia, and government to maintain cybersecurity advances in the energy delivery system environment. Collaboration among stakeholders in the energy sector provides access to resources and incentives to help sustain aggressive and proactive energy delivery system security improvements. It identifies the milestones and timeframes to achieve the intended goal, along with the associated barriers and priorities.

STRATEGY: Develop and Implement New Protective Measures to Reduce Risk

GOAL: Next-generation energy delivery system architectures provide "defense in depth" and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident

Milestones

Near-term (0–3 years)	Mid-term (4–7 years)	Long-term (8–10 years)
3.1 Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available	3.2 Scalable access control solutions for all energy delivery system devices available 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented	3.4 Self-configuring energy delivery system network architectures widely available 3.5 Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions 3.6 Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented

Barriers

- Difficult to provide quality data and robustness without introducing latency issues
- Performance/acceptance testing of energy delivery systems, networks, architectures, and components without disrupting real-time operations is difficult
- System architectures are widely distributed and complex
- Complexity of energy delivery systems increases exponentially with an increase in number of nodes
- Protective systems are not as fast as attack systems
- Security upgrades hard to retrofit to legacy systems, may be costly, and may degrade system performance

Priorities

Resilience Testing and Validation

- Develop security acceptance testing capability for evaluating security robustness of next-generation energy delivery systems, networks, architectures, and components; including architectures and guidelines for the capability
- Develop tools for automated code review in both static and runtime environments
- Develop a real-time adaptive security infrastructure that makes authorization and policy management an on-demand service for all systems and devices
- Develop tools to evaluate candidate architectures, concepts, and protocols before devices are built
- Develop security validation test beds

Systems

- **Developers and operators implement a systems approach to building, integrating, and operating resilient energy delivery systems**
- **Develop a nonbootable patching (hot patching) capability for the overall system**
- **Leverage existing robust platform-level solutions, such as those used in military applications**
- Develop safe harbor designs to prevent cascading failures
- Develop provisioning guidance to managing change in the configuration of energy delivery system environments
- Develop tools for secure change management across widely distributed systems
- Future-proof security capabilities
- Develop methods to streamline security administration
- Define security life cycle procurement specifications to guide vendor product development
- Improve understanding of interoperability requirements and needs

Access and Communications

- **Adopt agreed upon, available intrinsic data and source integrity in SCADA/EMS protocols to develop control systems that will inherently respond to and defend themselves against internal and external threats**
- **Develop techniques to provide explicit, managed communications trust**
- Develop software architectures that can isolate the impact of exploited vulnerabilities
- Develop adaptive assured quality of service protocols to support real-time data delivery
- Develop advanced cryptographic key management methods for securing millions of devices
- Develop trusted platform modules and trusted network connections for real-time communications that are nonproprietary
- Develop technology for one-over-one configuration changes by network administration (2-key rule) for insider assurance
- Develop end point security to protect against insider threat
- Develop scalable built-in security for embedded operating systems
- Develop capability to integrate new security technologies at the micro-level
- Develop white list capabilities for applications and communications
- Improve understanding of interoperability requirements and needs
- Develop cybersecurity solutions for the cyber-physical interface
- Continue to develop emerging technologies that meet security and privacy requirements

Figure 11. Development of Implementing New Protective Measures To Reduce Risk Strategy [30]

STRATEGY: Manage Incidents

GOAL: Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment

Milestones

Near-term (0–3 years)	Mid-term (4–7 years)	Long-term (8–10 years)
4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available	4.3 Incident reporting guidelines accepted and implemented by each energy subsector	4.6 Lessons learned from cyber incidents shared and implemented throughout the energy sector
4.2 Tools to support and implement cyber attack response decision making for the human operator commercially available	4.4 Real-time forensics capabilities commercially available	4.7 Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available
	4.5 Cyber event detection tools that evolve with the dynamic threat landscape commercially available	

Barriers

- Forensic systems are not as fast as attack systems
- Value proposition (and time function) of data as it relates to decision process is not well understood
- Difficult to recognize an incident once it is under way
- Traditional information technology solutions can disable or shut down energy delivery systems
- Unclear roles and responsibilities among stakeholders limits lessons learned after a cyber incident

Priorities

Intrusion Detection, Response, and Recovery Tools and Techniques

- **Develop real-time assisted detection, containment, remediation, and recover/ restoration actions in response to a cyber incident**
- Develop ability to contain attack while response and recovery measures are under way
- Develop ability to contain successful intrusions by establishing electronic security perimeter (ESP) compartmentalization techniques
- Use both cyber- and physical- state information in developing automated and assisted response capabilities
- Adapt intrusion prevention system for more robust application to network and application
- Develop and deploy sensor systems with mechanisms to detect and report anomalous activity
- Develop intrusion detection systems that incorporate chaos theory
- Develop methods to identify whether an incident will escalate to a national-scale incident
- Develop capabilities to measure the degree of resilience, including the cyber/physical impacts of a cyber incident

Lessons Learned

- Use existing Federal and private sector resources to identify existing incident reporting guidelines (both mandatory and voluntary) and best practices
- Use existing public-private partnerships to establish an easy to follow approach to incident reporting for the entire energy sector
- Develop capabilities that enable automated collection of security information, including incident reports and visualization tools for correlation
- Develop ability to conduct real-time forensics
- Develop audit trail capability for intrusion detection systems to enable automated reporting
- Develop a common system for reporting incidents by sector

Incident Management Training

- Provide operational energy delivery systems security training using a common and comprehensive set of simulation tools
- Train staff on enterprise security protocol compartmentalization techniques to effectively prevent and delay propagation in response to a cyber incident
- Set up and evaluate cyber incident and response simulators

Figure 12. Manage Incidents Strategy [30]

STRATEGY: Sustain Security Improvements
GOAL: Collaboration between industry, academia, and government maintains cybersecurity advances

Milestones

Near-term (0–3 years)	Mid-term (4–7 years)	Long-term (8–10 years)
5.1 Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders	5.3 Collaborative environments, mechanisms, and resources are available for connecting security and operations researchers, vendors, and asset owners	5.5 Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems
5.2 Federal and state incentives are available to accelerate investment in and adoption of resilient energy delivery systems	5.4 Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining	5.6 Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector

Barriers

- Bridging the technology transfer gap and accelerating progress, while addressing technology obsolescence
- Technology change is inhibited by lack of multi-disciplinary expertise, high costs, and fragmented government and industry programs
- Cybersecurity is a difficult business case
- Raising security levels is slow due to unclear roles and responsibilities among all stakeholders
- Limited understanding of how to share and what to do with vulnerability information
- Private sector partners have limited time and/or resources to invest in partnership efforts that do not provide meaningful and clear benefits to the company; government demands on their time appear to be growing while the workforce is being streamlined
- New regulations may impose requirements with unintended consequences
- Insufficient sharing of threat and incident information among government and industry entities

Priorities

Innovative Partnerships

- **Develop a forum and/or clear process for bringing the right people to the table for vulnerability reporting, analysis, and response information**
- **Develop a matchmaking forum to connect researchers, vendors, and asset owners to accelerate research from concept to commercialization**
- **Develop mechanisms for utility and vendor engagement for pilot research studies to address the business case up front**
- **Create a forum for industry to detail and request R&D topics**
- **Require diverse (academic, lab, industry) participation to receive funding**
- Provide dedicated resources and long-term commitments to address the most serious and complex issues that require longer term resource investment to bring solutions to market
- Create a protocol for working with partners including suppliers, law enforcement, etc.
- Initiate policy and collaboration mechanisms to accelerate the availability of cybersecurity solutions for the energy sector

Investment

- Implement effective incentives through federal and state governments to accelerate investment in secure energy delivery system technologies and practices
- Create appropriate incentives to invest in energy delivery systems security and resilience improvements
- Conduct analysis of incentives and benefits of implementing security to help fortify the business case
- Develop cost/benefit case studies and a mechanism to share them across the sector

Vulnerability Disclosure

- **Create a matrix of three critical vulnerability disclosure factors: who found the vulnerability, the interface list, and the degree of risk**
- **Adopt a vulnerability disclosure "Bill of Rights," which establishes roles and responsibilities of each party and communicates impacts**
- **Develop a clear, public, and industry-accepted vulnerability disclosure process**
- Support legislation that protects entities who disclose vulnerabilities in good faith to the appropriate parties

Information Sharing

- **Develop an asset inventory/configuration database to determine who has a need to know and to track configuration changes, regulatory compliance, and vulnerabilities**
- Develop standards, regulations, and/or tools for secure data exchange and communications
- Facilitate information sharing by guaranteeing protection of industry critical infrastructure protection information through legislation and other means (e.g., expedite security clearances)
- Enhance environments for securely sharing collected government information on threats and real-world attacks with asset owners and vendors
- Establish legal framework to enable effective information sharing between industry, government, and academia

Figure 13. Sustain Security Improvements Strategy [30]

4.4 U.S. Electricity Subsector (ES) Cybersecurity Capability Maturity Model (C2M2)

The DOE created the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) to improve electricity subsector cybersecurity capabilities and to understand the cybersecurity posture of the energy sector. Publicly available, the ES-C2M2 provides a mechanism to assist organizations with the evaluation, prioritization, and improvement of cybersecurity capabilities (Figure 14). The ES-C2M2 includes the core Cybersecurity Capability Maturity Model (C2M2) in addition to supplementary reference materials and implementation guidance. [32]

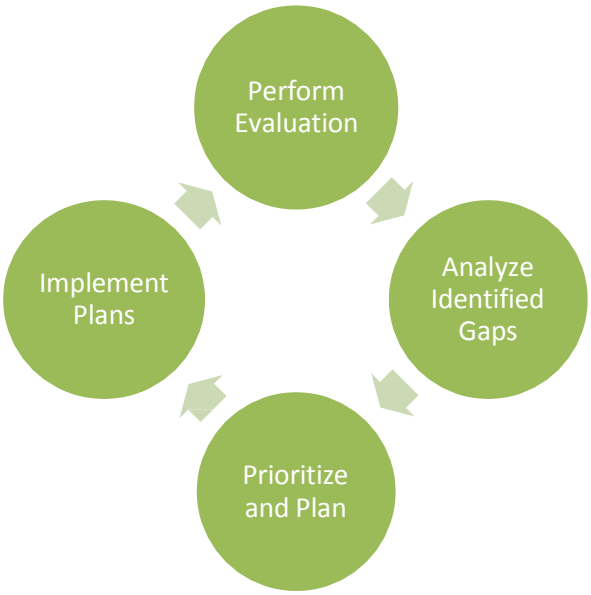

Figure 14. ES-C2M2 Process Model [32]

The model is composed of a set of common industry-vetted cybersecurity practices grouped into ten domains:

1. Risk Management
2. Asset, Change, and Configuration Management
3. Identity and Access Management
4. Threat and Vulnerability Management
5. Situational Awareness
6. Information Sharing and Communications
7. Event and Incident Response, Continuity of Operations
8. Supply Chain and External Dependencies Management
9. Workforce Management
10. Cybersecurity Program Management [32]

Each domain is arranged according to maturity level. The model defines four maturity indicator levels (MILs), ranging in value from MIL0 through MIL3, which are independently applied to

each of the ten domains, thus defining a dual progression of approach and institutionalization maturity. The management practices for each MIL are:

- **MIL0** – This model contains no practices. Performance at MIL0 indicates MIL1 in a given domain has not been achieved.
- **MIL1** – Initial set of domain practices are performed irregularly or in an ad hoc manner. In addition, at the organizational level, there is a lack of documentation of organizational practices, guidance, or lessons learned, thereby resulting in approaches and outcomes that are difficult to repeat or improve.
- **MIL2** – Practices within the domain are performed in accordance with facility documentation. Practice Stakeholders are identified and involved. Further, there are adequate resources (people, funding, and tools) provided to support the process, and documentation (e.g., standards, guidelines, references) has been identified to guide the implementation of domain practices. Overall, practices within MIL2 are more complete than MIL1, are performed regularly and in accordance to documentation, and lend confidence that the performance of domain practices will be sustained over time.
- **MIL3** – Practices within the domain have been institutionalized and guided by high-level organizational directives or policies, which are characteristics of sustainable performance practices. Five management practices support this progression:
    - Development of policy, organizational directives, and or governance;
    - Inclusion in policies of compliance requirements for specified standards and/or guidelines;
    - Activities that are periodically reviewed to ensure they conform to policy;
    - Responsibility and authority for performing domain practices assigned to personnel; and
    - Personnel performing the practices demonstrate adequate knowledge and skills. [32]

The ES-C2M2 is for use by an organization to consistently evaluate its cybersecurity capabilities, communicate its capability levels in meaningful terms, and inform the prioritization of its cybersecurity investments. An organization performs an evaluation against the model, uses that evaluation to identify capability gaps, prioritizes those gaps, develops plans to address them, and finally implements plans to address the identified gaps. As plans are implemented, business objectives change and the risk environment evolves, so the process repeats. Table 1 provides a succinct outline of the ES-C2M2 process. [32]

Table 1. ES-C2M2 Process [32]

	Inputs →	Activities →	Outputs
Perform Evaluation ↓	1. ES-C2M2 Self-Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	• Conduct ES-C2M2 Self-Evaluation Workshop with appropriate attendees	ES-C2M2 Self-Evaluation Report
Analyze Identified Gaps ↓	1. ES-C2M2 Self-Evaluation Report 2. Organizational objectives 3. Impact to critical infrastructure	• Analyze gaps in organization's context • Evaluate potential consequences from gaps • Determine which gaps need attention	List of gaps and potential consequences
Prioritize and Plan ↓	1. List of gaps and potential consequences 2. Organizational constraints	• Identify actions to address gaps • Cost-benefit analysis (CBA) on actions • Prioritize actions (CBA and consequences) • Plan to implement prioritize actions	Prioritized implementation plan
Implement Plans	1. Prioritized implementation plan	• Track progress to plan • Reevaluate periodically or in response to major change	Project tracking data

4.5 Organization for Security and Co-operation in Europe (OSCE)

The Organization for Security and Co-operation in Europe (OSCE) is the world's largest security-oriented intergovernmental organization. The OSCE mission includes issues such as arms control and the promotion of human rights, freedom of the press, and fair elections. More specifically related to the topic, protecting critical energy infrastructure from terrorist attacks is a significant issue for OSCE. The OSCE has 57 participating States, as well as 11 partners for Co-operation, who include some of the largest producers and consumers of energy as well as strategic transit countries. [31]

The "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks on Threats Emanating from Cyberspace" report is a guideline book developed by number of subject matter experts from the public and private sector of OSCE participating States as well as the European Union and the North Atlantic Treaty Organization. This guideline book addresses the threat issue of terrorist attacks on critical energy in structure and the protection from a terrorist attack. The framework encourages the formulation and implementation of cybersecurity related to the Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP), based on a co-operative, integrated and risk-based approach, including

emphasis on achieving incident response preparedness, overall infrastructure resilience and energy reliability. The issues include risk assessment, physical security, cybersecurity, contingency planning, public-private partnerships, community engagement, and international/cross-border co-operation. [31]

Based on the "Good Practices" report [31], recommended good practices for all economies and companies operating non-nuclear critical energy infrastructure are:

1. Raising awareness of the significance of non-nuclear critical energy infrastructure and the extent to which it is threatened by cyber-related terrorist attacks, as well as considering other potential threats.
2. Promoting national and international co-operation among public agencies, owners, and operators of non-nuclear critical energy infrastructure to face the threat of cyber-attacks on facilities.
3. Facilitating information exchange between public agencies and the operators of non-nuclear critical energy infrastructure regarding ways of addressing the threat of cyber-attacks on facilities.
4. Using existing national and international community forums and, if appropriate, creating standardized national/international community forums and frameworks. The purpose would be to address cyber-related terrorist attacks on non-nuclear critical energy infrastructure by considering coordinated measures such as raising awareness, conducting outreach, partnering with industry, and implementing adequate regulations.

Figure 15 illustrates the layout of the different non-nuclear energy infrastructures and commonly used components in the systems. A complete non-nuclear critical energy infrastructure includes the exploration for energy-bearing raw materials, energy production, transmission and distribution, storage, and final energy consumption.

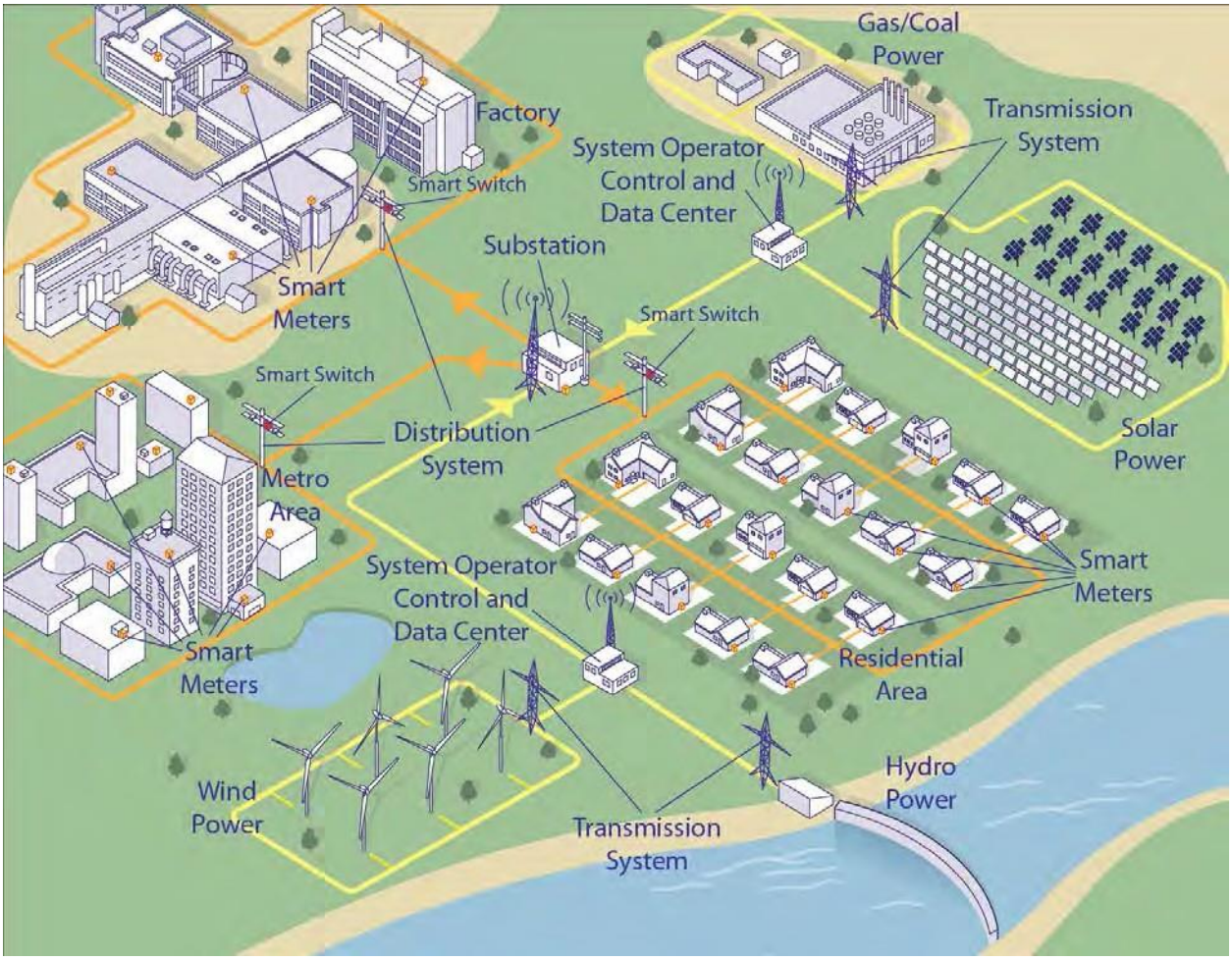

Figure 15. Layout of Electricity Non-Nuclear Energy Infrastructure and Energy Sources with Common Smart Grid Components [31]

The functions of the electricity industry are as follows:

- Transforming an energy source into electric power to produce energy. The energy sources can include products (as referenced in Figure 15) such as gas/coal (carbon based), solar, wind, and hydroelectric energy.
- Transmission and distribution are divided into two phases. Phase One includes the transport of the energy source via pipeline, ships, and trucks. Phase Two includes the transport of electrical power via power lines.
- Energy storage, similar to transmission and distribution, is also divided into two phases. Phase One includes storage of the energy source. Phase Two includes the storage of electric power. [31]
- Utilization of a portion of the generated energy in the non-nuclear critical energy infrastructure supply chain for power production. The final consumer (e.g., a household or a business) uses the power of the generated energy.

- Trading energy sources and power via trading platforms, which are necessary for international energy trade. These trading platforms all depend on information technology. The trading platforms play an important role in setting energy prices by matching demand and supply, which results in price fluctuation.
- Administration to ensure the whole supply chain functions, including management boards, Human Resources departments, service, and maintenance.

Figure 16 by the International Energy Agency (IEA) illustrates the contributing energy resources in global production in 2013. Together, the top three non-nuclear energy producers are crude oil, coal, and natural gas, which captures 81 percent of the energy resource produced globally, followed by nuclear (10 percent), and biofuels and waste (5 percent). These percentages help define the potential threat to various critical energy infrastructures by those using cyber tools to target control systems within the energy infrastructure.

Figure 16. Global Energy Production in 2013 [31]

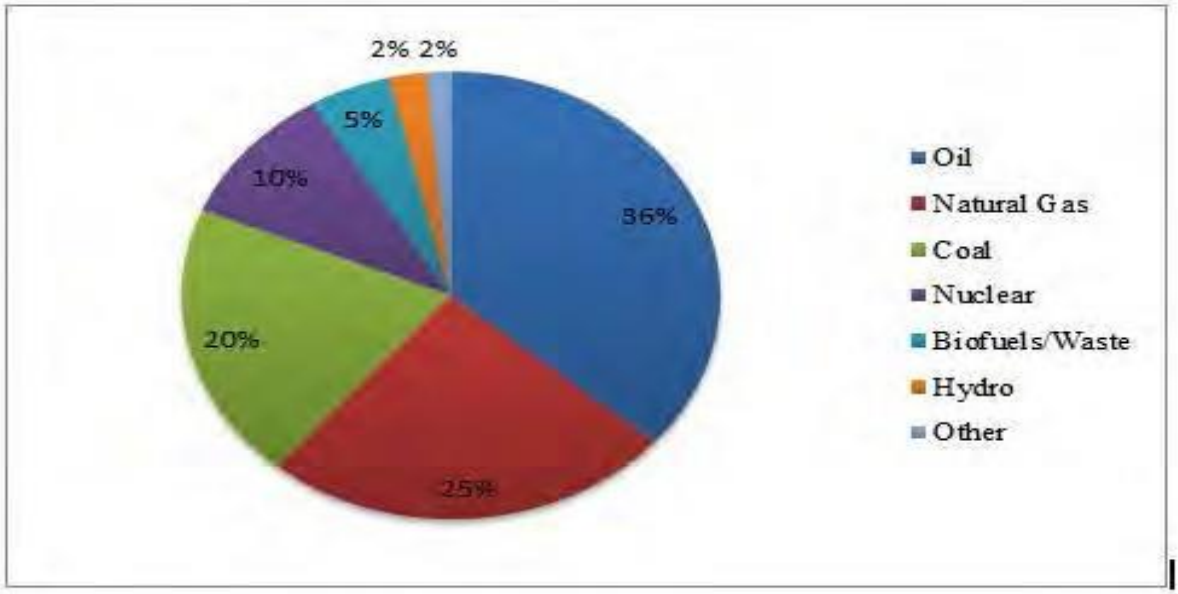

Figure 17 describes how a cyber-attack could affect a critical energy infrastructure. It also illustrates the location(s) at which an attack may occur. For example, item numbers 1 and 2 could occur either at the System Operator Control and Data Center and/or within the main energy facility. A virus (item number 3) can also represent a virus being introduced and spread throughout the cyber network infrastructure at multiple locations, whether through a component connected to the network at a remote sub-station location or in the main facility. Once the virus is present, the readings from the control unit components can be altered or affect the function of a safety feature of particular safety component. Ultimately, the end result could affect the disruption and loss of power to homes, businesses, and other consumers. Disruption or destruction of these services can have a serious impact on the security, safety, economic well-being, and health of individuals and the world as a whole. [31]

According to the OSCE, good practices adopted in the field of Information and Communication Technology (ICT) are based on the risk management and security measures framework that addresses cyber-related terrorist risks within the OSCE member States and elsewhere around the world. For comparison purposes, Figure 18 was developed from the OSCE report of known standards and best practices adopted in countries around the world. Table 2, Table 3, and Table 4 provide the member countries for OSCE, CERTs, and Reported Security Measures Adoption, respectively. All standards and best practices referenced are based on risk-based approaches compatible with risk management standards and security measures of industrial components. The standards and best practices identified are the cyber-security strategies and standards framework (ISO/IEC 27001, 27002, NIST SP 800-39, NIST SP 800-53, NIST IR 7628; NER CIP Standards CIP-002 through 009, IEC 62433, IEC 62351, FIPS 140-2; and IEEE 1402); and risk management framework (ISO/IEC 27000 family series and ISO 31000); reported security measures adoption; reported CIP framework adoption; and the European National/Government CERT adoption. [31]

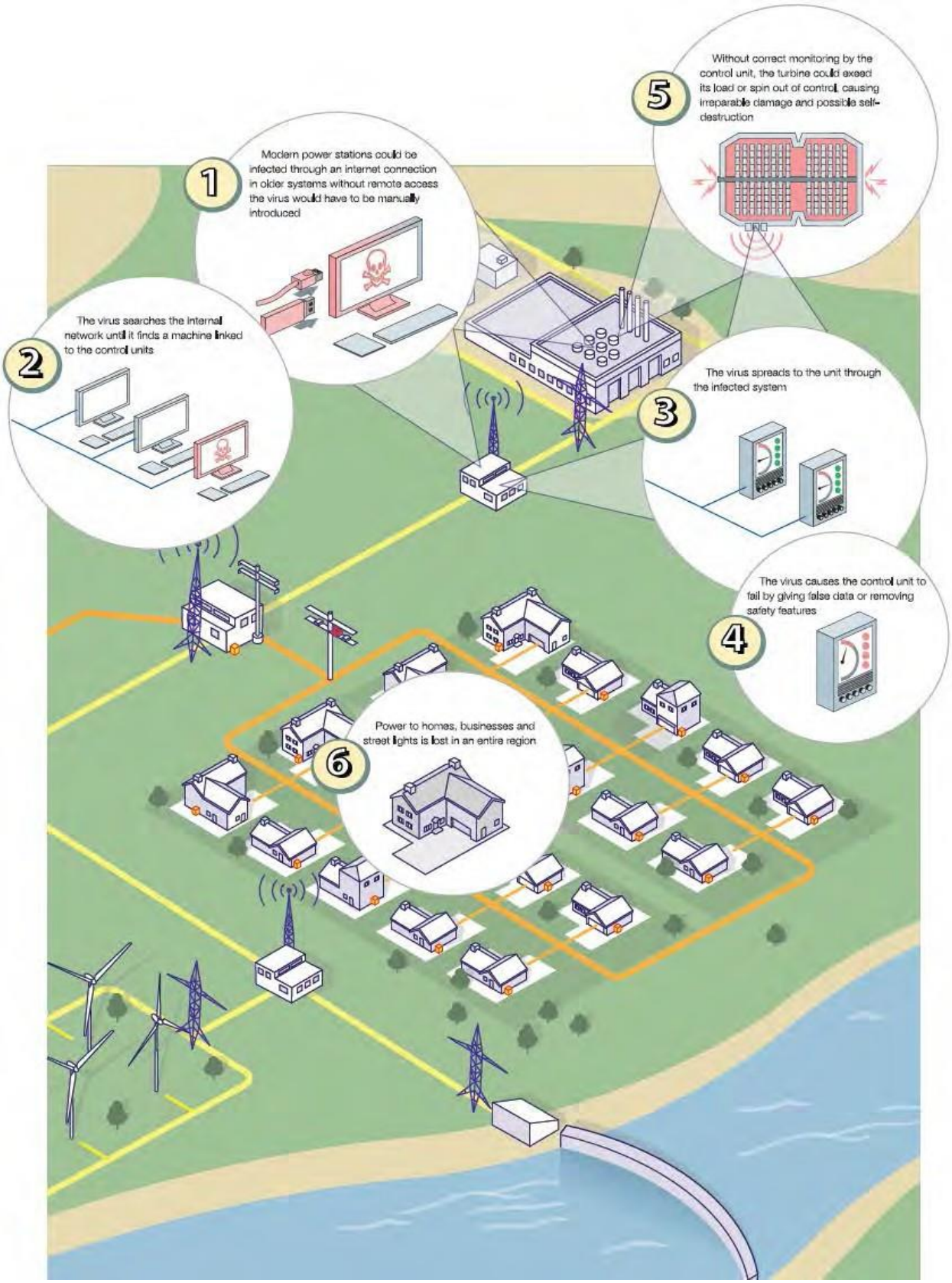

Figure 17. Effects of a Cyber-Attack on the Electric Grid [31]

No.	Threat	Explanation
1	Unauthorized use of remote maintenance access points	Maintenance access points are deliberately created external entrances to the ICS network and are often insufficiently secure.
2	Online attacks via office or enterprise networks	Office IT is usually linked to the network in several ways. In most cases, network connections from offices to the ICS network also exist, so attackers can gain access via this route.
3	Attacks on standard components used in the ICS network	Standard IT components (commercial off-the-shelf (COTS)) such as systems software, application servers or databases often contain flaws or vulnerabilities, which can be exploited by attackers. If these standard components are also used in the ICS network, the risk of a successful attack on the ICS network increases.
4	(D)DoS attacks	(Distributed) Denial-of-Service attacks can impair network connections and essential resources and cause systems to fail – in order to disrupt the operation of an ICS, for instance.
5	Human error and sabotage	Intentional deeds – whether by internal or external perpetrators – are a massive threat to all protection targets. Negligence and human error are also a great threat, especially in relation to the protection targets confidentiality and availability.
6	Introducing malware via removable media and external hardware	The use of removable media and mobile IT components of external staff always entails great risk of malware infection. See the Stuxnet case, for example.
7	Reading and writing news in the ICS network	Most control components currently use clear text protocols, so communication is unprotected. This makes it relatively easy to read and introduce control commands.
8	Unauthorized access to resources	Internal perpetrators and subsequent attacks following initial external penetration have it especially easy if services and components in the process network do not utilize authentication and authorization methods or if the methods are insecure.
9	Attacks on network components	Attackers can manipulate network components in order to carry out man-in-the-middle attacks or to make sniffing easier, for example.
10	Technical malfunctions or force majeure	Outages resulting from extreme weather or technical malfunctions can occur at any time – risk and potential damage can only be minimized in such cases.

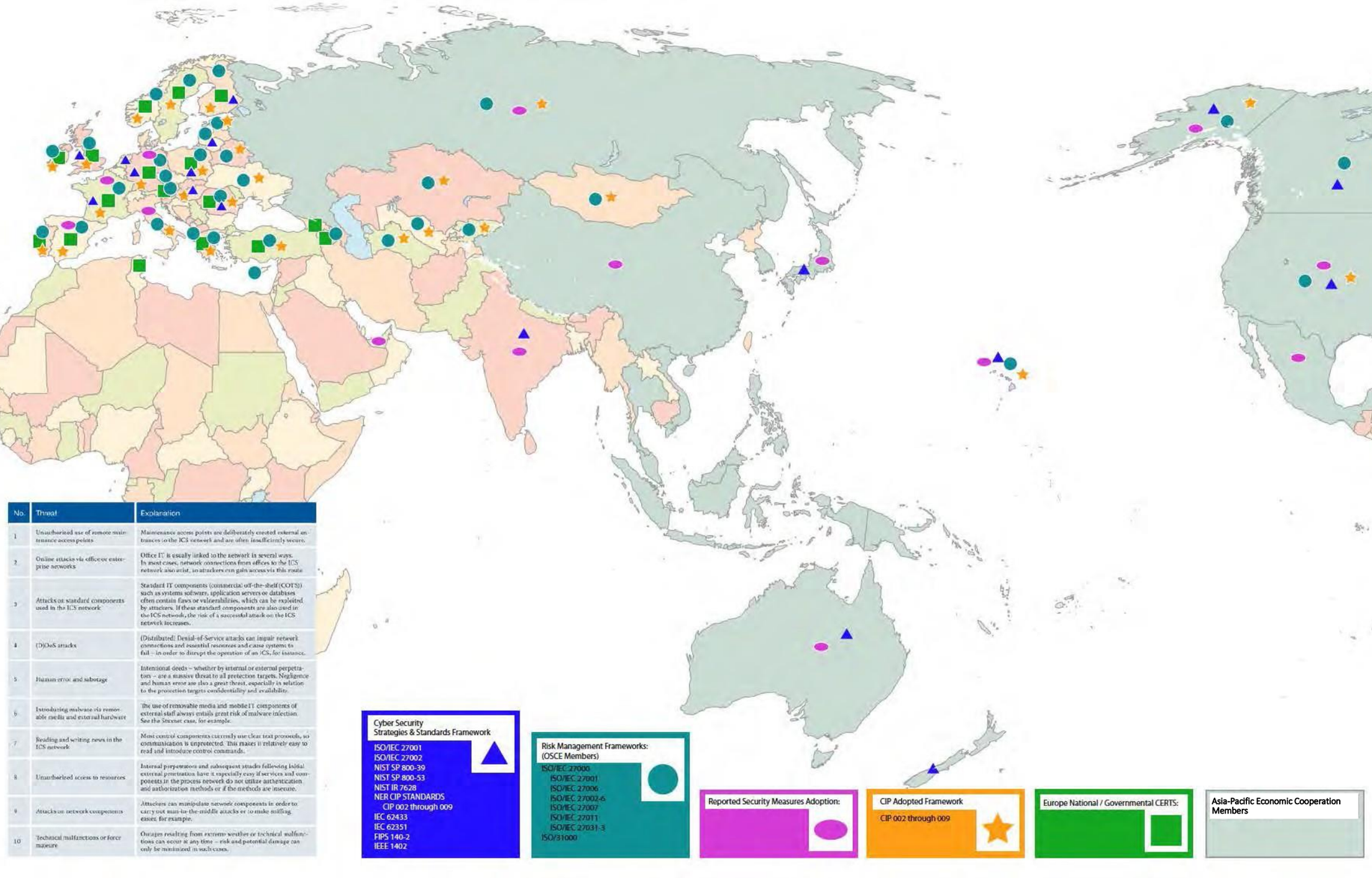

Figure 18. Globally Adopted Cybersecurity Framework [31]

Table 2. OSCE Member List

OSCE Member List				
Albania	Czech Republic	Ireland	Montenegro	Sweden
Andorra	Denmark	Italy	Netherlands	Switzerland
Armenia	Estonia	Kazakhstan	Norway	Tajikistan
Austria	Finland	Kyrgyzstan	Poland	Turkey
Azerbaijan	Former Yugoslav Republic of Macedonia	Latvia	Portugal	Turkmenistan
Belarus	France	Liechtenstein	Romania	Ukraine
Belgium	Georgia	Lithuania	Russia	United Kingdom
Bosnia / Herzegovina	Germany	Luxembourg	San Marino	United States
Bulgaria	Greece	Malta	Serbia	Uzbekistan
Canada	Holy See	Moldova	Slovak Republic	
Croatia	Hungary	Monaco	Slovenia	
Cyprus	Iceland	Mongolia	Spain	

Table 3. Europe National / Governmental CERTs

Europe National / Governmental CERTS				
Armenia	Estonia	Iceland	Malta	Slovenia
Austria	Finland	Ireland	Netherlands	Spain
Belgium	France	Israel	Norway	Sweden
Bulgaria	Georgia	Italy	Poland	Switzerland
Croatia	Germany	Latvia	Portugal	Turkey
Czech Republic	Greece	Lithuania	Romania	United Kingdom
Denmark	Hungry	Luxemburg	Slovakia	

Table 4. Reported Security Measures Adoption

Reported Security Measures Adoption				
Australia	France	Italy	Russia	United Kingdom
Brazil	Germany	Japan	Spain	United States
China	India	Mexico	UAE/Dubai	

The top 10 associated threats to which the standards and good practices apply are:

1. Unauthorized use of remote maintenance access points.
2. Online attack via office or enterprise networks.
3. Attacks on standard commercial off the shelf (COTS) components used in the ICS network.
4. Distributed Denial-of-Service attacks that can impair network connections and essential resources that can cause systems to fail.
5. Human error and sabotage or intentional deeds, from an internal or external adversary, are massive threats to protected targets.
6. Introducing malware via removable media and external hardware, which is a great risk.
7. Reading and writing news in the ICS network.
8. Unauthorized access to resources that does not use authentication and authorization protection measures/methods.
9. Attacks on network components used to carry out man-in-the-middle attacks or to simplify sniffing.
10. Technical malfunctions or force majeure. [31]

4.6 Global Smart Grid Federation (GSGF)

The Global Smart Grid Federation (GSGF), established in 2010, brings together smart grid initiatives from around the world. Over the past few years, various groups have initiated projects and programs to explore the potential of the new generation of information- and communication-based technologies emerging across the power sector. As these efforts matured, formal public-private initiatives formed. The GridWise Alliance in the United States was the first in 2003. Similar initiatives in the European Union, South Korea, Japan, Australia, Canada, India, and Ireland followed it. Many others are in the formative stages of their own initiatives. The GSGF:

- Facilitates the collaboration of national and international smart grid NGOs and governmental organizations from around the world to conduct and foster research in the application of smart grid technologies;
- Supports rapid implementation of smart grid technologies by establishing itself as the global center for competency on smart grid technologies and policy issues; and
- Fosters international exchange of ideas and best practices on energy issues including reliability, efficiency, security, and climate change to create avenues for dialogue and

cooperation between the public and private sectors in countries around the world on issues relating to the deployment of smart grid technologies.

Australia, Canada, Japan, Korea, Chinese Taipei, Mexico, and the United States are members of the GSGF. (Non-APEC Economy members include Denmark, the EU, Flanders, France, the United Kingdom, India, Norway, Ireland, Israel, the Netherlands, and Turkey.)

4.7 ISGAN (International Energy Agency [IEA] Implementing Agreement for a Co-operative Program on Smart Grids)

The International Smart Grid Action Network (ISGAN) is a mechanism for multilateral government-to-government collaboration to advance the development and deployment of smarter electric grid technologies, practices, and systems. It aims to improve the understanding of smart grid technologies, practices, and systems and to promote adoption of related enabling government policies.

ISGAN launched at the first Clean Energy Ministerial (CEM), a meeting of energy and environment ministers and stakeholders from 23 countries and the European Union held in Washington, D.C on July 19 and 20, 2010. The CEM focuses on high-level attention and commitment to concrete steps—both policies and programs—that accelerate the global transition to clean energy. The Ministerial was an outgrowth of the agreement at the Major Economies Forum on Energy and Climate (MEF) in L'Aquila, Italy in July 2009, where countries agreed to collaborate on advancing clean energy technologies.

ISGAN facilitates dynamic knowledge sharing, technical assistance, and project coordination, where appropriate. ISGAN participants report periodically on progress and projects to the Ministers of the Clean Energy Ministerial, in addition to satisfying all IEA Implementing Agreement reporting requirements. Membership in ISGAN is voluntary and currently includes Australia, Austria, Belgium, Canada, China, Denmark, European Commission, Finland, France, Germany, India, Ireland, Italy, Japan, Korea, Mexico, the Netherlands, Norway, Russia, Singapore, South Africa, Spain, Sweden, Switzerland and the United States.

Though the primary focus is on government-to-government cooperation, ISGAN is also open to entities designated by participating governments, and select private sector and industry associations and international organizations. To work as efficiently as possible, ISGAN has established strong cooperative ties with existing smart grid organizations.

ISGAN recognizes that robust, reliable, and smart electric grids play a key role in enabling greenhouse gas (GHG) emission reductions through the management of electricity demand, integration of growing supplies of both utility-scale and distributed, small-scale renewable energy systems, accommodation of an increasing number of electric and plug-in hybrid electric

vehicles, improvement of operational efficiency, and application of energy efficient technologies to their full potential. Smart grids also enable better utilization of existing electricity generation assets, thereby creating opportunities to forgo the addition of new long-lived, high emissions fossil fuel plants. In coordination with the International Energy Agency (IEA) and others, ISGAN seeks to improve understanding of the potential for smart grid technologies to enable reductions in GHG emissions and energy use at country, regional, and global levels. It focuses high-level government attention on the promise of smart grid to achieve such reductions as well as the challenges to accelerating their deployment.

ISGAN's vision is to accelerate progress on key aspects of smart grid policy, technology, and related standards through voluntary participation by governments in specific projects and programs. ISGAN will facilitate dynamic knowledge sharing, technical assistance, peer review and, where appropriate, project coordination among participants. ISGAN activities center on those aspects of the smart grid where governments have regulatory authority, expertise, convening power, or other leverage, focusing on five principal areas: 1) policy standards and regulation, 2) finance and business models, 3) technology system development, 4) workforce skills and knowledge, and 5) users and consumer engagement.

4.8 UN Group of Governmental Experts (UN GGE)

Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Russia, South Korea, Spain, the United Kingdom, and the United States participate in the UN GGE4 (2014/2015).

In 2013, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security released a report on information security. The Group formed in 2012. In its resolution establishing the group, "Developments in the field of information and telecommunications in the context of international security", the General Assembly requested that a group of governmental experts be established on the basis of equitable geographical distribution. The General Assembly requested it to study existing and potential threats in the sphere of information security and possible cooperative measures to address them including norms, rules or principles of responsible behavior of States and confidence-building measures with regard to information space, as well as the concepts aimed at strengthening the security of global information and telecommunications systems. They also tasked the Group to take into account the assessments and recommendations of a previous group from 2010 (A/65/201). The General Assembly asked the Secretary General to submit a report on the results of the study to it at its sixty-eighth session.

Appointed experts came from 15 States: Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, the United Kingdom of Great Britain and Northern Ireland and the United States of America. The Group of

Governmental Experts had a comprehensive, in-depth exchange of views on developments in the field of information and telecommunications in the context of international security over three sessions in 2012/2013.

The 2010 report had recommended further dialogue among States on norms pertaining to State use of ICTs to reduce collective risk and protect critical national and international infrastructure. It called for measures on confidence-building, stability and risk reduction, including exchanges of national views on the use of ICTs in conflict, information exchanges on national legislation, ICT security strategies, policies, technologies and best practices. The 2010 report stressed the importance of building capacity in States that may require assistance in addressing the security of their ICTs and suggested additional work to elaborate common terms and definitions.

The 2013 report notes that the expanding use of ICTs in critical infrastructures and industrial control systems creates new possibilities for disruption. The rapid increase in the use of mobile communications devices, web services, social networks and cloud computing services expands the challenges to security.

Among several other recommendations, under Subsection IV. "Recommendations on confidence building measures and the exchange of information", the report calls for increased cooperation to address incidents that could affect ICT or critical infrastructure that rely upon ICT-enabled industrial control systems. This could include guidelines and best practices among States against disruptions perpetrated by non-State actors.

Under Subsection V. "Recommendations on capacity-building measures", the report notes that capacity building is of vital importance to an effective cooperative global effort on securing ICTs and their use. Some States may require assistance in their efforts to improve the security of critical ICT infrastructure; develop technical skill and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridge the divide in the security of ICTs and their use.

4.9 Critical Five: Forging a Common Understanding for Critical Infrastructure

The Critical Five is an international forum, established in 2012, comprised of members from government agencies responsible for critical infrastructure protection and resilience in Australia, Canada, New Zealand, the United Kingdom, and the United States. The Critical Five aims to strengthen cooperation among members to address the threats to critical infrastructure, as well as to share information, practices and ideas on domestic policy and operational approaches to critical infrastructure protection and resilience.

The March 2014 “Forging a Common Understanding for Critical Infrastructure” document outlines the shared views of the Critical 5 members with the objective of providing a high-level overview of the meaning and importance of critical infrastructure.

This project supports the ongoing effort to clearly articulate and communicate a common message on the value, purpose, and historical trajectory of this important functional domain and seeks to arrive at a common understanding of critical infrastructure and its role in society. The project identifies shared priorities and interconnections among these five countries and lays the foundation for future collaboration. The approach used is to identify similarities in definition, approach, concept, and implementation in order to arrive at a shared understanding of critical infrastructure.

In order to forge a common understanding of critical infrastructure, the Critical 5 members analyzed the definitions and the specified sectors identified in their national infrastructure plans to identify commonality and overlap to find the similarities and differences to build a bridge of common understanding among their nations and situations. While each definition of critical infrastructure is slightly different, there are common threads that run throughout. The Critical 5 proposes the following definition as the starting point for a discussion about critical, nationally significant infrastructure:

“Critical infrastructure, also referred to as nationally significant infrastructure, can be broadly defined as the systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic security, prosperity, and health and safety of their respective nations.”

The Critical 5 members have adopted an all-hazards approach to address the current and future challenges facing their infrastructure. In particular, they cite that trends like climate change and demographic shifts are likely to accelerate in the future and have an impact on infrastructure systems and assets. Since there are high consequences to service disruption, it is important for nations to address these trends as part of critical infrastructure security and resilience. In many cases, it is best to address these trends and other potential disruptors when designing the infrastructure systems and assets. Critical infrastructure, particularly built systems and assets, can have a very long lifespan, so each Critical 5 member recognizes the importance of planning for future shifts that could disrupt the services infrastructure provides.

The Critical 5 members each have established departments and offices to help manage the risks to their critical, nationally significant infrastructure (in conjunction with the owners/operators), and in an effort to increase our international cooperation, each one of the Critical 5 members has come together to build a shared narrative that outlines the similarities and differences. By forging a common understanding of what each member means by critical infrastructure security and

resilience, the members seek to find opportunities to share information and analysis as well as leverage best practices.

Each of the Critical 5 members highlights the importance of secure and resilient systems. Therefore, it is important to reach a common definition of critical infrastructure resilience. An examination of the Critical 5's strategic guidance documents finds that each of the countries recognizes resilience as the need for systems to have the capacity to be flexible and adaptable to changing conditions, both foreseeable and unexpected, and to be able to recover rapidly from disruption. Although the definition can be broadened, they proposed using this definition when discussing critical infrastructure resilience among the Critical 5 partners as the foundation of what each is trying to achieve.

Similar to critical infrastructure resilience, one can reach a common definition for critical infrastructure security. It implies the end goal of security is to use physical, personnel and/or cyber defense measures to reduce both the risk to critical infrastructure and the risk of loss due to a disruption in essential services by minimizing the vulnerability of critical infrastructure assets, systems and networks. They articulate this common goal to facilitate the discussion on how each member works to enhance secure infrastructure and resilience. Each member provides strategic guidance on the need for both critical infrastructure security and resilience. Australia, Canada, New Zealand, the United Kingdom and the United States are approaching critical infrastructure security from a national security lens – whether regarding their physical assets, cyber assets, or a combination of the two. Importantly, through each of the members' strategic documents, national, economic and societal security is the driving force behind the need for critical infrastructure security and resilience.

Each of the Critical Five members has articulated how important critical infrastructure is to promoting economic prosperity and economic security. Governments make investments in critical infrastructure –whether directly or through partnerships – in order to strengthen their economies and help their societies prosper. Critical infrastructure forms the backbone to modern society by providing essential services that help businesses grow and flourish, such as high-speed communications, modern transportation networks, and reliable energy, which facilitates trade and economic growth. Critical infrastructure services are vital to economic growth, so governments work to ensure that these services are as secure and resilient as possible. By ensuring critical infrastructure is secure and resilient, the governments can protect and increase the strength and vitality of their respective economies. When governments focus on making critical infrastructure more secure and resilient by managing risk, trust and confidence grows in the public-private relationship, which then facilitates economic growth. This trust and confidence in critical infrastructure is essential to achieving safe, secure and prosperous societies. The strategic guidance of all the Critical 5 members highlights this concept of secure and resilient infrastructure instilling confidence in investors and their businesses.

While each of the Critical 5 members has unique characteristics, the security and resilience of vital infrastructure assets and systems is the same and all members are focused on managing the risk. All of the Critical 5 members work hard to build partnerships with their individual owners and operators, each promote collaboration, information sharing, and risk management. These commonalities provide the foundation through which the security and resilience of critical infrastructure can expand internationally and build the relationships between the Critical 5 members.

Each of the Critical 5 members maintains strong partnerships with their national, regional and local government counterparts and the critical infrastructure owners and operators. These partnerships are essential, because critical infrastructures systems are owned and operated by both private and public sector stakeholders. In addition, all partners recognize the importance of being a national leader for infrastructure security and resilience, and in general, they work in similar ways to build these partnerships.

Information sharing is critical to the critical infrastructure security and resilience strategy as well, and each member strives to share timely and relevant information in a safe and trusted environment. Each member is actively engaged in building these types of trusted information sharing channels by using public facing websites, information portals and gateways, partnerships, or a myriad of other approaches. At the national level, the governments work to make their critical infrastructure more secure and resilient in order to maintain and improve upon the essential services provided by that infrastructure.

The common actions the governments take in order to promote critical infrastructure security and resilience and help deliver the essential services to their respective populations include:

- Looking across regions and using their analytical resources to identify nationally significant critical infrastructure sectors and the services they provide.
- Coordinating with public and private sector partners on how to make that infrastructure more secure and resilient.
- Sharing important and timely information with relevant stakeholders.
- Collaborating with partners and stakeholders to share best practices.
- Identifying cross-sector dependencies.
- Developing a workforce and culture that is ready to handle the complex challenges impacting critical infrastructure.
- Identifying and assessing the criticality of infrastructure.
- Using a risk management approach that identifies ways to reduce risk to critical infrastructure.

Each Critical 5 member has identified the following sectors as critical: Communications; Energy; Healthcare and Public Health; Transportation Systems; and Water (to include Wastewater and Storm Water Systems).

They accept the following definitions to form the basis of a common understanding and to help facilitate a coordinated approach to, and next steps to enhance, critical infrastructure security and resilience:

> Critical Infrastructure:
> The systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic security, prosperity, and health and safety of their respective nations (also referred to as nationally significant infrastructure).
>
> Resilience:
> Systems have the capacity to be flexible and adaptable to changing conditions, both foreseeable and unexpected, and are able to recover rapidly from disruptions.
>
> Security:
> The use of physical, personnel and/or cyber defense measures to reduce both the risk to critical infrastructure and the risk of loss due to a disruption in essential services by minimizing the vulnerability of critical infrastructure assets, systems and networks.

4.10 ASEAN REGIONAL FORUM

The ASEAN Regional Forum (ARF) provides an important opportunity for open dialogue for its participants. Its objectives, which include fostering constructive dialogue and consultation on political and security issues of common interest and concern, now encompass cybersecurity issues. At the 19th ARF meeting on July 12, 2012, foreign ministers underscored the need to coordinate to ensure security for ICT, adopted an official statement on cooperation in ensuring cybersecurity, and agreed to develop a work plan relating to cybersecurity – a first step toward possibly enacting concrete confidence building measures. After the first work plan was completed (2014-2015), the second carried on the work for 2015-1017. In addition, the forum has hosted a number of workshops on cybersecurity matters such as the use of proxy actors, cyber incident responses, and confidence building measures in cyberspace.

4.11 ASEAN

At the regional level, critical infrastructure protection will be essential for member states of ASEAN. ASEAN plans include establishing “an integrated and regional connectivity” through the following measures: a) negotiating a regional energy security framework that includes the ASEAN power grid, trans-ASEAN gas pipeline, and planned grid interconnection projects such

as the regional gas grid; b) enhancing ICT infrastructure such as the optical fiber network; and c) developing an integrated transport network including air, road, rail, and maritime links.

The ASEAN Economic Community Blueprint identifies the importance of creating a secure and connected information infrastructure, and areas of cooperation include enhanced infrastructure and communications connectivity. The higher probability of cross-border challenges and transnational crime because of closer connectivity is recognized by the 2011 Master Plan on ASEAN Connectivity and the ASEAN ICT Masterplan 2015 (AIM2015). AIM2015 charts the region's approach to developing ICT through 2015 in line with the ASEAN Community and underlines that ASEAN can achieve greater competitiveness and attract global investment if it leverages ICT collectively. The document calls for the development of a common framework for network security, the establishment of minimum standards for network security to ensure the preparedness and integrity of networks, the implementation of a network security "health screening" program, the development in all sectors of best-practice models for business continuity and disaster recovery, and the establishment of the multi-stakeholder ASEAN Network Security Action Council (ANSAC) to promote CERT cooperation and the sharing of expertise.

In line with AIM2015, the ASEAN ministers responsible for ICT agreed in November 2012, under the Mactan Cebu Declaration, to implement a number of measures. These include: 1) promoting international and regional collaboration to enhance the security of information infrastructure for "sustainable economic and social development"; 2) working toward a "conducive, safe, secured and trusted environment and harmonized ICT rules and regulations that will promote trade, investment and entrepreneurship"; 3) facilitating "robust and resilient information infrastructure" through developing and implementing national frameworks on submarine cable connectivity protection and risk mitigation; 4) further enhancing the development of policy frameworks and the sharing of best practices on the protection of data and information infrastructure in order to safeguard the network between member states; and 6) continuing collaboration among ASEAN CERTs such as ASEAN CERTS incident drills so as to enhance incident investigation and coordination in support of ANSAC's activities.

4.12 The Organization of American States (OAS)

At the regional level, according to remarks by Christopher Painter in 2012 on strengthening Cyber Security in the Americas, the OAS adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity was ahead of its time in understanding that cybersecurity was a cross-cutting issue and required the participation of stakeholders across a variety of disciplines. The OAS includes the APEC Member Economies of Canada, the United States, Mexico, Peru and Chile.

He explained that the OAS/CICTE Cyber Security program has become the main forum in the Americas for debate and the exchange of ideas about current and future cybersecurity trends. The OAS Network of CSIRTs and Cyber Security officials have allowed incident response officers to respond to cybersecurity incidents in an environment of security and trust. Additional interactions through training activities, workshops and meetings have fostered stronger lines of communication, and trust. One important feature of the CICTE cybersecurity program is the political consensus that members have shared on its importance, urgency and direction. The CICTE Secretariat also promotes the development of national cybersecurity strategies. CICTE recognizes the central role that IT plays by committing to: increasing efforts to build CSIRTs and strengthen cooperation; by continuing to build the capacity within member states to establish and implement national cybersecurity strategies; and by underscoring the importance of promoting public-private sector cooperation in support of the security of critical information infrastructures.

In his remarks, Chris Painter further explained that the Inter-American Telecommunication Commission (CITEL) works with the private sector to coordinate regional positions on telecommunications standards, radio-communication spectrum use, broadcasting, and telecommunication policy in the Americas. The Member States of the region depend heavily on CITEL to provide the mechanism for developing regional input (Inter-American Proposals) to the ITU where regional positions hold significant influence on global telecommunication decisions.

The 2012 OAS/CICTE “Declaration Strengthening Cyber-Security in the Americas”, outlined that the Declaration on Security in the Americas (Mexico, 2003) identified as salient, amongst other new threats, terrorism and attacks to cybersecurity. The 2012 Declaration committed member states to develop a culture of cybersecurity in the Americas by taking effective preventive measures to anticipate, address, and respond to cyber-attacks, whatever their origin, fighting against cyber threats and cybercrime, criminalizing attacks against cyberspace, protecting critical infrastructure and securing networked systems.

The Declaration recalls AG/RES. 1939 (XXXIII-O/03), "Development of an Inter-American Strategy to Combat Threats to Cybersecurity" and AG/RES. 2004 (XXXIV-O/04) “Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity;” bearing in mind that the OAS Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity outlines a multidimensional and multidisciplinary approach that establishes specific mandates for CICTE, CITEL, and the Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA) and its Group of Governmental Experts on cybercrime. It noted with satisfaction the extensive work carried out since 2004 by the CICTE Secretariat to implement this strategy and the Work Plan that includes the area of Protection of Critical Infrastructure and, within it, the Cybersecurity Program.

It reiterated the importance of continuing to implement the OAS Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity and the need to strengthen partnerships among all cybersecurity stakeholders. It considers that properly developing cybersecurity capabilities, frameworks, and ICT infrastructure are critical to regional, national, and individual security, and economic stability. It declared its renewed commitment to implement the OAS Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: 1) the need for member states to continue efforts to establish, and/or strengthen national CSIRTs; 2) the need to increase information sharing and cooperation among Member States related to protecting their critical information infrastructure, and preventing and responding to cyber incidents; and, 3) the importance of enhancing the security and resilience of critical ICT infrastructure against cyber threats, with a particular focus on critical governmental institutions as well as those sectors critical to national security, including energy, financial, transportation and telecommunications systems.

It also renewed its commitment to: 1) continue developing comprehensive national cybersecurity strategies and to engage all relevant stakeholders in their development and implementation; 2) promote public sector cooperation with the private sector and academia in order to strengthen the security and protection of critical ICT infrastructure; and, 3) explore future opportunities to broaden CICTE's efforts to protect critical ICT infrastructure, including by implementing capacity building programs to strengthen all critical components of the global supply chain.

In March 2015, CICTE concluded its annual meeting with a call to combat terrorist threats to critical infrastructure. It concluded the meeting with a declaration on the "Protection of Critical Infrastructure from Emerging Threats". Members of the OAS established "their commitment to identifying and combating emerging terrorist threats, regardless of their origin or motivation, such as threats to critical infrastructure, and cyber security, among others." In addition, they declared "their willingness to identify and promote, when deemed appropriate, in accordance with domestic laws, forms of public-private partnerships in the fight against terrorism, and in connection with critical infrastructure and cyber security." The 2015 work plan includes activities for the Protection of Critical Infrastructure: Cyber security; Critical Infrastructure Protection; and Global Supply Chain Security and Strengthening Strategies on Emerging Terrorist Threats: Crisis Management and workshops. The Declaration urges the OAS members who have not yet done so, "to sign, ratify, or accede to as the case may be, and to implement in an effective way, the Inter-American Convention against Terrorism and the other pertinent universal legal instruments," as well as the resolutions of the United Nations General Assembly and Security Council related to combating terrorism.

The representatives also reaffirmed their commitment to "strengthen national and multilateral efforts, to prevent, combat, and eliminate terrorist threats and attacks against critical financial,

transportation, and telecommunications infrastructure." The document expresses their commitment to strengthen international cooperation and collaboration, given the interdependent nature of critical national infrastructure.

The TrendMicro/OAS 2015 report explains that overall, OAS members have shown unity on cybersecurity issues. Working with and through the OAS, members have been able to reach an agreement on a difficult topic. OAS resolutions and declarations have engendered a collaborative atmosphere, allowing the General Secretariat of the OAS to provide technical assistance and improve member states' cybersecurity on many levels.

This page intentionally left blank

Table 5. APEC Member Participation in International Security Related Forums

APEC Member	OSCE	"Critical Five: Forging a Common Understanding for Critical Infrastructure"	ASEAN Regional Forum	ASEAN	OAS	Global Smart Grid Federation	ISGAN
Australia		Critical 5 Member Nation	Participant			Member	Member
Brunei Darussalam			Participant	Member			
Canada	Member State	Critical 5 Member Nation	Member		Member	Member	Member
Chile					Member		
China			Participant				Member
Hong Kong, China							
Indonesia			Participant	Member			
Japan			Participant			Member	Member
Malaysia			Participant	Member			
Mexico					Member	Member	
New Zealand		Critical 5 Member Nation	Participant				
Papua New Guinea			Participant				
Peru					Member		
The Philippines			Participant	Member			
Russia	Member State		Participant				Member
Singapore			Participant	Member			Member
Republic of Korea			Participant			Member	Member
Chinese Taipei						Member	
Thailand			Participant	Member			
United States	Member State	Critical 5 Member Nation	Participant		Member	Member	Member
Viet Nam			Participant	Member			

This page intentionally left blank.

5 Framework Implementation Guidance

The U.S. DOE, in partnership with the Electricity Subsector Coordinating Council (ESCC) and Oil & Natural Gas Subsector Coordinating Council (ONG SCC) along with other sector-specific agencies, worked in collaboration to develop the Framework Implementation Guidance specifically for energy sector owners and operators. The guideline is tailored to the energy sector's risk environment and existing tools and processes used by organizations for cybersecurity and risk management. The Framework Implementation Guidance is designed to assist energy sector organizations to:

- Characterize their current and target cybersecurity postures.
- Identify gaps in their existing cybersecurity risk management programs, and identify areas where current practices may exceed the intended framework implementation.
- Recognize that existing sector tools, standards, and guidelines may support the intended framework implementation.
- Effectively demonstrate and communicate their risk management approach and use of the intended framework implementation for both internal and external stakeholders. [34]
- The Framework Implementation Guidance uses ES-C2M2 tool (see Section 5.4 in this report) as an example. The guideline is structured as follows:
- **Section 2** provides key framework terminology and concepts for its application. This section helps in preparation for the framework implementation by defining terminology, concepts, and overall benefits to the current cybersecurity posture [34].
- **Section 3** identifies an overview of some of the existing cybersecurity tools, processes, standards, and guidelines already in place by an organization that may support and align with the intended framework implementation. The section may also help in demonstrating how an organization is already applying other concepts in its programs. Organizations can map their current cybersecurity approaches to the framework implementation elements to help identify potential gaps that may need to be addressed as well as highlight where the framework does not align with the organization's cybersecurity approach. [34]
- **Section 4** outlines a general approach to implement a specific framework. A seven-step process is outlined, which can be used with any cybersecurity standard, energy-sector specific tool set, or commercial tool for managing cybersecurity risk. Each step

includes inputs, activities, and outputs. The seven-step process includes the following:

  - Step 1: Prioritize and Scope
  - Step 2: Orient
  - Step 3: Create a Current Profile
  - Step 4: Conduct a Risk Assessment
  - Step 5: Create a Target Profile
  - Step 6: Determine, Analyze, and Prioritize Gaps
  - Step 7: Implement Action Plan [34]

- Section 5 uses the ES-C2M2 tool as an example to demonstrate the implementation approach of a framework to an existing specific tool. The example uses the seven-steps defined in Section 4 to implement a framework using the ES-C2M2 practices. [34]

The DOE and the stakeholders in the private sector recognize many organizations operate in multiple infrastructure sectors and, therefore, there is a need for alignment of guidance between overlapping organizations and cybersecurity approaches. The DOE and other government partners are collaborating to incorporate cross-sector overlaps. As a result, this Framework Implementation Guidance may be updated or modified to harmonize the use of the framework across different sectors. [34]

6 Asia-Pacific Economic Cooperation (APEC) Members

This section describes what is happening in APEC Member Economies. For each, this section describes its energy sectors, smart grid initiatives, current cybersecurity nexus, cybersecurity challenges, future cybersecurity nexus, and smart grids.

6.1 Australia

6.1.1 Economy Energy Resources

According to the 2014 APEC Energy Overview Study, Australia has abundant, high-quality energy resources that are expected to last for many decades at current rates of production. The energy industry is a significant contributor to the economy. Australia produces energy for both domestic consumption and export. In 2011, Australia was the world's ninth largest energy producer, accounting for approximately 2.7 percent of world energy production.

6.1.2 Smart Grid Initiatives

Australia experienced severe energy shortages in 2006-2007, one result of which was the Council of Australian Governments (COAG) committing to a national smart meter rollout plan. The state of Victoria in 2007 was the first to launch a mandatory rollout of smart meters, in which the costs associated with deployment were passed on to consumers. The public negatively received this cost-recovery method. As a result, the state postponed the roll-out to December 2013. It is now largely complete with 2.8 million smart meters installed. A number of small-scale rollouts are also occurring in the states of Western Australia and New South Wales.

A 2012 Global Smart Grid Federation report explains that smart meters have been a controversial political issue in Australia. The State of Victoria commenced a mandatory rollout of smart metering infrastructure and, with it, new time-of-use pricing. All costs associated with this deployment passed to consumers, including the cost of the smart meter itself. Against the backdrop of already increasing electricity prices, consumer reaction to the project was negative. There was a temporary moratorium on the rollout. New South Wales has also proceeded with a smart meter trial deployment.

A May 2015 report by Northeast Group LLC, "Oceania Smart Grid: Market Forecast (2015 – 2025)", notes that Oceania has one of the most developed power sectors in the world, with well performing utilities, unsubsidized electricity prices, and high rates of electricity consumption. Australia (and New Zealand) is well positioned to continue existing smart grid projects and develop new ones. The sector will be underpinned by the economy's high per-capita income and a number of incentives for clean technology. The state of Victoria (representing 25 percent of the national market) has nearly completed its AMI rollout. So far, regulations in other Australian states and at the national level have been more limited. But customers and utilities in Victoria are already seeing clear benefits from AMI deployments, which could encourage other states to

begin incentivizing deployments. The rest of Australia is expected to begin AMI deployments in the next one to three years, followed by further investment in distribution automation, home energy management, and other smart grid segments.

Smart Grid Australia (SGA) is a non-profit, nonpartisan organization dedicated to modernizing Australia's electrical system. It holds meetings, organizes committees, assists government initiatives, and issues communications to accelerate progress on smart grid development. According to the GSGF website, SGA has played a key role in providing information and assistance to the Government for smart grid initiatives.

A 2011 country overview study prepared for the U.S. Energy Information Administration (EIA) on Australia notes that drivers for the smart grid included: energy efficiency goals; renewable integration (especially solar); reliability concerns; financial incentives; government policies/mandates; environmental goals; and smart grid development status.

In 2008, with the assistance of SGA, the Government initiated the Smart Grid Smart City program as part of its National Energy Efficiency Initiative. The Government is developing a regulatory reform strategy to remove barriers and improve incentives to smart grid investments, including measures that address demand-side regulation and time-of-use tariffs. It is also engaged in a review process to determine which public initiatives are needed to prepare electricity networks for a higher number of electric vehicles. State governments have also become involved in smart grid activities. New South Wales is examining whether restructuring distribution networks can yield efficiencies, which would relieve price pressures. Queensland has also expressed an interest in smart grid, and is seeking advice from industry on smart grid initiatives. Smart grids are on the agenda of every Australian distribution business, and most are engaged in projects of varying scope and scale.

The Department of Resources, Energy and Tourism (DRET) committed approximately $100 million in its May 2009 budget to develop and test this commercial scale project to gather robust information about the costs and benefits of smart grids to inform future decisions by government, electricity providers, technology suppliers and consumers. The technology introduced through the program allowed residents to see real time analysis of electricity usage for their households and for individual appliances. EnergyAustralia led the demonstration project and will become the first utility to use long-term evolution (LTE) for its 4G communications network according to reports. Australia's SmartGrid, SmartCity project was the first to use a 4G LTE network in a smart grid application. Under the Smart Grid, Smart City initiative, the Government tested the business case for key smart grid applications and technologies, and gathered information to inform future smart grid investment by Australia's electricity leaders.

The Smart Grid Smart City project also tested demand side response solutions, as well as new supply technologies, in a production environment with actual customers. This demonstration project gathered information about the benefits and costs of different smart grid technologies. As

part of the trial, customers monitored energy use and calculated energy costs and greenhouse gas emissions. Customers received a household energy management system, giving wireless control of appliances. The project included smart sensors, new back-end IT systems, smart meters, and a communications network.

It brought together representatives from both the public and private sector active in power generation, transmission, distribution, information technology, retail and community groups, and advance discussion about the future of electricity infrastructure in Australia. Ausgrid tested various technologies throughout the Smart Grid, Smart City project. These trials were either part of the grid-side trials or the network customer trials. The Grid trials concluded on 30 September 2013. The final report was published in July 2014. (More information can be found at http://www.smartgridsmartcity.com.au/About-Smart-Grid-Smart-City/Resources-and-results.aspx). The report concluded that potential benefits require an integrated solution and that there are four key aspects to realising these benefits and improving consumer pricing outcomes:

- Technological development and deployment of enabling (smart grid) technologies;
- The introduction of cost reflective electricity pricing including dynamic tariffs;
- Consumer behaviour change with respect to electricity consumption (to better manage any future growth in peak demand); and
- Energy market reform4 (many aspects of which are already underway).

SGA finds that the Smart Grid Smart City trial has provided a rich source of information, which is available for study, but the key outcome is that the business case is proven. It notes that the key findings from the report are: the business case for market led rollout of Smart Grid Infrastructure is positive; deployment of the infrastructure and associated technologies need to be integrated for maximum benefit; efficient tariffs are essential to support the necessary technologies and to prevent inefficient investment; and smart meter technologies provide the catalyst for better tariffs, improved reliability and reduced prices. Australia's Smart Grid, Smart City demonstration is one of a few globally that was designed to show the benefits of smart grid technologies across the electricity network, and as such, Australia is a leader. SGA argues that Government and industry should now show leadership and push a national rollout.

EnergyAustralia's Smart Grid, Smart City project is the largest and most high profile project, but there are many others. Some have cut back because of this project, which was seen as essentially conducting a large-scale pilot on behalf of the whole industry. Nevertheless, other pilots have been completed, or are complete enough that lessons can be drawn.

In the Intelligent Network Communities project, the distributor Essential Energy is testing network fault detection, isolation and restoration, power quality monitoring, and distribution automation using a commercial distribution management system. Combined with load control, this substation monitoring and four quadrant interactive inverters for Volt/Var controls, this

makes it a complete smart grid project. Customers have been invited to participate in energy management trials. As part of the project, Essential Energy is also testing advanced metering infrastructure, certain customer products and education, distributed generation, and storage.

Like most economies developing smart grid infrastructure, Australia has no one agency overseeing smart grid development. The Australian Energy Market Commission (AEMC) serves as the regulator of the National Electricity Market (NEM). The Australian Energy Regulator (AER) and the Australian Energy Market Operator (AEMO) work in conjunction with AEMC to enforce rules and ensure the smooth operation of the electricity markets. Additionally, the AEMO is responsible for planning the transmission grid. The Department of Climate Change and Energy Efficiency (DCCEE) and the Department of Resources, Energy and Tourism (DRET) set climate change and energy policy nationally. These agencies work together to define policy framework and develop the smart grid.

Some additional projects identified by the EIA report include:

> 1) Solar Cities Program: Designed by DCCEE to test new sustainable models for electricity supply and use. These models combined solar power, smart metering, energy efficiency, and cost reflective pricing. The goals of the program included cuts in peak electricity demand, testing of sustainable energy options, the development of better information on environmental and economic costs and benefits of the various energy options, and the reduction of greenhouse gas emissions. The seven cities participating included Adelaide, Alice Springs, Blacktown, Central Victoria, Moreland, Perth, and Townsville.
>
> The Australian Government's Solar Cities program trials new sustainable models for electricity supply and use, and is being implemented in seven separate electricity grid-connected areas around Australia. The Department of Climate Change and Energy Efficiency administered it in partnership with local and state governments, industry, business and local communities. Each Solar City trialed a unique combination of energy options such as energy efficiency measures for homes and businesses, the use of solar technologies, cost reflective pricing trials and community education about better energy usage in an increasingly energy-reliant world.
>
> 2) EnergyAustralia PowerSmart Program: Time-of-use (TOU) pricing system for small and medium sized business customers that use less the 40 MWh of electricity per year. A large number of businesses have had smart meters installed, allowing them to take advantage of the program.
>
> 5) Advanced Electricity Storage Technologies Program: A Government initiative that has awarded $20.4 million through DRET that ran from 2004 to 2012. This program sought

to increase the use of variable renewable energy sources, such as wind and solar, by promoting the development and demonstration of efficient electricity storage technologies. Such technologies include batteries, electro-mechanical, chemical, and thermal storage technologies, in either on- or off-grid configurations. The program funded projects such as: a) Wizard Power: A solar energy storage project using technology based on ammonia dissociation and re-association into hydrogen and nitrogen; b) Lloyd Energy Systems: A solar thermal energy storage system demonstration involving concentrated solar energy and graphite blocks; c) ZBB Technologies: An integrated zinc-bromine flow battery project at CSIRO's National Solar Energy Centre in Newcastle; d) RedFlow Pty Ltd: A zinc bromine battery demonstration in grid and fringe-of-grid solar photovoltaic systems; and e) Smart Storage Pty Ltd: An UltraBattery system project located at the end of a rural grid attached to a wind turbine.

In addition, Australia in March 2011 launched one of the largest research efforts on green telecommunications in the world, the Centre for Energy-Efficient Telecommunications, a partnership with Alcatel-Lucent Bell Labs, the University of Melbourne, and the Victorian State Government. The Centre will take advantage of the University of Melbourne's research in telecommunications network infrastructure.

Also in 2011, the National Digital Economy Strategy set a goal to provide smart technology to a majority of Australian households, businesses, and organizations by 2020 to manage energy use better.

Other projects include (non-exhaustive):

1) ActewAGL: Has completed a HAN trial. Continuing with the implementation of a multi-utility smart metering pilot with gas, water and electricity.

2) Aurora Energy: A number of major pilots underway – connecting with the NBN.

Intending to use its own broadband connections if the NBN is not available.

3) Country Energy Pilots in Armidale, Bega and Port Macquarie, which include testing many elements of the Smart grid as well as customer HANs. Over 10,000 customers currently involved in two IN (Intelligent Network) communities.

4) ENERGEX: A number of customer trials, such as a "peak rate rewards trial" and "cool change" air conditioner management in various Brisbane suburbs as well as working with Ergon on a trial of 1600 In Home Displays (IHDs). ENERGEX also focuses upon energy conservation and demand management, use of the fiber network (UbiNet), and feeder of the future project with Ergon.

5) Ergon Energy: Extensive work in Townsville. Focusing on distribution automation, protection upgrades and smart meter trials. Also trials in Cairns and Toowoomba, and working on funding for a larger trial. Work on Magnetic Island and the Townsville suburbs of Rocky Springs and Riverway with Solar Cities and NBN. Extensive involvement with the Solar Cities program. Continuing with a Feeder of the Future project. Looking at ways to use Google PowerMeter to reduce the cost of implementation.

6) ETSA Utilities: Significant demand management trial in Adelaide, using network sensing to trigger an automated demand response. Also pilots with three EVs, HANs, and trialing alternative communications. Work with NBN integration in Adelaide, with ETSA doing some of the NBN installation.

7) Hydro Tasmania: Pilot project in the Bass Strait Islands with 2000 people. Includes solar PV feed-in, interval metering (AMI and field devices for provision of demand-side response and improved power system quality), load shedding. Focus on demand-side response, reduction of diesel fuels and increased renewables. IHD and HAN trials in 1600 homes in early 2011.

8) Integral Energy: Trials around fault detection, peak load reduction, smart meters, network losses. Trialing an energy efficiency portal for consumers to compare usage with neighbors. Conducting a major solar energy trial in the Sydney suburb of Blacktown, and various customer-pricing trials. Part of the Smart Cities trial with EnergyAustralia.

9) Jemena: Completed a ground-fault neutralizer pilot with United Energy Distribution. Further work with outage verification and restoration. Smart metering and HAN trials to develop power quality information, to be followed by work in information management. Trialling IEC 61850 substation automation project.

10) SP AusNet: Has been very involved with Victoria's smart meter rollout. Trials with WiMAX technology. Substantial feeder automation work in locating faults and isolating faults. Trials with plug-in hybrid electric vehicles (PHEVs). Trialling Broadband over Power Line (BPL).

11) Western Power: Pilots involving demand management and 10,000 smart meters, including the communications infrastructure. Looking at direct load control and PV saturation from previous air conditioning trials, and time of use tariffs, IHDs and HANs. Also completing a segmentation analysis. Supporting the Smart Cities trial with EnergyAustralia.

According to various reports, Australia is reasonably well advanced in smart grid development, and is looking at things more holistically than the United States and Europe. The United States is

concentrating more on smart metering and consumer interface functionality, while in Europe the focus is on how to integrate renewable energy sources, with load control and demand management an after-thought.

Articles from March 2015 further explain that the market for large-scale renewable energy projects may well be at a standstill in Australia, but at the community level, things are happening quickly. Dozens of projects emerged as state governments tap into local ideas, offering grants for innovative projects that allow solar and other renewables to be developed at a local level, for innovative financing packages, and even the development of localized smart grid. Numerous towns in Australia are now looking to make themselves either zero net carbon, zero net energy, or 100 percent renewables; or to create community owned electricity retailers that focus on renewables. New housing estates may not be connected to the grid at all because of the possibilities offered by battery storage and other enabling technologies. The scale and breadth of ideas is further underlined by the new series of community energy grants announced by the NSW Government. They include a 1MW solar project in Goulburn, which would be the biggest community-owned solar project in the whole economy, solar arrays that will bring solar to low income housing and rentals, and a plan to take a whole village off grid, and a renewable energy 'smart' grid that will allow an 'eco-village' to generate and swap electricity among the 120 or so housing lots. The community-owned smart grid idea has attracted Australian $70,000 from the NSW Government to help the Narara Eco Village on the central coast develop the plan.

According to some websites, significant progress has been made within the industry in relation to the deployment of smart technologies that, over time, will create a smart national grid. All the electricity companies are now involved in the implementation of smart grids – a process that will take a decade, or perhaps several decades, to complete. Overall, some Australian $200 billion will be invested in the national energy structure (not just smart grids). The results from projects such as Smart Grid, Smart City indicate that the results have greatly exceeded expectations. A holistic government policy is seen as the key to success.

The main players in the Australian market include: ActewAGL; AGL Energy; Aurora Energy; Ausgrid; CitiPower and Powercor; Endeavour Energy; Energex; Ergon – Nexium Telecommunications; Essential Energy; Horizon; Hydro Tasmania; IBM; Jemena; Network NSW; Powerlink; SA Power Networks; SP Ausnet; Telstra; Transgrid; United Energy; and Western Power.

6.1.3 Current Cybersecurity Nexus

The Australian Government has three key priorities for maintaining Australia's electronic security:

1. Reducing the e-security risk to Australian Government information and communications systems.
2. Reducing the e-security risk to Australia's national critical infrastructure.

3. Enhancing the protection of home users and small/medium enterprises from electronic attacks and fraud.[2]

Smart Grid Communications Protocol and Interoperability Standards

In the SGSC project, Ericsson and Ausgrid signed an agreement, which allowed Ausgrid to be the first utility to use Long Term Evolution (LTE) for its 4G communications network. A 4G machine-to-machine communications network using WiMAX and LTE standards rolled out in 2011 across approximately 150 sites in Sydney, the Central Coast, and Hunter Valley regions.[3] Australia may face competition from broadband-over-power line (BPL) networks, as the economy is planning a National Broadband Network with 90 percent of households having fiber optic cabling for broadband by 2019.[4]

The Australian Department of Resources, Energy and Tourism commissioned the company, Standards Australia, to develop a roadmap for smart grid standards in Australia, an effort ongoing in 2016. Many of the recommendations to date provided by Standards Australia vary significantly from international standards developed by EIC and NIST and are geared towards developing standards based on near-term market commercialization.

Defining critical infrastructure protection

Under the New America study, which delineates key terms related to existing cybersecurity and information security definitions, the following terms are cited for Australia:

Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would adversely impact on the social or economic well-being of the nation or affect Australia's ability to ensure national security.

Under the "Critical 5" document of March 2014, "Forging a Common Understanding for Critical Infrastructure", Annex A provides the definitions of Critical Infrastructure and Associated Sectors. Australia defines its critical infrastructure as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defense and ensure national security.

The definition acknowledges that some elements of critical infrastructure are not assets, but are in fact networks or supply chains. Australia has adopted a resilience-based approach to critical

[2] APEC Cyber Security Workshop
[3] DNV KEMA
[4] NRG Expert

infrastructure in order to enable it to adapt to change, reduce the economy's exposure to risk and learn lessons from past incidents. Australia notes that a key element of disaster resilience is enhancing "the capacity to withstand and recover from emergencies and disasters." Australia's resilience strategy encourages organizations to identify ways in which they can be flexible and adaptable in the face of unforeseen shocks. Australia's Critical Infrastructure Resilience Strategy states, "A resilience approach to managing risks to our critical infrastructure encourages organizations to develop a more organic capacity to deal with rapid on-set shock. This is in preference of the Australian Government to the more traditional approach to developing plans to deal with a finite set of scenarios, especially in the context of an increasingly complex environment."

Australian Critical Infrastructure includes:

1) Banking and Finance: Financial services
2) Health: Supply of blood and blood products/hospitals
3) Communications: Broadcast media; Postal services; Telecommunications networks
4) Transport: Aviation; Land based mass passenger transport (including bridges and tunnels); Land freight; Maritime: Shipping and ports
5) Energy: Electricity systems; Offshore oil and gas; Onshore oil and gas; Coal supply
6) Water Services: Water utilities
7) Food Chain: Food supply sector
8) Other critical sub-sectors: Labs holding high-risk biological agents; Chemical manufacturing industry; Defense industries; Emergency Service

The Australian Government issued the Critical Infrastructure Resilience Strategy in 2010. The aim of this strategy is the continued operation of critical infrastructure in the face of all hazards, as this critical infrastructure supports Australia's national defense and national security, and underpins its economic prosperity and social wellbeing. More resilient critical infrastructure will also help to achieve the continued provision of essential services to the community.

The strategy highlights that it is important to note that some elements of critical infrastructure are not assets, but are in fact networks or supply chains. For example, "bringing food from the paddock to the plate is dependent not only on particular key facilities, but also on a complex network of producers, processors, manufacturers, distributors and retailers and the infrastructure supporting them."

In the context of critical infrastructure, resilience is referred to as: i) coordinated planning across sectors and networks; ii) responsive, flexible and timely recovery measures; and iii) the development of an organizational culture that has the ability to provide a minimum level of service during interruptions, emergencies and disasters, and return to full operations quickly. In

this way, building capacity in organizations to be agile, adaptive and to improve by learning from experience is part of the concept of CIR.

To meet the national interest, the actual extent of the Australian Government's role or interest in a particular issue will often depend on the likelihood and consequence of the risk or the actual incident. Accordingly, the Australian Government is a key stakeholder in understanding the vulnerabilities and dependencies in and across critical infrastructure sectors, and the risk mitigations being applied. The Australian Government also facilitates national coordination where there are cross-jurisdictional issues, international treaty obligations, or where an incident would have national consequences or require a national response.

The initiatives under this strategy assist critical infrastructure organizations to better prevent, prepare, respond to and recover from an incident. However, this Strategy does not focus on the existing response arrangements that are in place in the Australian Government, the States and Territories, and critical infrastructure organizations.

The Attorney General's Department is the lead agency for critical infrastructure policy across the Australian Government. A range of agencies directly contribute to the Australian Government's CIR Strategy. To ensure the Australian Government's policy settings remain appropriate, the CIR Strategy underwent a comprehensive review in 2015, after five years of operation.

A range of Australian Government agencies significantly contribute to the implementation of the Australian Government's CIR Strategy. Recognizing that all Australian Government agencies have a role to play in ensuring the security and resilience of Australia's critical infrastructure, the following agencies, among others, have clear responsibility for the delivery of the Australian Government's CIR Strategy:

a) The Attorney-General's Department (AGD) provides essential support to the Government in the maintenance and improvement of Australia's system of law and justice and its national security and emergency management systems. Under the CIR Strategy, the AGD is responsible for:

- Provision of strategic leadership and coordination in the development of a consistent Australian Government approach to CIR;
- Development of policy and advice to Government on CIR;
- Management of the Trusted Information Sharing Network (TISN);
- Provision of secretariat support to the Banking and Finance and Water Services Sector Groups, and the Resilience Expert Advisory Group;

- Provision of support to the Business-Government Advisory Group on National Security (BGAG), the National Critical Infrastructure Resilience Committee (NCIRC) and the Critical Infrastructure Advisory Council (CIAC);

- Management of information-sharing mechanisms including the TISN websites, the TISN calendar and the TISN deeds and register; and

- Coordination of the critical infrastructure threat assessment briefing programs.

b) The Australian Security Intelligence Organization's (ASIO) responsibilities include identifying and investigating threats to security, wherever they arise, and providing advice to protect Australia, its people and its interests. As agreed by the National Counter-Terrorism Committee, ASIO's responsibilities in relation to the CIR Strategy include:

- The identification and prioritization of national critical infrastructure, including maintaining a database of national critical infrastructure;

- The preparation of vital and sectoral critical infrastructure threat assessments;

- The briefing of owners and operators on vital and sectoral critical infrastructure threat assessments; and

- Protective security risk reviews for specified critical infrastructure.

c) The Department of Broadband, Communications and the Digital Economy (DBCDE) is responsible for policy development, advice and program delivery across a range of activities including the National Broadband Network rollout, Australia's digital television switchover, initiatives that support development of the digital economy, telecommunications policy, media policy, cyber security and cyber safety, managing the radio frequency spectrum and postal policy. Under the CIR Strategy, its responsibilities include:

- The provision of portfolio specific policy advice on critical infrastructure related issues;

- The provision of secretariat support to the Communications Sector Group and the IT Security Expert Advisory Group; and

- Drafting risk context statements and contributing to briefings under the threat assessment briefing process.

d) The Department of Resources, Energy and Tourism (DRET) provides advice and policy support to the Australian Government regarding Australia's resources, energy

and tourism sectors. DRET develops and delivers policies to increase Australia's international competitiveness, consistent with the principles of environmental responsibility and sustainable development. DRET is responsible for developing and maintaining government policies and programs to ensure resilient and secure energy systems. Under the CIR Strategy, its responsibilities include:

- The provision of portfolio specific policy advice on critical infrastructure related issues;
- The provision of secretariat support to the Energy Sector Group; and
- Drafting risk context statements and contributing to briefings under the threat assessment briefing process.

6.1.4 Cybersecurity Challenges (Issues)

Two of the key cybersecurity challenges for Australia are:

- Geographic differences, legacy issues, regional needs, and consumer education.
- Encouraging domestic regulators to learn about relevant activities at the international level, as well as understand how these standards can be used to meet their goals.

Defining cybersecurity

The Australian Government's Cyber Security Strategy (2009) priority objectives are:

a) All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online;
b) Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers; and
c) The Australian Government ensures its information and communications technologies are secure and resilient.

To achieve these objectives, the Australian Government applies the following strategic priorities to its programs:

a) Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest;
b) Educate and empower all Australians with the information, confidence and practical tools to protect themselves online;
c) Partner with business to promote security and resilience in infrastructure, networks, and services;

d) Model best practice in the protection of government ICT systems, including the systems of those transacting with government online;
e) Promote a secure, resilient and trusted global electronic operating environment that supports Australia's national interests;
f) Maintain an effective legal framework and enforcement capabilities to target and prosecute cybercrime; and
g) Promote the development of a skilled cybersecurity workforce with access to research and development to develop innovative solutions.

According to the 2015 ITU country report, the Cybercrime Legislation Amendment Act 2012 is the primary cybercrime legislation. Legislation and regulation related to cybersecurity is: a) the National Plan to Combat Cybercrime; b) the Australian Communications and Media Authority (ACMA) enforces the Spam Act; c) Australian Cybercrime Online Reporting Network; and d) data breach notification. CERT Australia is the officially recognized national CERT. The Cyber Security Operations Centre (CSOC) is responsible for coordinating and assisting operational responses to cyber events of national importance across government and systems of national importance. CERT Australia is a member of APCERT and FIRST. It is on the steering committee of APCERT and actively shares threat information with other CERTs across the world. CERT Australia, an agency of the Attorney-General's Department, provides services to business and critical infrastructure operators. It is the single point of contact for cybersecurity issues affecting major Australian businesses and works closely with its government partners. CERT IT is active in several international CERT forums. Australia is home to six members of FIRST and has a proactive approach to the introduction and effective operation of CERTs according to ASPI. The ASD is responsible for producing ICT security policy and standards for the government and publishes these in the Australian Government Information Security Manual.

Australia recognizes the National Plan to Combat Cybercrime and the 2009 Cyber Security Strategy as its national strategy. The national governance roadmap for cybersecurity is elaborated in the National Security Information Environment Roadmap: 2020 Vision. Australia entered into the following international partnerships: i) Statement of Intent regarding Cooperation on Cybersecurity and Cyber Incident Response between the United States Department of Homeland Security (DHS) and the Attorney-General's Department of the Commonwealth of Australia; and ii) CERT Australia has direct working relationships and a range of bilateral and multilateral agreements with government and business computer emergency response teams around the world.

Through the Govdex and Govshare platforms, agencies are encouraged and supported to share knowledge, skills, and resources in the pursuit of more effective, efficient and innovative solutions. These are the nationally recognized platforms for sharing cybersecurity assets within the public sector. The Trusted Information Sharing Network (TISN) is the framework for sharing cybersecurity assets between the public and private sectors in Australia.

Under the New America compilation of terms and definitions, the following key terms related to existing cybersecurity and information security definitions are delineated for Australia:

a) Information and Communications Technologies: Australia's national security, economic prosperity and social wellbeing are critically dependent upon the availability, integrity and confidentiality of a range of information and communications technologies (ICT). This includes desktop computers, the internet, mobile communications devices and other computer systems and networks.

b) Cyber Security: Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means. (Australia, Cyber Security Strategy, 2009, p. 5)

c) Information Security: The objective of information security, as defined in the OECD Guidelines for the Security of Information Systems and used by Australia is "....the protection of the interests of those relying on information systems from harm resulting from the failure of availability, confidentiality, and integrity". (Australia, Submission to the United Nations General Assembly Resolution A/54/213, p. 2)

d) Cybercrime: The Australian Government defines cybercrime as those computer offences under the Commonwealth Criminal Code Act 1995 (Part 10.7) which involves the unauthorized access to, modification or impairment of electronic communications. (Australia, Cyber Security Strategy, 2009, p. 23)

According to the 2013 UNIDIR Cyber Index, the Department of the Prime Minister and Cabinet, which assumed the responsibility from the Attorney General's Office in December 2011, coordinate Australia's cybersecurity policy. Australia's Cyber Security Operations Centre was established in 2010. It is part of the Department of Defense under the Defense Signals Directorate. Its staff of 130 is comprised of specialists from the Signals Directorate, the Attorney General's Department, the Federal Police and the Australian Security Intelligence Organization. The mission of the center is to advise the government on how best to protect the economy from cyber threats by disseminating information and coordinating incident response operations. A national CERT established in 2010 complements it and serves as a single point of contact for cybersecurity-related information. The Australian Security Intelligence Organization established a cyber investigations unit in March 2011. It focuses on response and intelligence regarding "state-sponsored cyber-attack."

The ASPI report on cyber maturity in the Asia Pacific notes that while the fundamentals of Australia's cyber organization are strong, it lacks a whole-of-government policy perspective. There has been significant ambiguity surrounding the economy's cyber leadership since the abolition of the Deputy National Security Adviser / Cyber Policy Coordinator role by the government in 201 since the last Cybersecurity White Paper was released five years ago. There is

apparently a need for greater clarity on policy leadership.

At the international level, Australia is active in both bilateral and multilateral forums, actively pushing to improve the cyber maturity of other economies in the region. There is generally a strong public understanding of cyber issues and an adequate level of business–government interaction, which should improve with the opening of the Australian Cyber Security Centre in 2014. The Australian Defense Force (ADF) possesses strong cyber capabilities, but is lacking a policy position to guide its and the wider Defense Department's approach to cyber threats.

It has a very effective range of cyber-related legislation, in particular Division 477.1 of the Criminal Code Act. The government has also worked closely with industry to create and implement a voluntary code of conduct for ISPs (the iCode). The iCode provides a consistent approach for ISPs when addressing cybersecurity issues and covers 90 percent of the Australian home internet market. Australia has also acceded to the Council of Europe Convention on Cybercrime.

The Australian Federal Police has also established strong cybercrime policing relationships across the region, particularly with Indonesia and South Korea according to ASPI. The Department of Defense maintains sophisticated cybersecurity capabilities.

The Australian Signals Directorate (ASD) is responsible for the development of the nation's signals intelligence capability. ASD is the Commonwealth Information Security Authority and maintains the Information security manual for Australian Government agencies. It also runs the Cyber Security Operations Centre, which is responsible for defending against threats to Australian interests in cyberspace and coordinates operational responses to cyber events of 'national importance'. Defense maintains the Network Operations Centre to protect and manage the security of its own networks.

6.1.5 Future Cybersecurity Nexus

The Critical Infrastructure Resilience Strategy states it is vital that owners and operators of critical infrastructure, both the private sector and government organizations, are able to plan for, withstand and respond to a broad range of threats and hazards, including pandemics, negligence, accidents, criminal activity, cyber-attack, and natural disasters that have the potential to disrupt their operations. Further, a disruption to critical infrastructure in one sector could have severe cascading impacts on critical infrastructure in other sectors.

The critical infrastructure networks and systems are themselves growing in complexity, and are operating in an increasingly complex environment. In this environment, the owners and operators of critical infrastructure need to be able to respond and adapt to foreseeable and unforeseen or unexpected risks and be able to continue to support other businesses, governments and the community.

Among other strategic imperatives, the strategy identifies the implementation of the Australian Government's Cyber Security Strategy. This is to maintain a secure, resilient and trusted electronic operating environment, including for critical infrastructure owners and operators. Cybersecurity is one of Australia's top national security priorities. Australia's ICTs underpin every aspect of modern lives, including the operation of critical infrastructure. As a result, cybersecurity and the resilience of critical infrastructure are identified as inherently linked by this strategy. It explains that the global community continues to experience an increase in the scale, sophistication and successful perpetration of cybercrime. Given the reliance of critical infrastructure organizations on ICT and the increasingly hostile cyber environment, it is essential that the implementation of the Australian Government's Cyber Security Strategy be incorporated into the CIR Strategy.

The Government launched its inaugural Cyber Security Strategy, with the explicit aim of maintaining a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximizes the benefits of the digital economy. Integral to the Cyber Security Strategy are two mutually supporting organizations: CERT Australia and the Cyber Security Operations Centre (CSOC). CERT Australia is the Australian Government's primary mechanism for engagement with the private sector on cyber security issues.

According to this strategy document, CIR is an ongoing process and occasional review and fine-tuning of the activities under each strategic imperative will be required as the Strategy is implemented. Success is measured by:

a) Effective engagement between governments and industry, both within and outside the TISN, for the exchange of information and intelligence, and the development of solutions to relevant security issues, on a sectoral and cross-sectoral basis;
b) Sector Groups being well supported by government and responsive to changes in the environment, individually and collectively;
c) Businesses and governments collaborating to develop and promote best practice in CIR and resilience capabilities being integrated into everyday business activities;
d) The need for investment in resilient, robust infrastructure being considered in market regulation decisions;
e) Businesses and governments collaborating to identify key cross-sectoral dependencies and vulnerabilities with respect to both cyber and physical infrastructure;
f) Businesses and governments collaborating to progress national research and development in CIR;
g) A positive and robust relationship between the different levels of government on CIR, and a level of national consistency and coordination while also supporting the different approaches of governments CIR issues and implications for owners and operators of critical infrastructure being considered in Australian Government policy development processes;

h) Lessons from exercise activities and real life events being propagated to all Sector Groups to enhance organizations' understanding of resilience and improve planning arrangements;
i) Owners and operators being integrated into the implementation of the Cyber Security Strategy and having useful engagement with CERT Australia; and
j) Australian Government international engagement is coordinated with updates being provided to NCIRC as required.

In 2009, the Australian Government released the first National Energy Security Assessment (NESA), which assessed the challenges that could affect Australia's current and future energy security. Energy security was defined as the adequate, reliable and affordable provision of energy needed to support the functioning of the economy and social development: 'adequate' is the provision of enough energy to support economic and social activity; 'reliable' is the provision of energy with minimal supply disruptions; and 'affordable' is the provision of energy at a price that does not affect the competitiveness of the economy and encourages investment in the sector. Using the same definition of energy security, the second NESA in 2011 found that energy security does not depend on Australian energy independence, or the ability to be self-sufficient. Australia's overall energy security was expected to remain adequate and reliable; increasingly being shaped by both the level of new investment going forward and the price of energy, which are both materially influenced by global trends. Work has commenced on the third NESA, with release planned for late 2014.

In February 2015, at the Global Conference on Cyber Space (GCCS 2015), Foreign Minister Julie Bishop called an international agreement on international security 'premature,' offering instead a proposal for peacetime norms that would place critical infrastructure off limits for cyber-attacks, recognize the special status of CERTs, and boost cooperation to reduce cybercrime.

Australia is a Critical Five nation party to the March 2014 document "Critical Five: Forging a Common Understanding for Critical Infrastructure".

At regional level, Australia is a participant in the ASEAN Regional Forum (ARF). In March 2014, it co-chaired an ARF workshop with Malaysia on confidence building measures in cyberspace.

The ASPI report on cyber maturity for 2014 notes that Australia has been actively involved in regional and international multilateral forums on international cyber policy issues. It also notes that CNI protection efforts in Australia require invigoration by government and industry stakeholders. Australia chaired the most recent iteration of the UN Group of Governmental Experts (UN GGE), which produced a consensus report confirming the applicability of international law to cyberspace.

6.2 Brunei Darussalam

6.2.1 Economy Energy Resources

According to the APEC Energy Overview Study published in March 2014, oil and gas have dominated Brunei Darussalam's economy since their discovery in 1929. The oil and gas sector is the economy's main source of revenue and constitutes around 95 percent of Brunei Darussalam's export earnings and around 68 percent of its GDP. In 2011, natural gas represented about 77 percent of the total primary energy supply and oil 23 percent. The main export destinations for Brunei Darussalam's oil and condensate in 2011 were Korea, the ASEAN economies, Australia, India, China, New Zealand and Japan. In 2011, natural gas generated almost all of the electricity.

6.2.2 Current Cybersecurity Nexus

Defining critical infrastructure protection

Open source searches do not currently produce material related to the definitions of critical infrastructure protection or critical infrastructure in Brunei Darussalam.

Defining cybersecurity

Under the New America compilation of terms and definitions, the following key terms related to existing cybersecurity and information security definitions are delineated for Brunei Darussalam:

Brunei Darussalam's submission to the UN General Assembly Resolution A/62/98, 2008, mentions, "information technology, encompassing all developments in the field of information and telecommunications, has come to play a vital role in all sectors of society".

There are no citation of Brunei Darussalam using definitions outside the term "information technology". Amongst other terms, "cybersecurity", "cyber incident", and "critical infrastructure" are not cited or defined.

6.2.3 Cybersecurity Challenges (Issues)

This section identifies the current and planned cybersecurity-energy nexus in Brunei Darussalam.

The 2014 APEC Energy Overview Study explains that Brunei Darussalam is formulating an Energy White Paper with the aim of securing the future of its energy sector. Three strategic goals have been set to drive the energy sector forward and realize the National Vision. One of these three goals includes ensuring the safe, secure, reliable and efficient supply and use of energy. In addition, Vision Brunei 2035, states that the economy's major goals for the next three decades are economic diversification and strengthening of the oil and gas sector. However, it is not clear whether this will include cyber resilience.

The CERT of Brunei Darussalam, BruCERT, formed in 2004 with collaboration from the Ministry of Communication. In 2013, it had 44 employees. It coordinates with other national CERTs, businesses, government agencies and internet service providers. In 2011, Brunei Darussalam hosted the first Interactive Technical Workshop on cybersecurity incident response for the Organization of Islamic Cooperation CERT (OIC-CERT). To facilitate the sharing of cybersecurity information, Brunei Darussalam also has recognized partnerships with ITU, APCERT, ASEAN, and FIRST. BruCERT is a member of FIRST.

According to the UNIDIR Cyber Index of 2013, the Government focuses on employing cyber capabilities defensively, protecting internal systems, and promoting information technology development.

However, according to ITU's country profile for Brunei Darussalam, it does not yet have an official national (or sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards. Nevertheless, the E-Government National Centre (EGNC) is developing a Brunei Darussalam National Cyber Security Framework. Brunei Darussalam does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals. It does have a recognized national cybersecurity strategy through what the ITU factsheet describes as the "E-Government Strategic Plan 2009-2014". According to ITU's national profile, Brunei Darussalam has 30 public sector professionals certified under internationally recognized certification programs in cybersecurity.

The "E-Government Strategic Plan 2009-2014" encompasses strategies such as increasing human capacity in ICT, R&D in optimizing online services tailored specifically for the public and improving connectivity among ministries. It addresses the needs of the three main stakeholders, namely the citizen, industry and government. It is based on five key strategic priorities, which have been developed based on the progress made in the e-government initiative so far.

The first strategic priority focuses upon the development of capabilities and capacity. Civil servants will be trained with the relevant ICT skills to successfully implement e-government projects. Competency accreditation programmers will also be identified and implemented.

Strategic Priority Two (SP2) will focus upon enhancing e-governance through reviewing, revising and developing policies and guidelines to allow for the effective delivery of e-government projects. Under this strategic priority, the legal framework will be updated to suit the e-government initiative.

Security and Trust in "electronic government" will be the focus of SP3, as the necessary infrastructure will be put in place to make sure that electronic transactions and exchange of information is kept confidential and is conducted in a secure manner. ICT awareness programmers will be introduced to educate all parties of the "cyber risks" available and the

precautions that can be taken to minimize these threats.

Strategic Priority Four aims to integrate the ministries under a common network, where government agencies will be able to work together more effectively under the e-government initiative. ICT facilities and resources will also be standardized to ensure efficient and cost-effective use of these resources. These criteria fall under the ambition of the realization of a "one government" network.

Strategic Priority Five calls for a more convenient and efficient approach to online government services for the public. Where applicable, the public will have 24-hour access to these e-services. Educational seminars and forums will also be held to encourage the public to use these services as well as provide a platform for the Government to receive feedback on their effectiveness. The plan, completed in 2014, is being implemented.

Several cyber-related policy opportunities and challenges for further consideration:

Greater connectivity in the region could raise the probability of transnational crime and cross-border cyber-related incidents. With increasing access to high-speed networks, low-level cybercrime has already risen in the ASEAN region. In Asia, policy experts further suggest that the growth of cybercrime could increase instability. Misappropriation of responsibility could lead to misunderstandings and the possible escalation in tensions or conflict because the accurate identification of those responsible for a cyber incident is not always easy (especially since there is now a wide range of varying threats that may also come from different non-state actors).

Geopolitically, challenges might arise for Brunei Darussalam given its location on the northwest coast of the island of Borneo and its coastline along the South China Sea. Under its ASEAN chairmanship in 2014, Brunei Darussalam tabled the establishment of a direct communications link (hotline) across ASEAN members for maritime issues, which could possibly be expanded to include issues with underwater cables and the energy sector.

Given the high importance of the energy sector, particularly oil and gas, to the economy of Brunei Darussalam, Brunei Darussalam should very closely consider possible cyber threats to oil and gas suppliers as globally some major global oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. This could possibly cause damage but breaches may also cause high damage to corporate assets, public infrastructure and safety, or the wider economy through energy prices. Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain. Brunei Darussalam should closely monitor cyber issues relevant to the electric grid as well as the supply chain.

Regarding international efforts, at the regional level, since Brunei Darussalam is a member of ASEAN,

critical infrastructure protection will be essential. Brunei Darussalam is also a participant at the ASEAN Regional Forum (ARF).

6.2.4 Future Cybersecurity Nexus

There is insufficient data on this topic for Brunei Darussalam. This is a potential area of growth in future cybersecurity nexus.

6.2.5 Smart Grids

2014 reports say that investment in Southeast Asia will include smart metering and the modernization of electricity transmission and distribution networks with sensors, communications and software. By 2024, the largest markets will be Thailand, Indonesia, Malaysia, Singapore, the Philippines, and Viet Nam, according to a recent study by Northeast Group LLC.

Southeast Asian economies are just beginning on the path of modernizing their electric infrastructure. Electrification programs and growth in renewable resources will also drive investment. 2014 reports online also outline that some emerging economies, such as Thailand, Malaysia, Indonesia, and the Philippines, are making plans to deploy smart grid technology. While this region is currently behind other global regions in terms of smart meter deployments and regulatory frameworks, its smart grid market is growing. There are already smart grid pilot projects in several economies throughout the region. By 2022, Southeast Asian economies will likely have an electricity demand profile similar to Latin American economies where large-scale smart meter deployments already exist. The region's current electricity consumption rates are among the lowest in the world, while distribution loss rates are comparatively moderate, offering less short-term savings potential compared with other global regions. Additionally, regulatory frameworks remain largely undeveloped in the region. Even in the more advanced economies, deployments are still at the initial pilot level.

This Northeast Group study finds that Singapore is currently leading the region in development but later in the decade, the large markets of Thailand, Indonesia, Malaysia, Viet Nam, and the Philippines will account for significant smart grid investment. Several economies in the region have drafted smart grid roadmaps and pilot projects are widespread. Regulatory frameworks are still developing but momentum will grow over the next several years. Both utilities and vendors are already working together to ensure preparedness when regulations are finalized. Many vendors are active across the region (these include ABB, Alstom, Echelon (NES), EDMI (Osaki), Elster, Enverv, GE, Itron, Schneider, Secure, Siemens, Silver Spring Networks, ST Electronics, Trilliant and other global and local vendors).

According to the APEC Energy Overview Study of March 2014, the potential of non-conventional energy resources and power transmission interconnection for energy exchange or power transactions needs to be exploited fully to create the additional power generation capacity

required in Brunei Darussalam. The economy's venture into renewable energy, along with its work to upgrade and expand existing electricity-generating facilities, will contribute to its energy security. Brunei Darussalam is exploring smart-grids as a complement to the possible increase in renewable energy. As it does so, enhancing cybersecurity will be essential to any large smart grid deployment activity.

Its immediate plans for the improvement of energy efficiency and conservation include, amongst others, improving overall power sector efficiency through the implementation of energy saving technology such as utilizing combined-cycle gas turbines instead of open-cycle gas turbines, reducing partial load operation, installing smart meters and upgrading the transmission and distribution network.

The Institut Teknologi Brunei is undertaking research on smart grids as part of its ICT work. In addition, the Universiti Brunei Darussalam in its partnership with the IBM Centre on sustainability is researching smart grid as part of its work on consumer and grid friendly homes.

6.3 Canada

6.3.1 Economy Energy Resources

The 2014 APEC Energy Overview Study outlines that Canada has vast natural resources, including large reserves of fossil energy and a significant potential for non-fossil energy whose land area is the world's second largest after Russia. It is one of the world's top energy producers, drawing on its vast oil and gas reserves. The economy is well known for its rich supply of indigenous energy resources, with abundant reserves of oil, natural gas, coal and uranium in its western provinces, and large hydropower resources in its provinces of Quebec, British Columbia, Newfoundland, Ontario and Manitoba. It also holds significant offshore oil and gas reserves near Nova Scotia and Newfoundland. Accordingly, energy production is important to the Canadian economy. Canada is the world's third largest gas producer, sixth largest oil producer and fifth largest energy producer. Canada's domestic energy production in 2011 was made predominantly with fossil fuels - oil (43.41 percent), natural gas (32.30 percent) and coal (8.21 percent) accounted for the bulk of Canada's primary energy production, while the remainder was made up by hydropower (7.88 percent), other renewable sources (0.83 percent) and nuclear (1.98 percent).

6.3.2 Smart Grid Initiatives

Several provinces (Ontario, British Columbia, Alberta, and Quebec) have implemented smart meter rollouts. The Provinces of Ontario and Quebec conducted smart grid projects, and other provinces and utilities are undertaking grid modernization projects, which test and incorporate smart grid technologies. Numerous other federally funded, smart grid-related programs are underway or in the planning stages throughout Canada. A large number of programs and pilots fall under the Clean Energy Fund administered by Natural Resources Canada (NRCan).

In addition, SmartGrid Canada (SGC) engages stakeholders and academia from across multiple industries in an effort to build smart grid awareness, promote R&D of new and innovative energy technologies, and advocate for policies that support smart grid development. Canada established the public/private group, SGC, to promote smart grid developments. It consists of utilities, vendors, technology and service providers, academia and other industry associations.

SGC facilitates information exchange within the industry through the Canadian smart grid Repository. Developed in 2012, the public repository helps utilities deploy the most effective technologies and promote Canada's smart grid industry nationally and internationally. It organizes international missions to facilitate trade opportunities for Canadian smart grid organizations, partnering with the Government and other stakeholders. It is the only organization in Canada that has performed primary research at the national level into the consumer and their attitudes toward the smart grid, smart meter and the smart home.

The APEC Energy Overview Study notes that the structure of the Canadian electricity markets gives the provinces and territories jurisdiction over generation, transmission and distribution of electricity within their boundaries, including restructuring initiatives and electricity prices. The Federal Government is responsible for electricity exports, international and designated inter-provincial power lines, and nuclear safety, which is especially important since the economy-wide market is interconnected at many points with the United States to form a larger grid. In most provinces, the electricity industry is highly integrated with the bulk of generation, transmission and distribution services provided by one or two dominant utilities. While some of these utilities are privately owned, many are Crown corporations owned by the provincial governments and, although independent power producers also exist, they are rarely in direct competition with a Crown corporation. Exceptions include the provinces of Alberta, which has moved to full wholesale and retail competition, and Ontario, which has established a hybrid system with competitive and regulated elements.

In fact, the Canadian grid is part of a North American transmission system which is comprised of three major interconnected grids: (1) the Eastern Interconnect, which spans the entire eastern and central states, (2) the Western Interconnect, which spans the Pacific Rocky Mountains and southwestern states in the United States, and (3) the Electric Reliability Council of Texas interconnect which includes most of the U.S. State of Texas.

A 2012 GSGF report, in their collective ambition that Canada be a global energy leader, the federal, provincial and territorial governments agree on some basic principles: (a) energy supply diversification is important; (b) energy efficiency and conservation improvements are required for economic competitiveness and environmental responsibility, and (c) aging energy infrastructure is a challenge. They also agree that a key objective should be the accelerated development of clean energy technologies and a workforce skilled in those technologies. In relation to smart grid initiatives specifically, the Federal Government has cited energy capacity,

efficiency, reliability, and sustainability as drivers.

The following projects are illustrative of Canada's early adoption of smart grid technologies. The GSGF reports that Canada's smart grids are notable for both their scale and that they are either completed or near completion. The report highlighted that the Canadian experience provides a good benchmark from which other economies can learn, as it has already implemented smart meters and time-of use rates for millions of customers.

- Transmission dynamic line rating: Manitoba Hydro with supplier The Valley Group used static rating (232 A) for a transmission circuit that had intermittent loading constraints that caused them to curtail low cost hydro generation. They installed a Dynamic Line Rating (DLR) System to optimize transfer capability in 2002.

- The Province of Ontario adopted green energy as a key pillar of its economic growth strategy and has become a leader in renewable energy, smart meters, and smart grid adoption. The Government initiated the economy's first smart metering deployment, the Ontario Smart Metering Initiative, to install smart meters province-wide. Along with smart meters, it introduced mandatory time-of-use pricing. Ontario is the largest electricity market in the world with mandated time-of-use rates.

- Hydro Québec is voltage stability limited in the Montréal area, and this creates major constraints on power exchanges with the United States. As Hydro Québec was already equipped with a modern Wide-Area Monitoring System, its own fast and reliable communication network, it sought to establish a Wide-Area Control of voltage through the installation of interoperable multi-vendors relays, PMUs and IEDs. The Hydro-Québec Wide-Area Monitoring System is connected to the Energy Management System and preemptively advises system operators about geomagnetic storms. Playback of voltage stability cases, simulated using PSS/E and ASTRE, allows assessment of the performance of the overall telecommunication chain. The control signal timing and accuracy across the different boxes can be traced.

Smart grid developments have been underway at both the national and provincial levels for several years. According to a 2011 report prepared for the U.S. Energy Information Administration, much of the smart grid activity in Canada has taken place at the provincial level, with Ontario the primary leader in efforts to develop and deploy smart grid applications. Ontario enacted the Energy Conservation Responsibility Act in 2006, which mandated the installation of smart meters in all Ontario businesses and residences by 2010. By early 2010, with more than 3.4 million meters installed, the program was on track to have 350,000 customers using TOU metering by mid-2011. (By 2014, it had installed about 5 million meters.) The report noted that at that time these programs meant that Ontario had arguably one of the world's most advanced smart grids.

Government agencies and programs that play a role in the electricity network and smart grid activities in Canada include the National Energy Board (NEB), Natural Resources Canada (NRCan), the Natural Sciences and Engineering Research Council of Canada (NSERC), and the Clean Energy Fund. At the federal level, NRCan oversees the coordination of smart grid activities. In addition, CanmetENERGY, Canada's clean and renewable energy research center and an agency of NRCan, in collaboration with the Standards Council of Canada (SCC) and other partners, has established a national smart grid Technology and Standardization Task Force. The SCC is overseeing the standardization process while the Canadian Standards Association is actively developing standards for the smart grid.

Key Projects/Programs identified under the 2011 EIA study included:

- Ontario London Hydro Phase II project: Installation of 1.8 million meters. All utilities participating in the project were assigned specific weighting factors to their individual technical requirements, supplied meter population data, and provided utility-specific cost and productivity factors.
- In February 2011, the NSERC announced grants to support research projects. Two of the projects related to smart grid applications: a) University of Ottawa, Intelligent Vehicular Networks and Applications (DIVA); and b) British Columbia Institute of Technology, NSERC Smart Microgrid Network.
- Ontario, City of Windsor, Water Systems: In 2010, the City of Windsor announced that it would connect the city water and waste water systems to the Ontario smart grid as part of a pilot program to allow entities that operate large electric equipment with a consistent workload and some process flexibility or functional range to be tied into the smart grid.
- British Columbia Green Energy Plan: Focus - greater conservation, energy efficiency and clean energy. A major feature is to achieve the goal of electricity self-sufficiency by 2016, and an eventual surplus in years with normal water flows. Another goal is to enable the export of more electricity to neighboring jurisdictions, in either Canada or the western United States.
- Projects under the Clean Energy Fund: a) Electricity Storage Demonstration: Utility-scale storage demonstration using both new and re-purposed lithium ion automotive batteries; b) Wind and Storage Demonstration: Located in Cowessess First Nation, Saskatchewan; c) Energy Storage and Demand Response: To demonstrate the feasibility of energy storage as a mechanism for reducing electricity demand at near peak capacity substations; d) Interactive Smart Zone Demonstration: Hydro-Québec will deploy infrastructure for charging electric and hybrid rechargeable vehicles at its Institut de recherché in Boucherville, Québec; e) New Brunswick Power Corporation Electricity Load Control Demonstration: Focus on the integration between smart grid technologies, customer loads, and intermittent renewable energy sources in a region with potentially significant renewable electricity capacity; and f) Prince Edward Island, Wind Technology Research and Development Park: The Wind Energy Institute of Canada will develop a wind park.

The report notes the highly integrated nature of the electricity grids of the United States and Canada. Canadian companies have been working with U.S. companies for many years to collaborate on power issues. For example, the Canadian company Energent has been working with U.S. utilities to develop smart grid solutions since 2007. The company was developing an Energy Hub Management System (EHMS). There are at least 33 major transmission interconnections between Canada and the United States. Because of this integration, Canada and the United States formed the Electricity Grid Working Group focused on bilateral collaboration to facilitate the transition to a modernized electric grid as part of their Clean Energy Dialogue. The integrated nature of the electricity grid with the United States is also a main driver for Canada's participation in the international coordination of smart grid standards.

Smart meter deployments have made significant progress in Canada. A majority of meters in Ontario are now smart meters, and a majority of Ontario customers are being phased onto TOU pricing.

BC Hydro started installing smart meters for 1.8 million of its customers in British Columbia in 2012. According to the utility, the smart meter deployment will detect and reduce energy theft, which costs BC Hydro about $100 million each year. BC Hydro emphasizes on its webpage that its smart meters will protect customers' privacy and not impact their health.

Hydro-Québec is planning to install 3.8 million smart meters in Quebec by 2017. Its roll out would likely be the largest deployment of smart meters in Canada, and one of the largest in North America.

The SGC smart grid project repository of Smart Grid Canada, as at May 2015, listed the following projects:

1) Accuracy Analysis of Smart Meters; University of British Colombia; researching into how most of the electricity in commercial, industrial, and private residences are in use. Research on power delivery. Focus on efficient power delivery and smart grid usage.
2) Automated Switching, Burlington, Ontario; Burlington, Hydro; Automated switching in the core of the city.
3) Intelligent Microgrid; Vancouver, British Columbia; BCIT.
4) Advanced Metering; Regina, Saskatchewan; SaskPower; Full-scale installation of advanced meters.
5) Alternative Energy; Calgary, Albera; Enmax; Generating solar or wind power at home.
6) Electric Vehicles; Vancouver, British Columbia; BC Hydro; Electric vehicle infrastructure guidelines.
7) Net Metering; Vancouver, British Columbia; BC Hydro; Interconnecting small generating units.

8) Feed-in Tariff Program, Toronto, Ontario; Toronto Hydro; Guaranteed pricing structure for renewable electricity.
9) Peaksaver; Toronto, Ontario; Toronto, Hydro; Regulating appliances when the system is at peak demand.
10) Smart Experience; Toronto, Ontario; Toronto Hydro; Consumer electric vehicle pilot project.
11) Intelligent Algorithms; Toronto, Ontario; Ryerson; Intelligent algorithms for integrating wind power.
12) Grid Iq™; Markham, Ontario; GE; $40 million Grid IQ™ Innovation Centre.
13) GridSmartCity; Burlington, Ontario; Burlington Hydro.Integrated projects to demonstrate the full capabilities.
14) Smart Zone; Boucherville, Quebec; Hydro Quebec.
15) Energy Storage; Vancouver, British Columbia; Powertech Labs Inc.; Zinc bromine battery demonstrations.
16) Energy Storage; Toronto, Ontario; Electrovaya; Utility Scale Electricity Storage Demonstration
17) Energy Management; Vancouver, British Columbia; Pulse Energy.
18) Smart Zone; Toronto, Ontario; Hydro One; Advanced distribution system project.
19) Powershift Atlantic; Fredericton, New Brunswick; NB Power; Innovative wind power research.
20) Smart Meters; Calgary, Alberta; Fortis Alberta; Automated meter reading.
21) Distribution Automation; Edmonton, Alberta, EPCOR; Installation of Distribution Automation circuits.
22) Dynamic Line Rating; Winnipeg, Manitoba; Manitoba Hydro; Installation of Dynamic Line Rating system
23) Smart Meters; Saskatoon, Saskatchewan; Saskatoon Light & Power; Smart meter installation pilot.
24) Wimax; Toronto, Ontario; Powerstream; Wide area communications to monitor distributed generation.
25) Energy Storage; Golden, British Columbia; BC Hydro; Installation of two 1MW batteries.
26) Smart Meters; Toronto, Ontario; Province of Ontario.
27) Dms; Vancouver, British Columbia; BC Hydro; Telvent DMS and OASyS DNA SCADA System.
28) Smart Meters; Vancouver, British Columbia; BC Hydro; BC Hydro installing smart meters.
29) Conservation Rate; Vancouver, British Columbia; BC Hydro.

A smart micro-grid project was successfully demonstrated in Hartley Bay, British Columbia. The community was able to reduce its diesel fuel consumption through the implementation of

the *Pulse* energy management system and optimal control of the diesel power plant. The peak load was achieved using a range of smart devices including wireless thermostats, controls on hot water heaters and ventilation systems in commercial buildings.

CanmetENERGY collaborated with the Xeni Gwet'in First Nation in the design and demonstration of solar photovoltaic "mini-grid" systems in a remote community in British Columbia. This is an example of a rural electric cooperative independently managed by local residents. Due to the high cost of electricity from three diesel generators (3 X 90 kilowatt), the community installed smart pre-payment meters that would provide the 22 residential homeowners with information on their daily electricity use through a "pay-as-you-go" program.

The Canadian Electricity Association has also authored a number of smart grid publications to increase understanding of the issues and challenges.

Canada is a member of the GSGF and of ISGAN. In addition, in 2015, Canada, the United States and Mexico began seriously looking at issues related to integrating the North American grid, especially smart grid and interoperability to include more of Mexico.

6.2.3 Current Cybersecurity Nexus

The Standards Council of Canada defines cybersecurity requirements for a smart grid. However, the Standards Council of Canada does not specify a suite of cryptographic algorithms to meet the requirements, except to specify that Security Hash Algorithm (SHA) be used as the secure hash function. An open research problem is finding a set of cryptographic algorithms that provide the right combination of security and ease of implementation for the smart grid metering and control system.[5]

In 2012, the Standards Council of Canada and the Canadian Electricity Association agreed to co-chair Canada's Smart Grid Standards Advisory Committee (SGSAC). This advisory committee provides strategic advice, input, and guidance for the implementation of the Canadian Smart Grid Standards Roadmap. Also in 2012, Natural Resources Canada (NRCan), in cooperation with the Standards Council of Canada's Canadian National Committee to the International Electrotechnical Commission (CNC/IEC), created a task force to produce a smart grid standards road map. They made a number of recommendations in the areas of transmission and distribution, and smart metering infrastructure.

Defining critical infrastructure protection

Under the "Critical 5" document of March 2014, "Forging a Common Understanding for Critical Infrastructure", Annex A provides country definitions of Critical Infrastructure and Associated Sectors.

[5] http://timreview.ca/article/702

> "In Canada, critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of the government."

Canada's strategic vision is for the nation to build a safer, more secure and more resilient Canada through its critical infrastructure. In Canada, the Emergency Management Framework for Canada, which informs the National Strategy for Infrastructure, defines resilience as "the capacity of a system, community or society exposed to hazards to adapt to disturbances resulting from hazards by persevering, recuperating or changing to reach and maintain an acceptable level of functioning."

The National Strategy for Critical Infrastructure is based on the understanding that "enhancing the resiliency of critical infrastructure can be achieved through the appropriate combination of security measures to address intentional and accidental incidents, business continuity practices to deal with disruptions and ensure the continuation of essential services, and emergency management planning to ensure adequate response procedures are in place to deal with unforeseen disruptions and natural disasters."

In addition, the Emergency Management Framework for Canada highlights the importance of reducing risk through prevention, mitigation, preparedness, planning and response. Embedded in their disaster risk reduction concept is the need for resilience, which they define as "the capacity of a system, community or society exposed to hazards to adapt to disturbances resulting from hazards by preserving, recuperating or changing to reach and maintain an acceptable level of functioning."

Canadian Critical Infrastructure includes: Energy and Utilities; Information and Communication Technology; Finance; Manufacturing; Food Safety; Government; Transportation; Health; and Water.

Under the New America study which delineates key terms related to existing cybersecurity and information security definitions, the following citation for critical infrastructure is made:

> "Information infrastructure is a key component of Canada's critical infrastructure, which includes the following sectors: energy and utilities, communications and information technology, finance, health care, food, water, transportation, Government and manufacturing. The challenges of securing the information infrastructure are the same across all sectors, of which up to 90 percent is estimated to be owned and operated privately."

Defining cybersecurity

According to the 2015 ITU country report for Canada, legislation on cybercrime has been enacted through the Criminal Code (1985). Legislation and regulation related to cybersecurity occurs through the following instruments: Anti-Spam Act; Secure Electronic Signature Regulations; Electronic Commerce Protection Regulations; Personal Information Protection and Electronic Documents Act; and the Draft Bill C-12: An Act to Amend the Personal Information Protection and Electronic Documents Act. The Canadian Cyber Incident Response Centre (CCIRC) is the officially recognized CIRT. The Cyber Threat Evaluation Centre (CTEC) is also responsible for the detection, analysis, and assessment of cyber threat activity on nationally important networks. The Management of Information Technology Security (MITS) is the body responsible for operational security standards. The Government has a security policy that states the requirements for protecting information and directs the federal departments and agencies to which it applies to have an IT security strategy. The Operational Standard for the Security of Information Act is the nationally recognized instrument for cybersecurity standards.

Canada published it national strategy for cybersecurity, "Canada's Cyber Security Strategy For a Stronger and More Prosperous Canada", in 2010. The Action Plan 2010-2015 for Canada's Cyber Security Strategy is the national roadmap for the governance of cybersecurity. Going forward, to ensure continued progress, this Action Plan will be reviewed and updated periodically in collaboration with partners within and outside the Federal Government.

The UNIDIR Cyber Index 2013 further outlines that the 2010 cybersecurity strategy also addresses international engagement between the Department of National Defense and allied militaries on cyber defense best practices. The Canadian Armed Forces Information Management Group is responsible for the protection of the armed forces' computer and communications networks. Subsidiary organizations include the Canadian Forces Network Operation Centre as well as a center for electronic warfare and signals intelligence.

Under submissions to the UN General Assembly, Canada has relayed that information infrastructure is a key component of Canada's critical infrastructure, which includes the following sectors: energy and utilities, communications and information technology, finance, health care, food, water, transportation, Government and manufacturing. The challenges of securing the information infrastructure are the same across all sectors, of which up to 90 percent is estimated to be owned and operated privately. The Canadian Security Intelligence Service also lists information security threats as one of its five priority areas.

UNIDIR's cyber index report of 2013 further notes that the 2010 cybersecurity strategy has three pillars: securing government systems, collaborating to secure vital cyber systems outside the Federal Government to strengthen resiliency, including for critical infrastructure, and helping Canadians to be secure online. Public Safety Canada, the agency responsible for public safety and national security preparedness, oversees implementation of the strategy.

The National Cybersecurity Strategy outlines under Pillar 2 that Canada's economic prosperity and Canadians' security depend on the smooth functioning of systems outside the Government. In cooperation with provincial and territorial governments and the private sector, the Government supports initiatives and is taking steps to strengthen Canada's cyber resiliency, including that of its critical infrastructure sector.

The 2010 Action Plan for 2010-2015 shows that the Government continues to engage critical infrastructure sectors, for example finance, transportation, and energy, which are interconnected and spread out across Canada. To move forward with an integrated approach to engage this large stakeholder community, in 2010, Public Service Canada and provincial/territorial partners launched the National Strategy and Action Plan for Critical Infrastructure. Together with Canada Cyber Security Strategy, these documents set out the national game plan to ensure that Canada's critical infrastructure sectors can respond and recover swiftly from incidents and disruptions, including cyber incidents.

ITU's country report for Canada states that the following agencies are responsible for cybersecurity: Royal Canadian Mounted Police (RCMP); CCIRC; Office of the Privacy Commissioner of Canada (OPC); and Office of the Critical Infrastructure Protection and Emergency Preparedness (OCIPEP).

Public-private sector considerations relating to cybersecurity and the energy sector are extremely important given that relay that 90 percent of these sectors is estimated to be owned and operated privately.

ITU says that Canada has recognized various types of awareness programs on cybersecurity, for the general public as well as for public and private sector employees, through: CCIRC; OCIPEP; the Canadian Anti-Fraud Centre (CAFC); and Public Safety Canada's Industrial Control Systems (ICS). Canada officially recognizes the Canada-U.S. Action plan on cybersecurity under the Beyond Border Action Plan. Additionally, the CCIRC works closely with its international counterparts such as U.S.-CERT, GovCert UK, CERT Australia, and New Zealand CCIP to mitigate cyber threats and to share information on best practices for protecting critical infrastructure. The OCIPEP and Shared Services Canada (SSC) facilitate communication and networking amongst Canadian organizations and businesses, and serve as a framework for sharing cybersecurity assets within the public sector. In addition, regarding public-private sector collaborations, the SSC streamlines and consolidates information and communications technologies between various government departments. The CCIRC works closely with ISPs and security companies to identify threats and develop effective countermeasures in cybersecurity.

The 2010-2015 Action Plan notes that in 2011, the Government clarified the roles and mandates for the Communications Security Establishment Canada and the CCIRC, embedded at Public Safety Canada, to improve Canada's ability to identify, prevent, and mitigate cyber security incidents.

Pillar Three of the Action Plan outlines that the ongoing success of Canada's private sector relies in large measure on its ability to commercialize innovative research and intellectual property, business transactions, and financial data. Failing to secure this vital digital information, and the systems that hold it, inevitably leads to lost market share, fewer customers and corporate breakdown for the companies involved. On a national scale, the theft of trade secrets, intellectual property and confidential corporate information can result in lost jobs and diminished economic prosperity for Canada and Canadians. Many of the risks and impacts of cyber incidents are shared between governments and the private sector. It explains that Canada's public and private sectors share a long history of working together to achieve shared economic and national security objectives. However, it identifies that this cooperation needs to be further strengthened.

It notes that the disruption of critical infrastructure and cyber systems can have direct impacts on businesses and communities around the world. Incidents on interconnected cyber networks can have cascading effects across industrial sectors and national borders. At the same time, Canada needs to be active in international fora dealing with critical infrastructure protection and cyber security.

The 2010 national cybersecurity strategy specifically outlines that many of the risks and impacts of cyber attacks are shared between the Government and private sector. For example, untrustworthy technology is harmful to both government and industry. Identifying these risks must be done in partnership. Each partner must share accurate and timely cyber security information regarding existing and emerging threats, defensive techniques and other best practices. Strengthened public/private partnerships will be fostered through existing structures and organizations, such as critical infrastructure sector networks. Cross sector mechanisms will also be established, providing opportunities for governments and industry to collaborate on a broad range of critical infrastructure issues, including cyber security. Another key area for collaboration is the security of process control systems. These systems control everything from machines and factories to critical infrastructures. It notes that the security of these systems is critical to the safe delivery of the services and products upon which Canadians depend. Joint public/private sector initiatives are needed to identify and share best practices for addressing threats to these systems.

Canada is party to the March 2014 "Forging a Common Understanding for Critical Infrastructure" document that outlines a narrative representing the shared views of the Critical 5 members (Australia, Canada, New Zealand, the United Kingdom, and the United States) with the objective to provide a high-level overview of the meaning and importance of critical infrastructure.

Media reports in 2013 outlined concerns in Canada when alerts were issued by the U.S. Department of Homeland Security warning of attacks against U.S. and Canadian natural gas pipeline companies. These reports cited how Telvent Canada Ltd., a company that then helped to

"manage 60 percent of the oil and gas pipelines in the Western hemisphere", experienced a "cyber-attack" that compromised its security systems and internal firewall. The industry had been acknowledging potential problems at that point. Concerns were voiced over hacking groups attacking the Canadian energy industry hoping to disrupt operations, steal intellectual property, commit fraud or steal services. Initiatives that were established included the Canadian Association of Petroleum Producers, for instance, which set up a cyber-security working group where member companies that have robust security programs can share best practices and non-competitive intelligence with others.

The Telvent attack resulted in malicious software installed on company machines and in stolen project files. One of the stolen items helps energy firms mesh older IT assets with more advanced "smart grid" technologies, according to cyber security expert Brian Krebs.

6.2.4 Cybersecurity Challenges (Issues)

Canada should continue to monitor closely possible cyber threats to oil and gas suppliers, the supply chain, its electric grid, and pipelines particularly since many major oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. These could cause damage the companies' facilities and competitiveness. In addition, these breaches may also cause high damage to public infrastructure and safety, or the wider economy. Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain.

Given the economy's nuclear plants, it should continue to consider closely the nexus between cybersecurity and this sector. The IAEA, for instance, provides guidance for consideration by states, competent authorities, and operators. The aim is to prevent the theft of material or sabotage of plants and facilities.

At regional level, Canada is a participant at the ASEAN Regional Forum (ARF). It is also a member of the Organization of American States (OAS).

6.2.5 Future Cybersecurity Nexus

There is insufficient data on this topic for Canada. This is a potential area of future growth.

6.2.6 Smart Grids

Given the interest in the smart grid, enhancing cybersecurity is essential. It should be closely considered as part of a larger smart grid deployment strategy.

A 2011 report prepared for the U.S. Energy Information Administration, described smart grid drivers in Canada as including: increasing demand; energy efficiency goals; energy security

goals; geographic grid constraints; environmental goals; Canadian-U.S. cooperation/coordination; and energy theft reduction.

The GSGF 2012 report has already noted that popular reaction to some smart grid initiatives was mixed in Canada. Various groups had protested smart meter implementations based on privacy and health concerns. As a result, the Government of British Columbia and the utilities in the Province of Ontario then engaged provincial privacy commissioners to review the privacy impact of these meters. Canadian consumers benefit from some of the lowest electricity prices in the developed world, particularly in provinces where hydro-electricity is the primary source of electricity, and the introduction of some projects had coincided with increases in electricity prices. Therefore, electricity pricing and, by association, smart metering and green energy initiatives generally has become politicized.

The Ontario Information & Privacy Commissioner released a report called "Operationalizing Privacy by Design: The Ontario Smart Grid Case Study" in 2011 to consider these issues. The report outlines that with the evolution of the smart grid, Hydro One and local distribution companies are undertaking large and complex initiatives that will transform technologies, processes and organization. Because the smart grid will potentially encompass the entire utility infrastructure, it is critical to ensure that the proposed solution meets not only electricity infrastructure needs, but also customers' needs. The paper builds on the Information and Privacy Commissioner of Ontario's previous work with Hydro One in their joint publication Privacy by Design: Achieving the Gold Standard in Data Protection for the smart grid, which provides an overview of the smart grid in Ontario, the concept of personal information, defines a set of Best Practices for Smart Grid Privacy by Design, and provides two use case scenarios.

The 2011 paper follows on the earlier one by answering the question: How can Best Practices for Smart Grid Privacy by Design be "operationalized" into smart grid systems? The answer is to incorporate these best practices into each of the following areas: smart grid requirements, business process analysis, architectural decisions, and design considerations, at each step in the development. Such a process will result in the subsequent implementation of smart grid solutions that have privacy deeply embedded within them. Hydro One was at the time of the paper applying this methodology in a major advanced distribution solution project, beginning with a stage known as the "Living Lab" deployment. The Living Lab was used to confirm solution and process details in a defined subset of its service area in Southern Ontario. Hydro One shares in this paper how it and its vendor partners, IBM, General Electric ('GE') and Telvent USA Corporation ('Telvent'), were laying the privacy groundwork for Hydro One's smart grid solutions. With the guidance of the Information and Privacy Commissioner of Ontario, Canada, and the on-the-ground experience of Hydro One, IBM, GE and Telvent, this paper is described as the first of its kind to demonstrate how to incorporate Privacy by Design considerations in developing smart grid solutions. The intent is that this effort will minimize or eliminate any impact on energy consumer privacy for years to come. The paper aims to demonstrate that by

carefully understanding business requirements and processes, operationalizing Privacy by Design will lead to choices in architecture and design that will significantly reduce privacy risks, such as the unauthorized dissemination of personally identifiable information, thereby eliminating or diminishing potential impacts on privacy.

This paper, shared with utilities, vendors and service providers, provided an example of how they can utilize the Best Practices for Smart Grid Privacy by Design in the implementation of smart grid systems, product design, and energy information services and processes. The Commissioner advised policy-makers in the energy field to use this paper as an example of implementing privacy in a pragmatic way — meaning, in a manner where privacy does not lose out to other policy objectives such as energy conservation, but coexists equally with them in a positive-sum manner.

6.4 Chile

6.4.1 Economy Energy Resources

According to the APEC Energy Overview Study published in March 2014, Chile's diverse geography and abundant natural resources are favorable to renewable energy but very limited in fossil fuel resources,. This makes Chile a net energy importer with a high priority to maintain a steady energy supply. Nearly all of Chile's crude oil supply in 2012 came from imports. As for natural gas, Chile meets its demand by three-quarters of imports and the rest by domestic production in 2012. Chile's domestic coal production accounted for less than 6percent of the total supply in 2012. Most of the oil and gas sector has been liberalized and is privately owned. The National Oil Company (Empresa Nacional del Petróleo or ENAP) is also a major participant in oil production activities and controls refining.

6.4.2 Smart Grid Initiatives

The Chilean Government's energy strategy calls for the development of distributed generation, Advanced Metering Infrastructure (AMI), and smart grids. The Enel Group is already testing these technologies under real working conditions. In 2011, Chilectra, a part of the Enel Group, started the first smart metering project in Santiago, and had implemented 65,000 smart meters by 2014.[6]

According to the 2014 ENEL Foundation working paper, aside from a distributed generation law, and despite increasing interest, the interest in smart grids is very recent and there is no specific regulation in the field yet. In 2012, the Government mentioned an intention to explore the technical and economic feasibility of smart grids for the first time (National Energy Strategy 2012-2030).

[6] http://www.cepal.org/publicaciones/xml/1/47451/SmartGridsinLatinAmericaandtheCaribbean.pdf

A 2012 UN ECLAC & Cooperazione Italiano project document explains that in Chile private companies develop electric system activities (generation, transmission and distribution) entirely. The Government only exerts its competences on system regulation, control and planning of the investments in generation and transmission. There are four non-interconnected, territorially defined electric systems, namely: SING, SIC, Aysén and Magallanes.

Energy efficiency is at the core of the Chilean Government's energy strategy, as clearly stated in the document "Estrategia Nacional de Energía 2012-2030" published by the Ministerio de Energía. This document indicates the development of distributed generation, smart metering technologies (focusing on Net Metering) and smart grids as a target.

Energy distribution ranks lower in the policy agenda than energy supply and generation. In order to bring it to the fore, Chilectra and other players are introducing technologies and solutions from other parts of the world and championing the demonstration of smart grid solutions through the project Smartcity Santiago (SCS) for example. SCS is a smart grid/smart city pilot deployed by Chilectra – in close partnership with other similar Enel initiatives. Its core objectives are to explore and showcase new innovative energy solutions and business models, and to support further energy-related regulatory change in Chile. It brings together a number of smart technology solutions in Cuidad Empresarial, an advanced private business park. The implementation and testing phase in Cuidad Empresarial began in January 2013. The showroom/monitoring/control center was built between January and September 2013. Its vision does not include the development of new technological upgrades, applied research, products or solutions. The focus is entirely on showcasing and on the development of new business models. The utility signed an agreement, not with a local government, but with a privately owned business park. SCS has gathered a network of advocates and technology supporters. New incentives and regulations are required if the efforts of the pilot are to be scaled up in other parts of the city.

The challenges that might arise include: 1) Although first steps are being taken, new regulation and government involvement will become increasingly necessary to scale up and steer the process further. For example, the roll out of new smart meters may likely rely on new regulation or the remuneration of investments and on the meter ownership; 2) Since more than 70 percent of the meters in the area are property of the user, showcasing the advantages are likely to be a necessary yet insufficient driver for the transition. There is also a degree of public distrust and the benefits of smart city solutions will need to be explained. To a lesser extent, the same applies to investments in the grid automation, as the gains in operational cost (which are already low overall in Chile) are considered to be insufficient to compensate for the necessary roll out investment; 3) Since these are politically and socially sensitive issues that influence energy prices, communication across stakeholders, citizens and government levels is key; 4) Operational budgets are constrained; and 5) Since many of the deployed technologies are already in relatively

mature stages, SCS needs to remain open to new emerging solutions beyond the current technologies in order to avoid lock-in.

The Enel Group, leveraging on European experience, is already testing under real working conditions these technologies in Chile, in line with the national regulatory plan. Chilectra is supporting the project through a communication campaign aimed at raising customer awareness. To demonstrate the benefits of the new network technologies in an urban area, the Enel Group selected Santiago as a living lab for smart grids technologies. The project includes: Smart Metering; Remote Control and Automation of Medium Voltage network; technology solutions enabling active demand; efficient public lighting; installation of LED lighting; installation of Video Surveillance Cameras; installation of LED traffic lights (pedestrian countdown type); wireless communication (free Wi-Fi hot spots); ornamental landscaping lighting; cellular antennas for broadband signal transmission; Electric Vehicles; and a charging system for Santiago Inteligente; Electric Taxi and electric buses. Santiago is one of the first cities in Latin America supporting the diffusion of electric mobility.

The SOCOEPA project, described on the NRECA website, provides metering, demand, power factor and power quality information for up to 1,100 SOCOEPA consumers. Project funds allowed installation of 590 single-phase smart meters for residential consumers and 50 three-phase smart meters for commercial consumers. Most of the residential meters are located in remote areas of the SOCOEPA distribution system. According to the website, the AMI system has been performing very well, communicating with a high percentage of the meters.

The 2014 bilateral U.S.-Chile agreement includes promotion of energy efficiency in industry, transportation, public buildings and the private sector, and a pledge to work together on an energy efficiency law in Chile. Chile's energy ministry also submitted seven regulatory changes to the local comptroller's office with the goal of fulfilling commitments made in the 2014-18 energy agenda. The proposed changes would modify rules for auctions and net-metering.

According to Kamstrup in 2012, with the deployment of an advanced smart metering system, the leading energy provider in Chile, the CGE Group, is well prepared for the full smart grid-rollout with a high performing smart metering system being the most important building block in the future smart grid.

Other articles outline that the MoE awarded ECLAREON to develop the study “Smart grids: opportunities for development and implementation strategy in Chile” in order to identify development opportunities and establish a strategy for smart grid implementation. ECLAREON is an international business-consulting firm specializing in renewables that is leading the consortium for the project implementation. This report assesses international success stories in the development of smart grids to understand how these technologies are implemented in other economies. The study includes long-term national strategies such as that of South Korea and projects focused on a specific segment of the grid,

such as that in Houston, which aims to improve the distribution network reliability. The results show that the strategy should be based on long-term specific objectives, as positive returns in short periods of analysis are hard to achieve. In many cases, the development of these technologies not only requires stability over time but also public incentives since social benefits may represent a significant portion of the total benefits. The study concluded that the most valued technologies for implementation in the economy include smart metering, local generation and storage, micro-grids, automation and sensors as well as asset management tools. The scope of distributed generation and industrial level applications offer the greatest potential benefit for the use of this system in Chile. From a regulatory perspective, the Chilean electricity market would require significant reforms to apply fully all the features and services that an intelligent network can provide.

6.4.3 Current Cybersecurity Nexus

Open source searches do not currently produce a list of material related to the definitions of critical infrastructure protection or critical infrastructure in Chile.

Defining cybersecurity

A 2015 report by Trend Micro and the Organization of American States (OAS) on Cybersecurity and Critical Infrastructure in the Americas cites Chile as doing a very interesting work in cybersecurity. Chile is a Member State of the OAS. Organizations like the Union of South American Nations (UNASUR) and Member States have included cybersecurity and cyber defense in their agenda. They have also organized military conferences in different cities, and analyzed alliances and cooperation initiatives. The report highlights, however, that data from Chile, among other economies in the region, reveals that most vulnerabilities are related to the wrong system configurations, followed by outdated versions and higher risk application problems. In Chile, a single victim suffered as much as 35 DDoS attacks in a month in 2014.

According to the 2015 ITU country report, Chile enacted specific legislation and regulations related to cybersecurity through the following instruments: Law on Personal Data Protection; and the Law on Electronic Documents and Digital Signature. Chile has a national CIRT, CLCERT. CLCERT-CL has existed and functioned within the Government but it is not a formal institutional entity so much as an operational capacity and structure maintained by the Ministry of the Interior and Public Safety. Chile has officially approved the Supreme Decree No. 1299, Program for the Improvement of Information Security Systems Management as the national framework for implementing internationally recognized cybersecurity standards. There is no information on any framework for certification and accreditation of national agencies and public sector professionals. While there is no official national cybersecurity strategy or policy document, Chilean authorities worked for several years to develop a strong national capacity for

cyber incident response and management. Emphasis is on developing standardized procedures and best practices for incident management and cybersecurity more broadly.

According to the OAS/Symantec 2014 report, Chile's approach has been somewhat unique, in that rather than focusing on the creation of a single national CSIRT or similar body, emphasis has been placed on developing standardized procedures and best practices for incident management and cybersecurity more broadly. These are outlined in Supreme Decree No. 1299, Program for the Improvement Information Security Systems Management.

There is no national or sector-specific governance roadmap for cybersecurity. The Ministry of the Interior and Public Safety, Cyber Crime Investigation Unit (BRICIB), the General Secretariat of the Presidency and the Sub-Secretariat of Telecommunications all play key roles in cybersecurity. There is no national benchmarking and referential to measure cybersecurity development in Chile.

Regular risk assessments and trainings for staff are carried out to help in the application of R&D programs/projects for cybersecurity standards, best practices and guidelines in the public sector. Personnel from CLCERT-CL receive technical training in aspects of cyber investigations and incident management from experts in the field. The University of Chile and other academic institutions offer cybersecurity and cybercrime-related Bachelors and Masters Degrees. To raise awareness and promote a culture of cybersecurity, the Ministry of Education has developed and is implementing, in partnership with several private sector entities, a long-term campaign called Internet Segura. Internet safety is taught in schools as part of the ethics competencies contained in the technology curriculum.

The ITU factsheet further outlines that the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity in Chile is not known. To facilitate sharing of cybersecurity assets across borders, CLCERT-CL has actively collaborated with other national CSIRTs around the region in responding to incidents. Chile does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector. CLCERT-CL provides cybersecurity-related support to the State Connectivity Network and other entities of the central government, and promotes national and international cooperation, awareness raising, and the strengthening of national laws and policies. To facilitate participation in regional and international cybersecurity platforms and forums, CLCERT is a member of FIRST. It has also participated in initiatives to train personnel in other OAS Member States. Private companies are able and encouraged by the Government to provide incident management-related services, both to other private enterprises as well as public institutions in Chile.

According to the 2014 OAS/Symantec report, several agencies within the Government share responsibilities related to promoting cybersecurity and combating cybercrime. On the cybersecurity front, the Ministry of the Interior and Public Safety, the General Secretariat of the

Presidency, and the Sub-secretariat of Telecommunications all play key roles. For cybercrime-related matters the Carabineros, or national police, is the designated lead, through its Investigative Department for Criminal Organizations (OS9). Within the operational structure of OS9 is the High Complexity Section, which serves as the lead for investigations involving ICTs or the collection and analysis of digital evidence. The Department of Criminology of the Carabineros (LABOCAR) also maintains a computer laboratory dedicated to performing analysis of computers and devices seized during investigations of threats, grooming, phishing, and other illicit activities.

Personnel from OS9, LABOCAR and CSIRT-CL receive technical training in aspects of cyber investigations and incident management from experts in the field. Additional training often takes the form of instruction provided by the suppliers of a particular hardware or software being utilized, to ensure the proper use of the device or program. Where there is a need for more specific expertise, experts are hired on a contract basis.

To promote systems resiliency and data integrity within their own institution, the Carabineros employ both disaster recovery plans and disaster recovery software, thus ensuring that operations can resume quickly in the event of a man-made or natural disaster. The systems administrators and security managers regularly review the processes, policies and procedures related to recovery and IT infrastructure continuity. Security policies and procedures exist to ensure that users within the institution contribute to secure information systems management. Regular risk assessments and trainings for staff are carried out.

Authorities reported that they do not have sufficient information to provide a quantitative assessment of any increase or decrease in cyber incidents or cybercrimes in 2013. However, they did report that based on available data, the most common types of incidents alerted to national authorities in 2013 involved phishing, malware, and the hacking of government websites by hacktivists, the latter reportedly having increased 30 fold in 2013. Of these, however, phishing reportedly accounts for the highest percentage of cyber-related cases in the economy. Other frequently reported incidents involved grooming and threats against persons. Authorities reported that there is no available record of the exact number of opened cybercrime cases in 2013 or the number of persons convicted of such crimes. They did highlight several significant cases in 2013. In one case, Operation Minerva, persons affiliated with a hacktivist movement developed malware they deployed through phishing in a successful effort to infect the computers of numerous government officials and gain unauthorized access to information. In a separate incident, a senior government official with security-related responsibilities received death threats made through Twitter.

6.4.4 Cybersecurity Challenges (Issues)

According to the Trend Micro/OAS 2015 report on Cybersecurity and Critical Infrastructure in the Americas, beyond the work done by each economy or by the organizations, there is no

official information about security incidents in industrial systems or critical infrastructures in the region.

Another 2013 Trend Micro/OAS report on cybersecurity trends and government responses in Latin America outlines that incident response only represents one area of cybersecurity in which Latin American and Caribbean states have made significant progress. Many are beginning to draft national cybersecurity policies and strategies. With the support of the OAS, Colombia became the first Latin American economy to adopt a comprehensive national cybersecurity and cyber-defense strategy. Others including Chile, Peru, and Mexico are endeavoring to do the same. Recent acknowledgment of vulnerabilities in critical infrastructures has spurred initiatives seeking to strengthen ICS security.

There is however a lack of defined and harmonized terminology. This TrendMicro/OAS report highlights that the term "cyber incident" was not uniformly understood or applied across the region. Some interpret a cyber incident as any report or complaint sent to a national response team, while others are more exacting in their classification. According to this report, collecting data to enable a truly comprehensive and detailed picture of the extent of all such incidents and activities in the Americas and the Caribbean, or anywhere else, is not possible at this point.

Hacktivism or politically motivated hacking received widespread media attention in 2012 and information from OAS members suggests that this form of cyber incident is indeed on the rise in the region. Law enforcement in at least one country found spyware on their servers. Numerous states provided information suggesting that traditional organized crime syndicates have increasingly turned to the internet to extort and launder funds—very much in keeping with observed global trends.

Both OAS and Trend Micro data also indicated a rise in the number of attacks against critical infrastructure. A publicly operated national energy utility in one economy experienced a spate of cyber attacks, although the national CSIRT was able to minimize damage caused by the breaches. While attacks involving critical infrastructures have not yet caused catastrophic losses or physical damage in the Americas and the Caribbean, they do highlight the need for vigilance and improved resilience.

One of the main impediments to curbing illicit cyber activity in 2012 was the lack of adequate legislation, robust cybersecurity policies and personnel. In surveys submitted to the OAS, countries consistently discussed a need for highly skilled professionals who can secure networks, diagnose intrusions, and effectively manage cyber incidents as they unfold. This problem is manifested in the region by low enrollment in technical-degree programs. Given the time it takes to acquire cybersecurity skills and expertise, this low enrollment may have a noticeable impact in the coming years.

ITU outlines that while there is no official national cybersecurity strategy or policy document, Chilean authorities have been working for several years to develop a strong national capacity for cyber incident response and management. Emphasis is on developing standardized procedures and best practices for incident management and cybersecurity more broadly.

The 2014 OAS/Symantec report outlines that no law in Chile requires that private enterprises share incident-related information with national authorities, unless that information is sought as part of an official criminal investigation. However, national authorities actively seek to develop and maintain channels with key private sector entities whose cooperation is essential for effective investigation or incident management.

The OAS/Symantec report further outlines that Chilean authorities cited two principal impediments to efforts to enhance cybersecurity and combat cybercrime. The first is the need to raise awareness among senior decision-makers as to the urgency of both cyber threats and the steps that must be taken to address them. The second is the lack of recognition about the extent of the costs of cybercrime and cyber vulnerabilities, for the public as well as private sector, and the importance of developing a strategic and integrated approach, which outlines the roles and responsibilities of all stakeholders.

Cyber-related policy opportunities and challenges for further consideration

According to some reports in 2013, there has been a lack of attention to the protection of critical infrastructures such as gas pipelines in Latin America. Domestic unrest, labor activism and the remote terrains through which most high-pressure pipelines traverse also add to the risk. In addition, the Chile in particular suffers from frequent earthquakes.

Recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain. Chile should therefore closely monitor cyber issues relevant to oil and gas security as well as the supply chain given its dependence on imports and a stable supply.

The electricity market is wholly served by private companies and most of the oil and gas sector is privately owned (although the National Oil Company (Empresa Nacional del Petróleo or ENAP) is also a major participant in oil production activities and controls its refining in the economy). In addition, private companies are able and encouraged by the Government to provide incident management-related services, both to other private enterprises as well as public institutions in Chile. It is therefore important that specific public-private sector considerations linked to cybersecurity and the energy sector be further examined.

In assessing the potential advantages and risks associated with the use of nuclear energy for power generation in Chile, it should also ensure that extensive computer security/cybersecurity measures are in place. The IAEA (as well as several nation states) provides guidance for

consideration by states, competent authorities, and operators prevent the theft of material or sabotage of plants and facilities.

Regarding multilateral efforts, at the regional level, Chile is a Member of the Organization of American States (OAS).

6.4.5 Future Cybersecurity Nexus

There is insufficient data on this topic for Chile. This is a potential area of future growth.

6.4.6 Smart Grids

Given the development of smart city pilots and interest in the smart grid, enhancing cybersecurity is also essential and should considered as part of a larger smart grid deployment strategy.

6.5 People's Republic of China

6.5.1 Economy Energy Sectors

The 2014 APEC Energy Overview Study provides an extensive outline of the energy sector in China. Due to its large population and booming economy, China plays an increasingly important role in the world's energy markets. Some statistics have reported that China was the world's largest energy consumer in 2012 and accounted for 21.9 percent of global primary energy consumption in 2012. However, its per capita primary energy supply is far lower than that of many developed economies and below the world's average.

6.5.2 Smart Grid Initiatives

Currently, China is leading the world in grid investment. The Chinese Government has developed a large, long-term stimulus plan to invest in water systems, rural infrastructure and power grids, including a substantial investment in smart grids. Smart grids are a way to reduce energy consumption, increase the efficiency of the electricity network, and manage electricity generation from renewable technologies. China's State Grid Corporation of China (SGCC) outlined plans in 2010 for a pilot smart grid program that maps out deployment to 2030. Smart grid investments will reach at least USD 96 billion by 2020. The theme of SGCC's smart grid effort is called Strong and Smart Grid and has five focus areas: Strong and Reliable, Clean and Environmental Friendly, Friendly and Interactive, Open and Transparent, and Economical and Efficient.

The Demand Response System Pilot was China‘s first smart grid pilot project and feasibility study to monitor and manage electricity use in commercial buildings. The project focuses on Demand Side Management (DSM) and utilized state-of-the-art smart grid technology, including automated demand response, advanced energy management, and sub-metering. The project is

part of an agreement between the U.S. Trade and Development Agency (USTDA) and the State Grid Electric Power Research Institute (SGEPRI). Honeywell implemented the project.

The APEC overview study explains that in 2011, the National People's Congress approved the Twelfth Five-Year Plan for National Economic and Social Development (the Twelfth Five-Year Plan), which clarifies the national strategic intent, the Government's focus and the people's common program of action during the five year period starting from 2011. The plan emphasized that China will continue to give priority to thrift, rely on domestic resources, encourage diverse patterns of development, protect the environment, increase international cooperation for mutual benefit, adjust and optimize the energy structure, and construct a modern energy industry with the merits of safety, stability, economy, and cleanliness. Some targets related to energy are also published in the plan, including increasing the proportion of non-fossil fuel usage in total primary energy consumption, reducing the energy consumption per unit of GDP and carbon dioxide emissions.

IEEE Spectrum reports from February 2014 state that China has become the new leader in smart grid spending. China spent USD 4.3 billion on smart grid investments in 2013 as the U.S. market contracted 33 percent to USD 3.6 billion. China is installing more than 60 million smart meters, which makes up the bulk of its spending. Advanced metering infrastructure, often referred to as smart meters, are still driving investment in next-generation grid technologies, but other categories of spending will dominate in the future according to this report.

In 2013, reports online also noted that China was in the midst of a wholesale rebuilding of its power grid, which will make it the biggest smart grid market in the world. Over the course of 2012 and 2013, China updated parts of its future national energy and smart grid plans, as contained with its twelfth Five-Year Plan. Those included carbon emissions reduction, renewable energy growth, and a whole host of projects that fall under China's Strong and Smart Grid initiative. On the "strong" side, SGCC planned to invest $269 billion in transmission lines through 2015 to for wind and solar power to be brought to the west of the economy. On the "smart" side of the grid, SGCC, Southern Grid and other utilities are working with a multitude of domestic and international partners, with on-the-ground distribution automation, smart meter, plug-in vehicle and smart city "pilot projects" that can stretch into the millions of customers per project.

It explains that in China, the landscape is simpler than in some other economies. The State Grid Corporation of China (SGCC) controls most of the electrical grid, so when it decides to move forward with metering it can do so more quickly than in a fragmented, deregulated market. Asian and European markets will drive growth through 2020 according to these reports while in North America the focus will continue to shift from hardware to software as utilities seek to squeeze additional value out of the vast amounts of grid data now available.

Online reports in 2012 further note that as the economy's principal utility, SGCC is dedicated to developing a smart grid to promote clean energy, elevate energy efficiency, tackle climate change and reduce emissions. SGCC's Strong and Smart Grid project, putting major efforts into grid planning, testing and research systems, demonstration projects, international cooperation and standardization. Considering local conditions, SGCC proposed to develop the Strong and Smart Grid based on an ultra-high-voltage (UHV) grid backbone and coordinated development of subordinate grids at all levels. These subordinate grids would be IT-based, automated and interactive. Realizing the importance of top-level architecture design in building the smart grid, SGCC launched a planning process, compiling and drafting standards at the outset. The strategic targets can be summed up as "one goal, two main lines, three stages, four systems, five characteristics and six sectors".

Thus, the goal of building a strong and smart grid features two parallel efforts: technology (to incorporate information into the grid to make it automatic and interactive), and management (integrated operation, consolidated development, standardized construction and streamlined control). As for the three stages, the program's pilot study phase was executed in 2009-2010, construction of key elements took place in 2010-2015 and enhancements are planned for 2016-2020. The four systems refer to the strong and smart grid's foundation, technical support, applications and standards. Its five characteristics are to be strong and reliable, cost-efficient, clean and environmentally-friendly, open and transparent, and user-friendly and interactive. The six sectors it embraces are generation, transmission, energy conversion, distribution, supply and dispatch. SGCC has developed a "Smart Grid Technical Standards System" as the roadmap for smart grid standardization, which covers 8 domains, 26 technical areas and 92 standards series. SGCC will revise the framework on a rolling basis and incorporate suitable advances that have been achieved internationally.

As of June 2012, SGCC finished the first phase of the National Wind and Solar Power Generation/Energy Storage/Transmission Demonstration Project, including 100 MW of wind power, 40 MW of solar power and 14 MW of energy storage; and put in place 65 newly built and refurbished smart substations (increasing capacity from 10(66) KV to 750 KV). It carried out distribution automation pilots in 23 urban centers, deployed energy consumption information collection systems in 25 provinces, and built 243 charging stations.

In 2011, SGCC and IEEE jointly hosted the Smart Grid World Forum in Beijing. In addition, SGCC plays an active role in standardization activities of IEC and other international standard organizations. It serves as the Secretariat of IEC PC 118 Smart Grid User Interface.

An SAIC report prepared for the U.S. DOE's Energy Information Administration in 2011 provided an overview of China and the smart grid. It notes that smart grid drivers include increasing demand, energy efficiency goals, renewable integration, geographic grid constraints, economic competitiveness, and financial incentives.

It describes the development of the smart grid as follows: In 2010, Chinese Premier Wen Jiabao announced that construction of a smart grid was a national priority, with completion planned for 2020. Subsequently, SGCC announced that construction would begin on major nationwide grid upgrades in 2011. Cost of the projects is estimated to be $100 billion through 2020. Because of increased spending, China surpassed the United States in 2010 in total smart grid expenditures, and is anticipated to spend more than any other economy on smart grid developments for several years at least. As China establishes standards, seeks equipment, and develops its own technologies, it will play a central role in setting the tone of smart grid development worldwide, through the sheer size of its smart grid activities according to this report.

It notes that despite China's centralized structure, a number of government agencies share responsibilities for smart grid development. The State Electricity Regulatory Commission (SERC) oversees regulatory policies and rate structures. The National Development and Reform Commission (NDRC), is the central planning authority for all significant national initiatives n. The National Energy Administration has responsibility for administering energy related programs.

China's Energy Conditions and Policies, announced in 2007, established energy policies and targets to be achieved in the 11th Five Year Plan and beyond, as well as a number of measures and targets focused on smart grid measures to achieve policy goals. In addition, like many other economies, China created a hybrid governmental/industrial organization, the China Electricity Council (CEC) to promote R&D of smart grid applications. Operating under the CEC, the SGCC, which controls the T&D network, coordinates and guides smart grid developments in China. The energy policies established in 2007 underlie China's plans for moving forward on smart grid in seven key areas: rationalization of power grids; strengthening of regional power grids and power T&D networks; development of an emergency response system for power safety and reliability; strengthening of demand-side management (DSM); control of power use to conserve energy and increase energy utilization efficiency; strengthening of the Renewable Energy Law and policies for renewable energy electricity; and renovation of the rural energy grid.

Key Projects/Programs outlined by the SAIC report include:

- Smart Community Demonstration Project: The project, consisting of 655 households and 11 buildings, is the first demonstration community built by North China Power Grid as well as the first project constructed under SGCC's guideline on smart communities. The project, located at the Xin'ao Golf Garden residential complex in Langfang, Heibei province, was completed in September 2010. The project includes a low-voltage electricity network, power usage information collection, an interactive service platform, smart household installment, electric automobile charging facilities, distributed power generation and energy storage, automatic electricity distribution,

integrated network using low-voltage fiber optic cables, and AMI meters for electricity, gas and water.

- Smart Grid, Demand Side Management Pilot: IEEE, China. The project, developed and implemented by Honeywell, is China's first smart grid pilot project and feasibility study to monitor and manage electricity use in commercial buildings. The project focuses on DSM, and utilizes Honeywell's state-of-the-art smart grid technology, including automated demand response, advanced energy management, and sub-metering. The project is part of an agreement between the U.S. Trade and Development Agency (USTDA) and the State Grid Electric Power Research Institute (SGEPRI), a subsidiary of the SGCC.

- National Wind Power Integration Research and Test Center of China: The project centers on the development of renewable energy and clean energy storage. Toward that goal, the SGCC is installing 30 wind turbines with at least 78 MW of generating capacity, 640 kW of solar photovoltaic (PV) capacity, and 2.5 MW of energy storage. Prudent Energy is providing vanadium redox batteries. When it is completed, the testing center will be the largest facility of its kind in the world.

- Power System Digital Real-Time Simulation Device: This research project developed the first large-scale power system real-time simulation device. The device can simulate a power system with up to 1,000 generators and 10,000 bus bars. The development of this device will contribute to the safe operation of the power grid by researching the access of new large-scale equipment and enhancing power system incident analysis. The device will also allow equipment tests such as the safe and stable operation and control of a large AC/DC hybrid transmission system.

- 1000-kV Jindongnan Nanyang-Jingmen Ultra High Voltage (UHV) AC Pilot Project: Construction of a single circuit line of 640 kilometers, with a capacity of 6,000 MVA, and an operational voltage of 1,100 kV.

- Xiangjiaba-Shanghai +/-800-kV UHV DC Transmission Pilot Project: Construction of an advanced UHV DC high capacity, long distance, DC transmission line.

- Ningdong-Shandong +/-660-kV DC Project: Approved in November 2010 as a key project in the development of the West to East transmission project designed to move both hydro and thermal power from generation sites in the West to demand centers in the East.

- Qinghai-Tibet 750-kV/+/-400-kV AC/DC Grid Interconnection Project: Construction of a 750-kV AC project and a +/-400-kV DC power transmission project from Qinghai

to Tibet, allowing the integration for the first time of all provinces in SGCC's service area.

In addition, SGCC plans to implement 11 different types of smart grid projects, including building smart substations, installing 50 million smart meters, accommodating the integration of 20 GW of wind power, increasing electric vehicle recharging facilities by seven-fold, formulating 88 standards on smart grid, and completing construction of the integrated smart grid demonstration project in Sino-Singapore Tianjin Eco-City. The Eco-City, developed in partnership with Singapore as an environmentally friendly city, is located east of Tianjin's city center. Another smart grid project highlighted by SGCC is the Fujian Electric Power Company's 15.77 billion Yuan ($2.47 billion) investment in smart grid projects in the inland areas of Fujian province. In addition to 35 110-kV substations, the investment will include nine electric vehicle battery replacement stations, nine battery distribution stations, and 1,070 AC charging poles.

6.5.3 Current Cybersecurity Nexus

The State Grid Corporation has developed a draft Framework and Roadmap for Strong and Smart Grid Standards.

China is already leading the world in Wide Area Monitoring systems (WAMs) using phasor measurement units based on the Global Positioning System (GPS) with more than one thousand phased measurement units installed. The installation of WAMs is part of the Government's current five-year plan. By 2012, the State Grid had a target for phasor measurement unit (PMU) sensors at all generators of 300 MW and above, and all substations of 500 kV and above. Of the substations installed, all of the 110 kW substations and most of the 35 kV and 66 kV substations have an ISA system (International Society of Automation) and can be controlled remotely. New substations are likely to conform to the IEC61850 standard developed by State Grid.

Defining critical infrastructure protection

A 2013 EastWest Institute article on "China's Critical Cyber Infrastructure Protection" explains that in 2012, a policy working group in China issued a Blue Paper on China's Protection for Critical Information Infrastructure. This document does not give much insight into policy but it is, according to the EastWest article, significant. Above all, it demonstrates the relatively recent focus by China on a number of key policy decisions affecting its information security. The document is offered as a quick guide, an "introductory note for the international community to understand China's laws, regulations, and policies for the protection of critical information infrastructure." It was issued by the Information Security Law Research Center of the Xian Jiaotong University; one of the economy's self-designated top nine (C9) universities. The research center describes itself as the "executive body for China's Cloud Computing Security Policy and Law Working Group, and the composition of the working group which produced the paper is notable, according to the article, given representatives from the Protection Bureau of the

Ministry of Public Security (its lead Bureau), the First and Third Research Institutes of the Ministry of Public Security, leading private sector corporations (including Microsoft, Intel, Qihoo and Huawei), government and Communist Party agencies, and researchers.

The paper identified the following priority sectors: government affairs information systems; Communist Party affairs information systems; livelihood sectors (finance, banking, taxation, customs, auditing, industry, commerce, social welfare, energy, communication and transportation, and national defense industry); educational and governmental research institutes; and public communications, such as radio and television.

The article explains further that, apart from mentioning the 1994 introduction of a law on a national grading system for information security and various international commitments by China on information security in the framework of the Shanghai Cooperation Organization (SCO), the SCO's Blue Paper takes as its major reference point a set of 18 standards issued in 2010 by China's Information Security Standardization Technical Committee addressing Public Key Infrastructure Security, Cryptography and Certificate Authentication Systems, and a Guide for Graded Protection of Information System.

Under the New America study, which delineates key terms related to existing cybersecurity and information security definitions, no citations were made for critical infrastructure and China.

Defining cybersecurity

According to the 2015 ITU country report for China, legislation on cybercrime has been enacted through the following instruments: Art 285,286 & 287 Criminal Law, 1997; Art 285, Criminal Law, 2009. Legislation and regulation related to cybersecurity has been enacted through the following instruments: Regulations on Safeguarding Computer Information Systems 1996; Measures on Management of Internet Information Services 2000; Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security 2000.

The official national CERT is the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT). It produces reports used for educational and professional training purposes. There is a high level of cooperation among the Internet Society of China, China mobile, China Telecom, China Unicom, China Internet Network Information Center and CNCERT/CC. CNCERT, along with China Education and Research Network Emergency Response Team (CCERT), is an operational member of APCERT. China also hosts four members of FIRST according to ASPI's report. China's Information Security Standardization Technical committee issued 18 standards in 2010.

China's national cybersecurity policy, according to the ITU factsheet, is the National Medium- and Long-Term Program for Science and Technology Development (2006-2020). China does not currently have any national governance roadmap for cybersecurity. ITU's factsheet explains that

the agencies responsible for implementing national cybersecurity strategy and policy include the Ministry of Industry and Information Technology (MIIT); State Internet information Office; and National Network & Information Security Coordination Team; Ministry of Science and Technology; and The Central Internet Security and Informatization Leading Group. The Central Internet Security and Information Leading Group increases the coordination among different government department sectors. ITU's report explains that the Annual Chinese Conference on Computer and Network Security by the Office of the Cyber Affairs is the officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector. China is a member of the ITU-IMPACT initiative.

The 2013 UNIDIR Cyber Index report notes that in 2012, China's State Council issued a set of new cybersecurity policy guidelines calling for intensified efforts to better detect and handle "information emergencies", reduce internet crime and better protect personal information. Several ministries in China have responsibility for cybersecurity, including the Ministry of Public Security and the Ministry of Industry and Information Technology, both of which are overseen by the State Council. The Ministry of Public Security is responsible for investigating cybercrime and responding to emergencies. The Ministry of Industry and Information Technology is responsible for regulation and development, and has domestic responsibilities similar to those of the Department of Homeland Security in the United States; it sets standards, holds exercises, carries out inspections on network security, and operates the national CERT.

Under the New America compilation of terms and definitions, the following key terms related to existing cybersecurity and information security definitions are delineated for China:

> Information Security: It is the view of China that the problem of information security not only involves the risks arising from the weakness of the basic information infrastructure, but also the political, economic, military, social, cultural and numerous other types of problems created by the misuse of information technology. Each of these two factors is worthy of equal concern when studying the problem of information security.
>
> It is the view of China that the issue of information security involves not only the risks arising from the weakness and interconnected nature of the basic information infrastructure, but also the political, economic, military, social, cultural and numerous other types of problems created by the misuse of information technology. Both of these factors are worthy of concern when studying the issue of information security.

A 2013 Carnegie Endowment report by Michael D. Swaine on "The Chinese Definition of Cybersecurity and the Challenge It Presents" notes that authoritative Chinese sources do not provide a detailed definition of cybersecurity and the challenge it poses. Statements largely refer in general terms to the growth of the internet, the increasing dependence of many nations on cyber-based activities, the potential dangers posed by cyber-based attacks or incursions, and the need for governments to provide more supervision over the internet. Nonetheless, such general

statements, combined with the more detailed discussion of such issues appearing in non-authoritative sources, suggest that most Chinese conceive of cybersecurity in a similar manner to observers in other economies. That is, it involves the protection of the internet against harmful activities directed against or having the effect of undermining national security or commercial, social, and individual interests. Such interests include the capacity of the state to defend itself and society, the ability to compete fairly and productively in the national and global economic order, the preservation of social norms, and the privacy and security of the individual citizen.

A 2014 Georgetown Journal of International Affairs explains that over the past two decades, the Chinese Government has defined the term "Informatization" to describe a policy of modernization via digitalization nationwide and to apply new ICT in all areas of government, industry, commerce, education and culture. It has become a key component of China's five-year planning process for central and local governments.

6.5.4 Cybersecurity Challenges (Issues)

A key challenge is encouraging domestic regulators to learn about relevant activities at the international level, as well as understand how these standards can be used to meet their goals.

Challenges faced by China also include the variable nature of renewables and the need to transfer energy over long distances. Therefore, a key enabler for integrating renewable sources of energy into the smart grid in China will be large storage technology.

A McAfee report on crucial industries explains that when it comes to how governments are responding to the vulnerability of their core civilian infrastructures, in general, they continue to play an ambiguous role in cybersecurity—sometimes helping the private sector, sometimes ignoring it. Here, China continues to draw the most attention according to the report. China's Government seems to play a strong role in demanding security from its critical infrastructure. Chinese respondents, for example, view Chinese Government security requirements, with respect, and China had the second highest rate (after Japan) of government security audits.

More than 40 percent of the executives interviewed expected a major cyber-attack within 12 months—an attack, that is, that causes severe loss of services for at least 24 hours, a loss of life or personal injury, or the failure of a company. Fear of a major attack was relatively high in China, where over half of respondents expected such an attack in 2010 or 2011.

To measure public-private relationships, McAfee asked IT executives how they interacted with government, suggesting many alternatives, including no interaction at all, informal information-sharing, and regulatory oversight. Chinese executives were at the top of the scale—reporting high levels of both formal and informal interaction with their government on security topics. Similarly, only a handful of Chinese executives (about one in 20) said that they had no contact with government agencies regarding network security—one of the lowest non-involvement rates in any economy.

However, the ASPI 2014 report on cyber maturity explains that China's cyber capabilities are well established, but what is less well understood is whether there is sufficient internal cyber coordination within the Government. This is reflective of a wider domestic disinterest in establishing solid cybercrime or cybersecurity legislation or working constructively with businesses. Attention is instead diverted to bolstering domestic surveillance laws and promoting the primacy of the state in internet governance within international forums.

It further notes that China has an array of government organs involved in cyber issues, including the Ministry of Information Industry, the Department of Information Security Coordination, the Bureau of Communications Security, the Ministry of State Security and the National Administration for the Protection of State Secrets, to name a few. The report highlights the uncoordinated way these organizations operate and the seeming lack of overarching, comprehensible, national cyber policy goals or strategy.

Moreover, it notes that in February 2014, China established the Central Internet Security and Information Leading Group, a high-level committee charged with addressing increased cyber-attacks, guiding public opinion and turning China into a global internet power. Headed by President Xi Jinping and including Premier Li Keqiang, the group has great influence, but it is unclear what impact, if any, it will have on Chinese cyber policymaking. The report notes that engagement between the business community and the Government on cyber issues is often confused by a lack of clarity in areas of responsibilities within government, complex regulatory regimes and inconsistent implementation of policy. The Chinese Government has recognized the threat of cyber attacks to Chinese business, but comprehensive action on the issue is not widely evident. The report notes the need for legislation to address cyber issues comprehensively. In addition, it finds that CNCERT, which coordinates other CERTs within China, is difficult to rate in terms of effectiveness using open sources. The report notes that CNCERT also plays a role in national monitoring.

The 2013 Carnegie Endowment report sheds some further light be explaining that most Chinese have the same concerns as much of the rest of the world about harmful cyber activities, including: efforts to crash, slow, or paralyze vital cyber-based infrastructure; the promulgation of information or images harmful to the polity, society, or the economy (such as pornography, false or misleading commercial information, and the advocacy of violent political revolution); espionage; the theft of proprietary commercial data or information; and specific actions designed to weaken the capacity of the state to defend itself through military and other means. Thus, both authoritative and other Chinese observers believe that "cyber security is an international . . . issue and hacker attack is a common challenge facing the whole world." The Chinese also seem to agree with observers in other economies that cybersecurity is a particularly challenging issue because of the technical characteristics of the internet and the growing presence of cybercrimes and other forms of dangerous behavior.

Both Ministry of Foreign Affairs and Ministry of Defense officials state, "China is a major victim of hacker attacks." In response to such threats, and the overall security challenge presented by cyber activities, authoritative Chinese sources declare the Chinese Government always opposes and strictly prohibits any illegal criminal activity by hackers. The Chinese law stipulates unequivocally that those who commit cybercrimes should undertake criminal liability in accordance with the Criminal Law of the People's Republic of China.

The 2014 material in the Georgetown Journal of International Affairs explains that the State Informatization National Development Strategy (2006–2020) includes goals for social progress and increased access to technology. It also includes goals for progress related to China's information security policies in the following areas: information security laws and regulations; State sponsorship of strategies for indigenous innovation; domestic security standardization and enforcement; security assurance and certification (China Compulsory Compliance); and government security requirements for procurement. The 12th Five Year Plan for Informatization published by the Ministry of Industry and Information Technology (MIIT), which was released in 2013, continued to list information security as a top priority. However, public information on strategy in China is limited.

As a part of the 11th Five Year Plan (2006-2010), China began investing in the protection of government information systems. The Government defined and implemented a Multilevel Protection Scheme (MLPS) with mandatory security controls for all government systems and Internet services considered critical to the economy. The MLPS has a five-level risk-based classification to identify and protect those systems that are critical for national security and the economy (Level 3 and above). The MLPS is enforced for all government systems nationwide, and in recent years, large internet service providers have been included in this enforcement effort.

Cyber-related policy opportunities and challenges for further consideration:

China should continue to monitor closely possible cyber threats to oil and gas suppliers, the supply chain, its electric grid, and pipelines particularly since many major global oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. This could possibly cause damage but breaches may also cause high damage to corporate assets, public infrastructure and safety, or the wider economy. Analysts have noted that, while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain.

Since the Fukushima Daiichi nuclear plant disaster in 2011, China has paid more attention to the safety of nuclear energy. Given the economy's interest in nuclear energy, it should continue to monitor the nexus between cybersecurity and this sector. The IAEA (as well as several other

nation states), for instance, provide guidance for consideration by states, competent authorities, and operators.

Regarding international efforts, the ASPI report finds that there is a systematic approach of Chinese to engagement in bilateral and multilateral international forums across the full spectrum of international cyber policy and security issues, including the UNGGE. In 2011, China joined Russia, Tajikistan and Uzbekistan in proposing to the United Nations an international code of conduct for information security, followed by a multistate proposal in 2012 to give the ITU greater control over the internet.

In May 2015, reports outlined the signing of "a nonaggression pact in cyberspace" between Russia and China. While reports note that China and Russia have always had a very close and friendly historical relationship, analysts note that Russia has energy and China needs energy. Under the agreement, the reports note that the two economies have agreed not to hack each other. Both economies also pledged to thwart technology that might "destabilize the internal political and socio-economic atmosphere," "disturb public order" or "interfere with the internal affairs of the state." Additionally, both sides will exchange cyber threat data and information technology.

At regional level, China is a participant in the ASEAN Regional Forum (ARF).

China is participating in the fourth UN GGE (2014/2015), the fourth Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

6.5.5 Future Cybersecurity Nexus

According to a report by the consulting firm, GlobalData, the Chinese SCADA market will soar in value in the coming years, from $3 billion in 2012 to $20 billion by 2020.

6.5.6 Smart Grids

Given its interest in the smart grid, enhancing cybersecurity is essential and it should be considered as part of a larger smart grid deployment strategy.

The McAfee Report specifically notes that regarding growing interconnectivity and the smart grid, despite widespread industry unease about the growing vulnerability of the power grid, and the lack of preparedness for a network attack, power companies and governments seem to be "doubling down on the danger". The report notes that plans to exercise far more precise control over consumers' use of electricity has aroused great enthusiasm among government policymakers. At the same time, customers and consumer groups have raised concerns about what the smart grid will mean for energy prices and privacy. The report notes that its data shows an industry that is charging ahead with smart grid implementation. Four out of five industry executives said their company intended to implement some form of smart grid controls, such as time-sensitive rates, service cutoffs, and service reductions. However, extending network control

to the household or even the appliance level will create new opportunities for harm if the network itself is not secure. If the new smart meters or the network that supports them are taken over by attackers, they could be used to disrupt the delivery of electricity in a fine-grained way, singling out particular users or even appliances for power cuts or perhaps surges. Most executives and outside observers do not believe that the networks controlling power systems are secure today, according to the report. Measured objectively, some economies are clearly more security conscious than others. China was a standout, well ahead of other economies in adoption of security measures. It maintained its position as the economy with the highest security adoption rate overall at 59 percent, followed by Italy and Japan.

6.6 Hong Kong, China

6.6.1 Economy Energy Resources

The 2014 APEC Energy Overview Study provides an extensive outline of the energy sector in Hong Kong, China. Hong Kong, China has no domestic energy reserves or petroleum refineries - it imports all of its primary energy needs. A substantial share of imported energy is converted into secondary energy such as electricity and gas for final consumption.

6.6.2 Smart Grid Initiatives

Hong Kong, China has made limited progress in the development of smart grids. It has not yet formulated a specific policy framework or plans and programs for smart grid technologies. Universities and utilities conduct some R&D projects and small-scale community pilots (Cheung, 2011; Li and Yang, 2011). One of these initiatives is a smart meter pilot conducted in Lohas in Tseung Kwan O by China Light & Power Company (CLP) (Cheung, 2011). Several smart grid companies provide IT services and smart grid appliances in the city (Tsang, 2011). These initiatives, however, are relatively small in scale and limited in scope. Studies examining economic benefits and costs of the potential deployment of smart grids in Hong Kong, China have been
lacking, although such studies could generate important data with which policy makers and other stakeholders can assess technological and policy options.

A major target for the economy's energy policy is to reduce its energy intensity by 40 percent by 2025 and key actions are focused on economic, regulatory, educational and social measures.

In addition, CLP describes its mission on its website as finding better ways to deliver cleaner energy, better services and more value to customers through a reliable and secure power grid. It describes its strategy as incorporating the latest and most relevant technologies to improve the power grid performance.

Its ultimate goal is the development of a smart grid by integrating digital, telecommunications and metering technologies with the power systems. The expected result is to improve the power grid management system in terms of monitoring, analysis, control and information collection capabilities. CLP's website describes the implementation of a smart grid as possibly long, challenging, and involving system automation, condition monitoring, and customer interaction. It highlights as equally important the grid's capabilities in accommodating connections with renewable energy sources and distributed generation, and supporting electric vehicles.

As part of building customer awareness and buy-in, CLP highlights its "Smart Grid Experience Centre". The website explains that the smart grid era is coming; it should enable safe and seamless connection of renewable energies, and electric vehicles, further improve power supply reliability at a lower cost and enable its customers to take control over their energy usage. This is the first exhibition and education facility of its kind in Hong Kong, China according to CLP and the facility showcases the benefits of a smart grid together with the latest smart grid specific technologies such as smart meters. It also demonstrates projects currently undertaken by CLP.

The University of Hong Kong has a section on its website discussing the "Smart Grid, Smart Planet". It describes a future where power comes from a seamless mix of renewable energy and traditional sources delivered by a computer-controlled grid that manages thousands of windmills and thousands of customers. The website explains that Professor Felix Wu of the Department of Electrical and Electronic Engineering developed a working prototype. It describes how this is a green solution to outdated management systems that will result in energy savings and allow consumers a choice in electricity charges. It notes, however, that the difficulty for the energy industry is that smart grids do not yet exist and power companies cannot experiment with existing supplies. Without an actual grid to conduct research, Professor Wu designed a simulated lab, including inbuilt equipment failures to test the system, which is "self-healing".

6.6.3 Current Cybersecurity Nexus

Defining critical infrastructure protection

According to a 2011 brief on cybersecurity from the Office of the Government Chief Information Officer (OGCIO) at the Commerce and Economic Development Bureau, critical infrastructures in Hong Kong, China are owned either by the Government or under the governance of regulatory bodies. Since the regulatory bodies are the domain experts of their respective regulated sectors, the 2011 brief outlines that it would be most effective and appropriate for them to determine the extent of regulatory measures including those in relation to information security and cyber threats.

According to this brief, for the protection of the local internet infrastructure, the OGCIO set up the Internet Infrastructure Liaison Group (IILG) in 2005 to provide a platform for communication and exchanges on issues concerning the stability, security, availability and

resilience of the local internet infrastructure. The IILG collaborates among the relevant stakeholders during major events or situations with emerging information security threats. The HK Police Force (HKPF) and the OGCIO render advice and assistance as necessary on information security enhancement measures for regulated bodies/sectors under their purview.

Defining cybersecurity

The OGCIO at the Commerce and Economic Development Bureau brief on the "cyber security posture" in Hong Kong, China explains that, like other economies, the Government, businesses and citizens in Hong Kong, China rely heavily on information and communications technology (ICT) and the internet in their business operations and daily lives. At the same time, cybercriminals or malicious attackers are also employing advanced technologies to carry out illegal or illicit activities. The "cyber space, which comprises the telecommunications infrastructure, critical information infrastructure and systems, becomes a domain that should be better protected for public security and economic prosperity".

According to this brief, cybercrime, or computer crime, in general refers to any crime in the cyber space that involves a computer and a network. Cyber-attack refers to a form of cybercrime using special software to cause the malfunctioning of targeted computer systems or networks resulting in information leakage, identity theft and/or disrupted businesses or services.

6.6.4 Cybersecurity Challenges (Issues)

In January 2014, Mr Victor Lam, the Deputy Government Chief Information Officer, addressed the Cyber Security Symposium organized by the HKPF to discuss "cyber security challenges in maintaining large-scale information systems". He explained that it is crucial to maintain a safe cyber environment for the Government, businesses, and the public. He explained that concern over cyber-attacks on critical infrastructures is growing worldwide and that in Hong Kong, China the information systems of critical infrastructures, including those of the financial, transportation and telecommunications are also subject to information and network security threats, which could affect daily life if the telecommunications networks or power plants or traffic control systems are affected. He outlined that it is important to strengthen the protection of information systems supporting the critical infrastructures. This requires effective partnerships that foster integrated and collaborative engagement among the public and private sectors. In Hong Kong, China the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) is responsible for the coordination of computer security incident response for local enterprises and the public. To strengthen the economy's resilience against cyber-attacks, HKCERT has been collaborating closely with global security organizations and CERTs, the HKPF, and the OGCIO through the sharing of intelligence and by acting as a contact point on global security incidents.

He further explained that cybersecurity is no longer a local or regional subject matter, and that effective collaboration among local organizations as well as related organizations in other

economies is of vital importance to strengthen Hong Kong, China's resilience against cyber-attacks. OGCIO, HKPF, and HKCERT have been collaborating and maintaining close ties with both local and overseas security organizations, CERT bodies and law enforcement agencies.
Initiatives are in place to increase the protection of the local critical infrastructures' information systems, and to strengthen cooperation among government departments and stakeholders. He argues that organizations and critical infrastructures should recognize the importance of collaboration and information sharing in protecting their IT assets.

The OGCIO brief explains that in Hong Kong, China the national and military angles are not applicable. The Security Bureau (SB) and the OGCIO provide guidance and advice to bureaus and departments on information security. The SB and OGCIO work closely to maintain surveillance on any emerging cyber security threats, examine and tackle cyber security issues and continue to introduce additional measures to strengthen Hong Kong, China's cyber security posture.

It further explains that HKCERT, operated by the Hong Kong Productivity Council (HKPC), plays a key role in the protection of the local cyber environment. One of the core functions of HKCERT is to serve as a focal point in Hong Kong, China for computer security incident reporting and response. It also assists the community against computer security threats and hacking attacks, and in recovery actions for computer security incidents. The OGCIO and HKPC jointly review and enhance the service of HKCERT according to cyber security trends and public needs from time to time.

HKCERT has also organized local information security incident response drills annually since 2009, to ascertain the responsiveness by local key internet stakeholders against cyber-attacks. Through the exercise, the participants gain experience on how to respond to emergency conditions and the organizer can gain insights on how to coordinate and improve communication amongst the stakeholders during major incidents. HKCERT has participated in some of the APCERT drill exercises.

The OGCIO set up the INFOSEC website (www.infosec.gov.hk) in 2002 to provide a one-stop portal facilitating public access to various information security related resources and updates. To raise public awareness on information security and strengthen the protection of their computer and information assets from cyber-attacks, the OGCIO, HKPF and HKCERT have jointly organized an annual promotion campaign "Hong Kong Clean PC Day" since 2005. According to the APEC Counter-Terrorism Action Plan, submitted by Hong Kong, China in February 2014, it has held crime prevention seminars between January and August 2013 for Small and Medium Enterprises to raise their cybersecurity awareness.

In order to enhance the protection of critical infrastructures and strengthen Hong Kong, China's resilience against cyber-attacks, Hong Kong, China established the Cyber Security Centre under the Hong Kong Police Force in December 2012. According to the APEC Counter-Terrorism

Action Plan, leaders and ministers' commitments include:

- Countering terrorism by implementing and enhancing critical information infrastructure protection and cyber security to ensure a trusted, secure and sustainable online environment (2002); and
- Enhancing cooperation on countering malicious online activities and engage in efforts to increase cybersecurity awareness (2010).

According to this submission:

- HKC attaches great importance to strengthening information security and providing a secure environment for the conduct of e-commerce in Hong Kong, China.
- The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and the Hong Kong Police Force, co-organize an annual security campaign to raise public awareness on information security especially on mobile computing, social networking, cloud computing and targeted attacks.
- Security seminars were organized for the public in May, November 2012 and January, April, August 2013 on topics related to the latest cybercrime trends and security threats, and protective measures when using mobile devices, social networks and cloud services.
- A "Combating Cyber Attack" poster design was organized from May to July 2012 with an aim to enhance public awareness about the importance of safeguarding their computer and information assets from cyber-attacks.
- A Cyber Security Symposium was held in August 2012 for major internet infrastructure stakeholders, including internet/network service providers and online service platform providers to discuss major cyber security issues & trends and measures to strengthen cyber security and coordination among multiple parties.
- An incident response drill with the theme "Defending against Hacktivist Cyber Attack" was conducted in October 2012. Key players in the internet community of HKC participated. The drill successfully tested the malware detection and malicious website tracking capabilities as well as incident handling procedures of participants.
- Videos on best practices of information security have been posted to the InfoSec YouTube channel since December 2012.
- Security alerts have been disseminated through GovHK Notifications service to subscribed mobile users since December 2012.
- The Technology Crime Division (TCD) of the Hong Kong Police organizes various professional training courses in relation to technology crime investigation and computer forensics with a view to maintaining professional capabilities of local and overseas counterparts. To raise the cyber security awareness of Small and Medium Enterprises (SME) in Hong Kong, China, the Hong Kong Trade Development Council, SME One of Hong Kong Productivity Council and the Hong Kong SME Association held four crime prevention seminars between January and August of 2013.

Plans include:

- Public promotion and education events will be held in the coming years through various channels. These include disseminating information security tips via mobile apps, websites and radio broadcast; arranging security seminars for the general public and thematic cyber security symposium for the internet infrastructure stakeholders and other key players.
- Dissemination of crime prevention messages to members of the public in different sectors will continue through TV, radio, e-banners on websites, press releases and public seminars in collaboration with other stakeholders.
- Working with the INTERPOL Group of Experts on IT Crime Asia and South Pacific (EGASP), the Hong Kong Police will continue to support the INTERPOL in conducting various Train-the-Trainer Workshops on IT crime investigation and computer forensics to consolidate the cyber-attack response capabilities in the Asia-South Pacific Region.

According to ITU's profile, Hong Kong, China has an officially recognized national cybersecurity policy (Baseline IT Security Policy) and a national governance roadmap for cybersecurity. The Information Security Management Committee is the officially recognized agency responsible for implementing the national cybersecurity strategy, policy and roadmap. To raise public awareness on information security and strengthen the protection of their computers from cyber-attacks, Hong Kong, China has organized annual campaigns covering contemporary topics since 2005. Every year, it organizes seminars, conferences, competition events to raise public awareness to protect their computer assets and be mindful of suspicious cyber-attacks with a
view to building a "Secure Cyber Space". Hong Kong, China also disseminates security alerts, news and tips through the one-stop portal INFOSEC website, as well as promotes security awareness through posters, leaflets and radio clips. It has partnerships with ITU, APCERT, APEC, and INTERPOL. The OGCIO established the IILG in 2005 to maintain close liaison with internet infrastructure stakeholders. The Deputy Government Chief Information Officer (Consulting and Operations) chairs the IILG. Members of the IILG including OGCIO, HKCERT, Hong Kong Internet Registration Corporation Limited (HKIRC), Hong Kong Internet Service Providers Association (HKISPA), HKPF, and Office of the Communications Authority (OFCA). The Cybersecurity Security Centre (CSC) under the Technology Crime Division of Commercial Crime Bureau of the HKPF began operating in 2012. Its mission, according to the factsheet, is to enhance the protection of critical infrastructures and strengthen resilience against cyber-attacks in Hong Kong, China. HKCERT is a member of FIRST.

Since 2009, OGCIO, HKPF and HKCERT have also collaborated to organize information security incident response drills for the stakeholders of internet infrastructure, including internet service providers, mobile operators, and domain name registrars. The drill exercises aim to test the stakeholders' incident handling capabilities and practice their incident response procedures.

They urge critical infrastructure companies and other related organizations to participate actively in forthcoming drills to enhance their incident response readiness.

Cyber-related policy opportunities and challenges for further consideration:

Hong Kong, China should closely consider cyber issues relevant to the electric grid as well as the supply chain.

Hong Kong, China should consider possible cyber threats to oil and gas suppliers, particularly since major oil and gas producers globally have fallen victim over recent years to cyber-attacks or had their networks infected. These might cause damage but breaches may also cause high damage to corporate assets, public infrastructure and safety, or the wider economy. In addition, it could affect the economy's competitiveness. Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain.

Since Hong Kong, China has developed an energy end-use database to provide an understanding of the energy consumption patterns and usages, and arouses public interest and concern over the future development of energy in Hong Kong, China. A basic data set is publicly available on the internet and the Government is able to analyze the current system, while the private sector can use the data to benchmark their own energy efficiency.

To increase the public's confidence in nuclear safety, CLP in January 2011 contributed to an enhanced program of public education and awareness about nuclear energy through initiatives such as plant visits, roving exhibitions and an online education platform. The program aims to inform the public on nuclear related matters, and to bring a higher degree of confidence in the future role of nuclear energy in powering Hong Kong, China. Including measures to counter malicious or accidental cyber incidents would also help ensure that public confidence is maintained. The aim is to prevent the theft of material or sabotage of plants and facilities.

Hong Kong, China proposes to reduce significantly its reliance on fossil fuels, gradually phasing out existing coal-fired power generation units, and increasing the use of non-fossil, cleaner and low-carbon fuels, including renewable energy and imported nuclear energy. In 2015, the Government promulgated the fuel mix for 2020, which is to increase the proportion of natural gas for power generation from around 20 percent at present to around 50 percent in 2020, to maintain the current interim measure of importing 80 percent of the nuclear output from the Daya Bay Nuclear Power Station (i.e. the nuclear power import will account for around 25% of the total fuel mix), and to meet the remaining demand for electricity by coal-fired generation and renewable energy.

Reports outline that greenhouse gas emissions reduction measures include, improving energy efficiency in commercial buildings through good housekeeping, information technology products

and intelligent building environmental management systems, so that by 2020 up to 25 percent of existing commercial buildings will be 15 percent more energy efficient compared with 2005, along with measures to promote the use of electric vehicles and to implement energy efficiency standards for vehicles. Again, measures to deal with cyber-related incidents should be incorporated.

Some 90 percent of daily commuter trips are via the public transport system. The Government is committed to further expanding and upgrading its public transport infrastructure with emphasis on railways. The Government actively promotes wider use of electric vehicles. Again, these plans should include cybersecurity considerations.

6.6.5 Future Cybersecurity Nexus

There is insufficient data on this topic for Hong Kong, China. This is a potential area of future growth for the economy.

6.6.6 Smart Grids

Hong Kong, China's stated ultimate goal is the development of a smart grid integrating digital, metering technologies and telecommunications with the power systems. The expected result is to improve the power-grid management system in terms of monitoring, analysis, control and information collection capabilities. Given that CLP is hoping to find better ways to deliver cleaner energy, better services and more value to customers through a reliable and secure power grid by incorporating the latest technologies to improve the power grid performance, cybersecurity considerations should be a priority from inception.

Hong Kong, China is aware that it is important customers are informed and comfortable with such developments and undertake efforts to educate and increase awareness by CLP through its Smart Grid Experience Centre. Consequently, reassuring consumers that their data is being used appropriately, that they have control of their data, and that strong cybersecurity measures are in place should go some way to reinforce their confidence in these new systems. (CLP's Smart Grid Experience Centre is listed on the ESCI Knowledge Sharing Platform.)

According to reports, buildings consume about 90 percent of the electricity used in Hong Kong, China. The economy's first priority is conserving building energy. To strengthen its efforts to improve the effects of building energy conservation, the Government has enhanced the regulatory system for building energy efficiency. The Buildings Energy Efficiency Ordinance was fully implemented in 2012. Key opportunities to consider should include cybersecurity measures for both new buildings and retrofitting, and when audits are conducted, cybersecurity measures should be included. Given that reports state that the Government continues to demonstrate in government buildings state-of-the-art energy efficient designs and building energy conservation technologies, this should ideally include best practice cybersecurity measures.

6.7 Indonesia

6.7.1 Economy Energy Resources

According to the APEC Energy Overview Study published in March 2014, domestic oil, gas and coal reserves have played an important role in Indonesia's economy as a source of energy, industrial raw material and foreign exchange. In 2011, oil and gas exports contributed 20.4 percent and coal exports contributed 13.4 percent of Indonesia's total exports. Indonesia's total primary energy supply comprised oil (46.8 percent), coal (26.8 percent), natural gas (21.2 percent) and other energy (mainly hydropower and geothermal) (5.3 percent), and biomass. Indonesia is a net exporter of energy.

6.7.2 Smart Grid Initiatives

2014 reports online outline that some emerging economies, such as Thailand, Malaysia, Indonesia, and the Philippines, are making plans to deploy smart grid technology. While this region is currently behind other global regions in terms of smart meter deployments and regulatory frameworks, its smart grid market is growing. There are already smart grid pilot projects in several economies throughout the region. By 2022, Southeast Asian economies will likely have an electricity demand profile similar to Latin American economies where large-scale smart meter deployments already exist. The region's current electricity consumption rates are among the lowest in the world, while distribution loss rates are comparatively moderate, offering less short-term savings potential compared with other global regions. Additionally, regulatory frameworks remain largely undeveloped in the region. Even in the more advanced economies, deployments are still at the initial pilot level.

These 2014 reports say that investment in Southeast Asia will include smart metering and the modernization of electricity transmission and distribution networks with sensors, communications and software. By 2024, the largest markets will be Thailand, Indonesia, Malaysia, Singapore, the Philippines, and Viet Nam, according to a recent study by Northeast Group LLC.

Southeast Asian economies are just beginning on the path of modernizing their electric infrastructure. Electrification programs and growth in renewable resources will also drive investment. Singapore is currently leading the region in development but later in the decade, the large markets of Thailand, Indonesia, Malaysia, Viet Nam and the Philippines will account for significant smart grid investment. Several economies in the region have drafted smart grid roadmaps and pilot projects are widespread. Regulatory frameworks are still developing but momentum will grow over the next several years. Both utilities and vendors are already working together to ensure preparedness when regulations are finalized. Many vendors are active across the region (these include ABB, Alstom, Echelon (NES), EDMI (Osaki), Elster, Enverv, GE,

Itron, Schneider, Secure, Siemens, Silver Spring Networks, ST Electronics, Trilliant and other global and local vendors).

2013 presentation slides from the Indonesian Coordinating Ministry of Economic Affairs cite pilot projects as including the Smart Microgrid on Sumba, and potential projects such as Jakarta Smart City (comprising Superblock Smart Micro Grid).

The objective of the World Bank 2014 project, Capacity Building for Smart Grid Investment for Transmission and Distribution, is to assist the Government of Indonesia meet growing electricity demand and increase access to electricity in a sustainable manner. The project will strengthen and expand the capacity of the power transmission networks in Java-Bali and other islands in East and West Indonesia and improve the PLN's capacity to plan and operate the transmission and distribution network in an efficient and transparent way through introduction of smart grid technologies. The proposed project would consist of four components: 1) extension, rehabilitation and construction of substations in Java-Bali system; 2) extension, rehabilitation and construction of substations in East Indonesia; 3) extension, rehabilitation and construction of substations in West Indonesia; and 4) technical assistance for capacity building for planning and implementation of smart grid technologies for PLN transmission and distribution systems.

Earlier online reports stated that PLN reported in 2011 that it was in the early planning stage for three small smart grid pilots in Jakarta, Batam, Sumba and Bangka. However, reports then said that smart grid was secondary to PLN's top three priorities of universal access, network reliability, and quality of service. These projects began in 2012 and continue.

6.7.3 Current Cybersecurity Nexus

Indonesia and Australia collaborated in 2011 to establish the Cyber Crime Investigation Center in Jakarta. In May 2013, a second joint cyber-crime office opened to share information, coordinate investigations, and tackle cyber-crime originating in Indonesia.

Defining critical infrastructure protection

Open source searches do not currently produce a list of material related to the definitions of critical infrastructure protection or critical infrastructure in Indonesia. DAKA's Advisory report notes that Indonesia lacks a formal definition of critical infrastructures.

Defining cybersecurity

According to the 2015 ITU country report, specific legislation on cybercrime has been enacted through the Law of The Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transaction (Articles 29-37). Regulations regarding cybersecurity and compliance requirements include: Government Regulation of The Republic of Indonesia Number 82 of 2012 concerning Implementation of Electronic Systems and Transactions; SNI/ISO/EIC

27001: 2013, Information Security Management System; National Information Security Index (Index KAMI). Indonesia has national and sector specific CIRTs that include Gov-CERT, ID-SIRTII, ID-CERT, and Academic CERT. It has several public and private CERTs. While the operational capacity of the CERTs could be stronger according to the ASPI report on cyber maturity in 2014, Indonesia participates actively in forums such as APCERT, which it co-founded with Australia and Japan. Both ID-CERT and the Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (ID-SIRTII/CC) are operational members of APCERT.

The ITU country report for Indonesia cites that it does not yet have officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards. It does not currently have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals. It also does not currently have an officially recognized national cybersecurity strategy or national governance roadmap for cybersecurity.

The Directorate of Information Security, the Directorate General of Informatics Applications and the Ministry of Communication and Information Security are the officially recognized agencies responsible for implementing a national cybersecurity strategy, policy and roadmap in Indonesia. According to the 2014 ASPI report, Indonesia is developing higher-level cyber policy frameworks and has plans to create a 'national cybersecurity body'.

The ITU country report outlines that Indonesia does not currently have any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development but that the current measurement is based on the National Information Security Index (Index KAMI). The Directorate of Information Security and Ministry of Communication & Information Technology conduct awareness-raising and technical assistance programs that provide educational and professional training programs for the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in the public and private sectors. Indonesia has approximatively 500 public sector professionals certified under internationally recognized certification programs in cybersecurity such as ISO 270001, CEH, CISA, CISM and CISSP. It has six government institutions certified under internationally recognized standards in cybersecurity such as ISO 270001. It also has an officially recognized partnership with the National Information Security Council (NISC) of Japan.

Indonesia is in the process of recognizing national or sector-specific programs for sharing cybersecurity assets within the public sector as they are developing a national government security-monitoring center. Indonesia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. It has anticipated in cybersecurity activities with the following organizations/forums: FIRST; APCERT; ASEAN-Japan expert cybersecurity Forum; Indonesia-

JAPAN Bilateral Cybersecurity Forum; Internet Governance Forum; ASEAN Network Security Council (ANSAC) Working Group; and the World Conference on International Communication. The DAKA Advisory report mentions that IS-SIRTII is also a member of OIC-CERT.

The ASPI cyber maturity report of 2014 finds that, while Indonesia is engaged internationally, its participation is generally passive. Indonesia has enacted some cyber-specific and cyber-related legislation, including the 2010 TIPITI (cybercrime) Act, but it is not clear that those laws are systematically enforced. It conducts targeted filtering of content, including pornography and extremist websites, but the filtering is often applied inconsistently by ISPs.

Similarly, the DAKA Advisory report finds that Indonesia is particularly weak in legislative measures and officials have publicly acknowledged that it is vulnerable to cyber threats in part because of weak legislation. Experts cite the current legislation frequently as Indonesia's most glaring weakness in meeting the cybersecurity challenge. It deals primarily with cybercrime. Strong regulation is not viewed solely as an end to self-regulation but also as deterrence and an important part of a strong defense.

ASPI's report also highlights that the Indonesian Defense Minister has announced plans to establish a Cyber Defense Operations Centre to coordinate national cybersecurity efforts, including service-specific work by the Indonesian military on cybersecurity. The Centre, established in 2014, is to draft a national doctrine on cybersecurity and conduct implementation strategies across defense and other departments. The creation of a dedicated 'cyber army' has also been proposed. The Defense Minister explained that the force would consist of elite membership embedded in the various branches of the Indonesian military to protect domestic networks against cyber-attacks. In January 2015, Indonesia announced that it would form a National Cyber Agency (NCA) to coordinate an integrated defense against rising cyber-attacks. These developments show that there is awareness of cyber threats in the Indonesian military and government. There also are some moves by the Government to engage business on cyber issues specifically related to the oversight and regulation of ISPs.

ASPI's report explains that recently, there has been strong domestic media coverage of foreign intelligence gathering targeting Indonesian leaders. There is also semi-frequent coverage of "attacks" against government websites and debates about freedom of speech online. Indonesian leaders have recently taken to publicly emphasizing cybersecurity issues, which should help to broaden the debate beyond its current focus on foreign surveillance.

6.7.4 Cybersecurity Challenges (Issues)

In 2007, Indonesia enacted Law No. 30/2007 for energy issues. This Energy Law contains principles for utilization of energy resources and final energy use, security of supply, energy conservation, protection of the environment with regard to energy use, pricing of energy, and international cooperation. It defines the outline of the National Energy Policy (Kebijakan Energi

Nasional or KEN); the roles and responsibilities of the Government and regional governments in planning, policy and regulation; energy development priorities; energy R&D; and the role of businesses. The Energy Law mandated the creation of the National Energy Council (Dewan Energi Nasional, DEN). DEN's tasks are to draft the National Energy Policy (KEN); endorse the National Energy Master Plan (Rencana Umum Energi Nasional, RUEN); declare measures to resolve energy crises and energy emergencies; and provide oversight on the implementation of energy policies that are cross-sectoral.

The 2013 UNIDIR Cyber Index reports outlines that in 2012, Indonesia's Deputy Defense Minister announced plans for the creation of a cyber defense unit to secure networks related to defense and military infrastructures. In addition, a 2007 decree by the Ministry of Communication and Information Technology tasked Indonesia's Security Incident Response Team of the Internet Infrastructure/Coordination Center with a wide range of cybersecurity functions, including advising on major cyber threats, improving national cyber defense (especially in critical infrastructure), and supporting law enforcement with regard to cybercrime.

The ASPI report on cyber maturity in 2014 finds that the Government is aware of cyber threats but it cites a scattered and ineffective response. The Ministry of Communications and Information and the Ministry of Defense jointly address cyber policy and security. The Communications Ministry had plans to develop a national cybersecurity body that brings together all cyber stakeholders in the Indonesian Government, but it is unclear whether those plans have been implemented. Similarly, the Ministry of Defense has created the Cyber Defense Operations Centre to have responsibility for national cybersecurity policy and network defense.

A December 2014 reports cite discussions of a national body to fight cyber-attacks. The Cyber National Body (Badan Cyber Nasional in Bahasa, or BCN) subsequently established in 2015. The Government recognizes how complex and dangerous cyber threats can be to the economy, particularly the security of national data that is still sectoral and uncoordinated according to the Minister of Politics, Law and Security. The need for a robust security strategy to support the growth of ICT as well as the protection of privacy in the telecommunications, energy, aviation and banking industries is recognized.

Cyber-related policy opportunities and challenges for further consideration:

Greater connectivity in the region could raise the probability of transnational crime and cross-border cyber-related incidents. With increasing access to high-speed networks, low-level cybercrime has already risen in the ASEAN region. In Asia, policy experts further suggest that the growth of cybercrime could increase instability. Misappropriation of responsibility could lead to misunderstandings and the possible escalation in tensions or conflict because the accurate identification of those responsible for a cyber incident is not always easy (especially since there are a wide range of threats that may come from different non-state actors).

Politically motivated attacks in the recent past appear limited to hacktivism. Indonesia is also very susceptible to cybercrimes, which is indicative of the level of ICT development. The DAKA report found that information security awareness in Indonesia is limited and it finds the legal foundation for cybersecurity is weak.

It finds that if there is a national threat, the Ministry of Communication and Information Technology (KOMINFO) is the lead organization regarding civil cybersecurity while threats that concern national security also involve the Ministry of Defense. ID-SIRTII monitors and provides an early warning system of threats and takes measures to counter them. It also offers educational activities to improve handling of security incidents. In 2013, it supported the Ministry of Defense in preparing a Military CSIRT. The objective of Gov-CSIRT is to work with a range of stakeholders to improve information security for its government members by providing them with a platform for sharing of information and incident handling.

Given the importance of oil and gas in Indonesia, it should closely consider possible cyber threats to oil and gas suppliers. Particularly since global major oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. This could possibly cause damage but breaches may also cause damage to corporate assets, public infrastructure and safety. Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain. Indonesia should therefore closely monitor cyber issues relevant to oil and gas security as well as the supply chain.

If the Government builds nuclear plants to fulfill its future energy demands, the IAEA (as well as several nation states) provides guidance for consideration by states, competent authorities, and operators. The aim is to prevent the theft of material or sabotage of plants and facilities.

If the role of the private sector in the energy supply chain is to continue increasing in the economy, specific public-private sector considerations relating to cybersecurity and the energy sector should be examined. Of note, the DAKA Advisory report finds that there are lingering questions surrounding the effectiveness of public-private partnerships for civilian cybersecurity response. They have not worked optimally according to interviewees in the report because there is a gap in security understanding between the public and private sectors. Nevertheless, all participants agree on the importance of taking a multi-stakeholder approach to cybersecurity. The Government realizes the private sector owns or operates many critical infrastructures and the local companies recognize the need for cooperation.

Capacity building related to cybersecurity issues specifically in the energy sector should not solely focus on technical capacity building but also include policy as well as legislative, organizational, and law enforcement training. In addition, external offers of capacity building should also be coordinated and reflect the unique needs of Indonesia.

For example, in 2013, DAKA's report highlights that the Bandung Institute of Technology in cooperation with the Korean International Cooperation Agency (KOICA) built Indonesia's first cybersecurity center, which includes research and graduate education. Similarly, the report notes weak legislation, an educational deficit, and a shortage of technical talent. The report also recommends that executives and policy-makers should consider the lessons learned elsewhere.

Regarding international efforts, the ASPI cyber maturity report of 2014 finds, for instance, that Indonesia is active in bilateral and multilateral cyber forums, including in ASEAN-led initiatives. It is also active in cybercrime and cybersecurity information exchanges with key partners and through membership in the ITU-IMPACT program. It was a member of the 2013 UNGGE. It has also reached out to international partners to improve its own internal governance and capabilities, most notably by signing a memorandum of understanding with Japan's National Institute of Information and Communications Technology for cooperation in the ICT field. The Government is also reportedly undertaking cybersecurity cooperation programs with Estonia and others.

At the regional level, Indonesia is a member of ASEAN. Critical infrastructure protection will be essential, particularly in consideration of ASEAN plans. Indonesia is a participant at the ASEAN Regional Forum (ARF).

6.7.5 Future Cybersecurity Nexus

There is insufficient data on this topic for Indonesia. This is a potential area of future growth for the economy.

6.7.6 Smart Grids

Given the developing interest in the smart grid and pilot projects, enhancing cybersecurity is essential and should be part of a larger smart grid deployment strategy.

6.8 Japan

6.8.1 Economy Energy Resources

The 2014 APEC Energy Overview Study provides an extensive outline of the energy sector in Japan. The report finds that since indigenous energy resources are modest, Japan imports nearly all of its fossil fuels to sustain economic activity. The aim of Japan's energy policy is to achieve the '3E' goals—energy security, economic growth and environmental protection (for example, against global warming)—in an integrated manner.

6.8.2 Smart Grid Initiatives

Smart grid initiatives in Japan are in their early stages, but are picking up momentum with various initiatives started and large-scale deployment just a few years away. For example, Tokyo Electric Power Company (TEPCO) intends to finish the deployment of 27 million smart meters by 2020. Three types of communication units are mounted in the smart meter including wireless

multi-hop, power line communications (PLC), and mobile. Japan's other utilities aim to roll out their smart meter initiatives by 2024.

Smart grid issues are under the direction of the Ministry of Economy, Trade and Industry (METI). In 2010, METI established the New Energy and Industrial Technology Development Organization (NEDO) as a public management organization to undertake development of new technologies dealing with energy and energy-conservation. METI and NEDO created the Smart Grid Community Alliance, a public-private partnership that created four working groups to develop international strategies, international standardization, a roadmap, and a smart house information infrastructure.

Since 2008, the Japanese Government has supported an "Eco-Model Cities" program to develop next generation energy infrastructure using low carbon technology. The program is piloting various systems in a handful of cities, including Kansai Science City (Electric Vehicles and Photovoltaic installations in homes), Kitakyushu City (real-time energy management of homes and commercial buildings), Yokohama City (real-time energy management systems for homes and buildings, which integrate PV installation and EVs), and Toyota City (demand response solutions and electric vehicles).

A study prepared by SAIC in 2011 provides an overview of smart grid initiatives in Japan. It finds that smart grid drivers in Japan include renewable integration, environmental goals, demand management controls, electric vehicle integration, and financial incentives. According to the study, smart grid activities are centralized and considered to be at the core of Japan's national strategy. This strategy focuses on connectivity, energy efficiency, and the integration of renewable resources into the grid, as well as concerns regarding sustainability and reduction of carbon emissions.

Unlike most other economies, the report finds that reliability is not an issue in Japan. The economy has undertaken significant generation and transmission infrastructure improvements because of investments of more than $100 billion beginning in the 1990s. A key focus area for Japan is the introduction of advanced integrated controls for DSM and connectivity to the end-use customer, known as the "last mile." The last mile is the final link or leg in connecting the end user to the grid or communications provider. Japan is also focused on integration of intermittent energy sources (particularly solar) and sustainability with the goal of moving toward becoming a low-carbon emission society. It has begun establishing standards for smart grid applications. One such standard is the Association of Radio Industries and Businesses ARIB STD-T96 protocol, which is specified for the automatic transmission and measurement of data from remote sources by low-power radio equipment.

Key Projects/Programs delineated by the study include:

- METI Smart Grid Trial: In 2010, METI announced a large-scale five-year $1.1 billion smart grid trial project to take place in four cities and focus on grid-scale energy storage, plug-in hybrid electric vehicles and vehicle to grid connections, smart homes and networks, and the integration of renewable such as solar power into the grid while maintaining grid reliability. The four project cities are:

    - Kyoto Keihanna District (Kansai Science City) where PV systems and fuel cells were installed on 1,000 residential units, grid connected to test load management systems, electric vehicle car sharing programs, and an incentive plan for the use of green energy "Kyoto-eco points" was tested. The Kansai Research Institute oversees the project, which has a target of reducing CO2 emissions by 20 percent in the residential sector and by 30 percent in the transportation sector from 2005 levels by 2030.

    - Yokohama Smart City Project: 4,000 homes was equipped with smart meters using Home Energy Management Systems (HEMS) and Building Energy Management Systems (BEMS) to automatically adjust the amount of electricity supplied to each home, while monitoring electricity usage throughout the project. In addition, 27 MW of solar generation was installed, and 2,000 electric vehicles deployed. The project has a target of reducing CO2 emissions by 30 percent from 2004 levels by 2025.

    - Toyota City Project introduced 3,100 electric vehicles in the city to test grid-to- vehicle and vehicle-to-grid connectivity. DSM applications focused on using heat and unused energy were tested at 70 residential locations. The project has a target of reducing CO2 emissions by 20 percent in the residential sector and by 40 percent in the transportation sector by 2025.

    - Kitakyushu City Project deployed energy management equipment using HEMS and BEMS capable of real-time management at 70 commercial and 200 residential locations. The energy system coordinated DSM with the overall power system and reduce CO2 emissions by 50 percent from the 2005 level by 2030 and 80 percent by 2050.

- Energy Storage Initiatives: It is likely that Japan has more stationary energy storage installed than any other economy in the world. The development of sodium sulfur (NAS) and lithium ion batteries has enjoyed government and large industrial support, and led to deployment at a number of facilities in Japan and other economies, including the United States and Australia.

In addition, Japanese companies have also developed smart grid projects abroad. For example, by May 2011, NEDO selected six Japanese companies to work with U.S. project partners to develop and install smart grid technologies on Maui, Hawaii as part of the Hawaiian Electric Company's Maui Smart Grid Project. The aim was to improve integration of renewable energy resources and prepare the electric system for widespread electric vehicle use. NEDO has also entered into an agreement with Málaga, Spain to implement the Smart Community System Demonstration Project, focused on establishing electric vehicle infrastructure in the city.

The study finds that because Japan's electricity grid is already considered reliable, Japan's smart grid activities are quite focused. Key objectives of the smart grid in Japan include advanced integrated controls to facilitate demand response and prepare for the integration of large amounts of renewables, such as PV.

A Global Smart Grid Federation Report (GSGF) in 2012 outlines that Japanese policymakers were already seriously considering implementing demand-side controls, smart meter infrastructure, flexible pricing structures, and diversified electricity sources and retail options for consumers. Some argue that this has helped lead to efforts to deregulate the electricity industry and introduce greater competition to the benefit of consumers.

As consumer empowerment in the power system gained momentum as a political cause after the Fukushima nuclear disaster, the Government adopted smart metering as a tool to improve demand side management. A publicly traded company, Tokyo Electric Power Co. (TEPCO) is the largest of the ten power companies. In early 2012, at the Government's instigation, TEPCO announced its intention to commence a smart meter rollout in its service territory in the fall of 2013. This is the first massive deployment of smart meters in Japan.

The report also notes the role of the Japan Smart Community Alliance, which is an organization that represents a cross-section of views from industry, the public sector, and academia. It is an important forum for discussion and cooperation on matters concerning the smart grid, including the development of global standards for smart grid technologies. The projects profiled below represent a sample of leading-edge activities undertaken by the membership. They are indicative of the early Japanese activity and interest in the smart grid:

1) Ad hoc communication technology: Organization Kit Carson Electric Cooperative; Supplier Fujitsu; Scale 2100 Smart Meters; Type Advanced Metering Infrastructure. This project provided the foundation for Fujitsu's smart meter business.

2) Hachinohe microgrid demonstration project: Organizations NEDO (New Energy and Industrial Technology Development Organization) • Hachinohe-city; Suppliers Mitsubishi Electric Corporation and Mitsubishi Research Institute Inc.; Type Microgrid. This project in Aomori tested the performance of a demand-supply control system in managing the impact of renewable energy on a commercial power grid with real end users (605kW demand) for an electrical island. The project successfully

conducted one-week of islanded operations relying on 100 percent renewable energy. Total Energy Solutions test bed Project: Organization Singapore Government; Supplier Panasonic Corporation; Type Multiple Technologies. In a two-year project that began in August 2011, Panasonic provided total energy solutions tailored to a building to enable local energy generation for consumption in the building's common facilities. Rooftop photovoltaic systems and lithium-ion batteries combined to create and store energy. Demand Response was implemented by combining smart meters with a Home Energy Management System (HEMS). Each household had an in-home display (IHD) so that the user could view how much electricity, water, or gas is being used. Demand response was achieved through Smart Energy Gateway (SEG) which connects the smart meter and home appliances, such as air-conditioners.

3) Distribution Stabilizing Solution: Organization NEDO; Suppliers Hitachi and CRIEPI (Central Research Institute of Electric Power Industry); Type Distribution Management System. The goal of this project was to maintain voltage stability and power quality in the face of distributed renewable energy integration. The project equipment simulated photovoltaic generation and electricity consumption in-house and on the distribution network (2004-2007).

4) Mass introduction of EVs and energy management system using EVs as parts of Yokohama Smart City Project: In addition to the cities participating in the Government's EcoModel Cities program, there are other smart grid projects of note. In Yokohama City, participated in the Eco-Model Cities program, a consortium of industry players (Nissan, Toshiba, Panasonic, Meidensha Corporation and others) developed smart city programs. One of Nissan related program to introduced 2000 EVs by the end of FY2014 into the city.

5) Miyako Island mega solar demonstration research facility: Organization: The Okinawa Electric Power Company; Supplier Toshiba Corp. This was a pilot project conducted in Okinawa by The Okinawa Electric Company and Toshiba to test the integration of large-scale renewable energy sources into the power system and study the impact of photovoltaic power generation facilities and rechargeable batteries on power system stabilization. The pilot commenced operation in 2010 for a four-year testing period.

The Federation of Electric Power Companies of Japan is developing by 2020 a smart grid that incorporates solar power generation with government investment of over USD 100 million. The Japanese Government has announced a national smart metering initiative and large utilities have announced smart grid programmers. It has developed an initial standards roadmap for smart grids and the Smart Community Alliance has extended the concept of smart grids beyond the electric system to encompass energy efficiency and efficient management of other resources, such as water, gas and transportation. Media outlets in 2014 report that Mitsubishi Electric has

implemented a smart grid experiment at three sites in Japan. The objective of this experiment is to operate a real system in the field, to log data and validate fundamental technologies.

In 2015, online reports further note that Japan's plan for liberalizing the electricity sector puts smart meters as a vital sensor at the heart of the smart grid. Under the Japanese model, advanced metering units act as a conduit between the A route - everything that happens before electricity enters a home, - and the B route, where energy demand is controlled within the customer's environment through a home energy management system. Smart meters are seen as playing an essential role in helping players further upstream to correct imbalances between supply and demand by reporting data in 30 minute intervals with a 60-minute lag. The economy expected to install 70 million smart electricity meters by the end of the national rollout. Meters are being made by consortia of Japanese and Chinese Taipei manufacturers supplying the metering module, and Japanese and Japanese-subsidiary companies such as Toshiba's Landis+Gyr providing the communication module.

These reports state that the failure of the Daiichi nuclear power plant in Fukushima in 2011 prompted the Government to adopt reform of the power system to ensure a future stable supply at lower costs to customers through market liberalization. The economy will start the reform program in 2016 and will complete the full unbundling of the electricity system by 2020. In addition, the fact that Tokyo will host the Olympic Games in 2020 means that there is an urgency to install smart grid infrastructure within the next five years. The economy's largest utility TEPCO declared they would have 27 million smart meters in the field by 2020. However, there seems still to be some disconnect between what utilities are officially saying and what is happening on the ground. Another question is whether Japan's utilities had cracked the connectivity issue. Officially, they have according to the online articles and two of the technology providers for major rollouts - Toshiba and Mitsubishi Electric - both confirmed they are using a golden triangle of communication methods - cellular for rural areas, wireless 920MHz radio frequency for urban areas and PLC for households in high-rise buildings.

Under the Japanese smart grid model, energy demand from the customer side is managed by variations of energy management systems to control and reduce demand, from communities (CEMS) to buildings (BEMS) and households (HEMS). These types of systems manage what Japan defines as the B route, anything that happens after the smart meter. Utilities, which are supplying the system hardware, are adopting both automated and customer-led reduction in energy usage. The report further notes that the Japanese utility model faces a potential threat from electricity deregulation opening the door to new power producers and suppliers. In September 2013, the economy had 106 registered PPS companies. In January 2015, it had 526 companies, with 40 signing up to be electricity retailers in the previous month. Industry insiders spoke about a large number of these new entrants coming from the telecommunication sector, bringing with them expertise at customer engagement.

Japan is a member of the GSGF and ISGAN.

6.8.3 Current Cybersecurity Nexus

Since completion of this report, Japan has undertaken several additional actions to develop standards and protect its critical energy infrastructure from cyber threats. Ongoing work includes:

- The Ministry of Economy, Trade and Industry is developing standards for smart grid components. Tokyo Gas, Osaka Gas, and Toho Gas are developing a communication standard for the remote reading of meters. It is likely that this technology will be the same for water and electric meters.
- Japan created a "Study Group on International Standardization for Next Generation Energy Systems." The study group released a roadmap in January 2010, which identified 26 focus areas in the system of systems. Through a public-private partnership, Japan Smart Community Association, Japan's stakeholders are active in IEC, IEEE, SGIP, and other international standardizing activities.[7]
- Japan has begun establishing standards for smart grid applications, including the Association of Radio Industries and Businesses ARIB STD-T96 protocol, which is specified for the automatic transmission and measurement of data from remote sources by low-power radio equipment
- The Home Energy management systems standard communications protocol includes ECHONET Lite and SEP.
- The Yokohama City project will use SCADA, HEMS, BEMS, and EV data centers for demand response.

Defining critical infrastructure protection

Under the New America study, which delineates key terms related to existing cybersecurity and information security definitions, citations made for critical infrastructure and Japan include:

Critical Infrastructure:
"Critical infrastructures are formed by business entities providing highly irreplaceable services and are essential for people's social lives and economic activities. If its function is suspended, reduced or unavailable, peoples social lives and economic activities will be greatly disrupted, and the same below."

According to the Information Security Policy Council Second Action Plan on Information Security Measures for Critical Infrastructures (p. 10), the Japan National Information Security Center categorizes critical infrastructure into 10 sectors: data communication, finance, airlines,

[7] ARCAM

railway, electric power, gas, government and administrative services (including municipal governments), medical, water service and logistics.

The 2013 Information Security Policy Council (ISPC) cybersecurity strategy specifically outlines the roles of critical infrastructure providers. It specifies that “any impairment or disruption of the functions of "critical infrastructure," which is the basis of people’s social lives and economic activities formed by businesses that provide services which are extremely difficult to be substituted by others, due to cyber-attacks and others, has the potential to cause serious damages the lives of people and so on.”

In particular, the strategy mentions that, for this reason, presently, Japan requires initiatives for "critical infrastructure providers" in the 10 sectors of information and communications, finance, aviation, railways, electricity, gas, government and administrative services (including local public authorities), medical services, water and logistics, in accordance with measures in government institutions and others. It specifies that it is “necessary to even further strengthen measures at these and other providers in hereafter. In addition, there are fields which have not been considered critical infrastructure within Japan up until now, but for which any impediment or disruption of the information systems for the relevant services (and so on) has the potential to have a major effect on the lives of people and socioeconomic activities. Specifically these include smart cities and smart towns, ITS and other transportation control systems and other new network type systems, as well as the defense industry and energy related industries, which are considered critical infrastructures in the United States.”

The ISPC issued “The Basic Policy of Critical Information Infrastructure Protection (3rd Edition)” in May 2014. This policy is described as a shared basic policy with the Government, which bears responsibility for the protection of the CII, and CII providers that independently carry out relevant protective measures. It was established to serve as the basis for the policy related to information security measures for Japan's critical infrastructure, such as the enactment of the "Special Action Plan on Cyber-terrorism Countermeasures for Critical Infrastructure" (concluded in the December 2000 Information Security Measure Promotion Meeting), prior to the establishment of NISC. After the establishment of the NISC, in 2005, the "First Action Plan on Information Security Measures for Critical Information Infrastructures" based on the “Basic Orientation for Countermeasures Necessary for Protecting Critical Infrastructure from IT Outages and Ensuring Business Continuity of Critical Infrastructure Providers". Based on the First Action Plan, the stakeholders including the Government and 10 CII sectors undertook relevant measures to reduce IT outages at CII to as close to zero as possible. The “Second Action Plan on Information Security Measures for Critical Information Infrastructure" was established in 2009. It identified policies to be implemented based on the basic measures for CIIP and the public-private information-sharing framework established by the First Action Plan.

The Second Action Plan has taken over the measures of "maintenance and promotion of the safety principles", "enhancement of information sharing", "common threat analysis" and "cross-sectoral exercises" from the First Action Plan and also identified policies for "response to environmental changes" in order to appropriately address the ever-changing social and technological environment. The 2014 policy document explains relevant measures are implemented steadily based on five policies such as establishing a robust information sharing system. As such, it reflects the lessons learned through the assessment of a group of policies identified in the Second Action Plan while taking into account the 2013 Cybersecurity Strategy.

In addition, it takes into account the lessons learned from the experience of dealing with system outages and data loss during the Great East Japan Earthquake. It also reflects responses to the ever-changing social and technological environment and the trends of increasingly sophisticated and complex cyber-attacks carried out in recent years.

In order to continuously provide CII services and to avoid serious effects on the public welfare and socioeconomic activities from IT outages resulting from natural disasters, cyber-attacks or other causes, all stakeholders are to protect CII by reducing the risk of IT outages as much as possible and by ensuring prompt recovery from IT outages.

Basic Principles for CIIP are:

- CII operators should implement measures for CIIP on their own responsibility. In addition, a sense of security should be nurtured among the public and social development, resilience and international competitiveness should be promoted through cooperative activities between Government and private sectors.
- The CII operators should respectively take measures and make effort for continuous improvement of those measures as entities providing services and bearing social responsibilities.
- Government organizations should provide necessary support for CII operators' activities for CIIP.
- Each CII operator should cooperate and coordinate with other stakeholders due to the limit of each operator’s individual information security measures to address various threats.

The policy document further notes that during the process of compiling the policy, deliberation was carried out on the scope of CII, which is currently composed of 10 sectors identified in the Second Action Plan. Further study occurred to determine whether new sectors should be added in the list of CII.

As a result, in this Basic Policy, the CII sectors now include 13 sectors: "information and communication services", "financial services", "aviation services", "railway services", "electric power supply services", "gas supply services", "government and administrative services

(including municipal government)", "medical services", "water services", "logistics services", "chemical industries", "credit card services" and "petroleum industries".

Defining cybersecurity

The 2013 Information Security Policy Council cybersecurity strategy establishes the National Information Security Center (NISC) in the Cabinet Secretariat and the Information Security Policy Council (ISPC) in the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters) to strengthen measures for information security issues. The ISPC was responsible for the "First National Strategy on Information Security" (2006), the "Second National Strategy on Information Security" (2009) and the "Information Security Strategy for Protecting the Nation", to improve the level of information security within Japan while balancing the free flow of information and dealing with risks.

The latest strategy was named the "Cybersecurity Strategy" in order to make clear the necessity to promote measures widely related to cyberspace as distinguished from the efforts for assuring "information security".

Under the New America compilation of terms and definitions, the following key terms related to existing cybersecurity and information security definitions are delineated for Japan:

- Cyber Space: "Cyberspace," global virtual spaces such as the internet, composed of information systems, information communications networks and similar systems and which circulate large quantities of a large variety of information, have rapidly expanded and begun permeating real-space.
- Cyberspace: A global domain comprised of information systems, telecommunications networks and others, provides a foundation for social, economic, military and other activities.
- Cyber Security: Japan aims to construct a "world-leading," "resilient" and "vigorous" cyberspace, and incorporate this cyberspace as a social system to realize a "cybersecurity nation" as a society that is strong against cyber-attacks, full of innovations and of which its people will be proud.
- Information Security: The role of an information security is to make the IT infrastructure truly dependable and solid within the framework of Japanese national objectives, as a major economic power; specifically, to maintain continuous development, to achieve better lives for the people through the use and utilization of IT, and to ensure national security from a new perspective.

It specifically defines information security as “To make the IT infrastructure as to be truly reliable and rigid” by: 1) sustainable development through the use of IT, 2) achievement higher

quality of life of people through the use of IT, and 3) security against the threats related to the use of IT.

According to the ITU country report for Japan, legislation pertaining to cybercrime includes the Unauthorized Computer Access Law 2000. Legislation and regulation related to cybersecurity has been enacted through the following instruments: Electronically Recorded Monetary Claims Act; Telecommunications Business Law; Act on Regulation of Transmission of Specified Electronic Mail; Act on the Protection of Personal Information; Law Concerning Electronic Signatures and Certification Business; and Basic Act on the Formation of an Advanced Information and Telecommunications Network Society.

There are two National CSIRTs in Japan; NISC in charge of the Government network and JPCERT/CC in charge of the private sector network. Japan has 27 members of FIRST, and JPCERT/CC is the key Computer Security Incident Response Team (CSIRT) in the economy. JPCERT/CC helped to form, and provides secretariat functions for, APCERT and regularly engages with CERTs in the larger Asia–Pacific region.

The ITU factsheet explains that Japan has an approved national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through the Technical Standards for Information Security Measures for Central Government Computer Systems (April 2012). The Management Standards for Information Security Measures for the Central Government Computer Systems is the framework for certification and accreditation of national agencies and public sector professionals. Japan has an Information Security Research and Development Strategy for cybersecurity standards, best practices and guidelines. Training programs for raising awareness with the public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors include: Information Security Human Resource Development Program; NISC Information Security Awareness Month; Information Security Outreach and Awareness Program; and JPCERT/CC. The METI Cybersecurity Information Sharing Partnership Japan (J-CSIP) serve as frameworks for sharing cybersecurity assets between agencies. The officially recognized body for information sharing between the public and private sector is (JPCERT/CC) which shares information with domestic vendors particularly the private sector. J-CSIP is also responsible for sharing cybersecurity assets between the public and private sector.

6.8.4 Cybersecurity Challenges (Issues)

Japan is working to increase communication between government and industry as it relates to securing critical energy infrastructure from cyber-attacks. This section identifies the current and planned cybersecurity-energy nexus in Japan.

The 2013 national cybersecurity strategy established the NISC as the command post for information security policy, to carry out the planning, proposal and general coordination related

to planning of basic strategy and other centralized/cross-cutting promotion of information security measures for the public and private sectors. The ISCP, established for centralized/cross-cutting promotion of information security measures for the public and private sectors, works towards improving the level of information security and strengthening ability to deal with cyber-attacks for government institutions and critical infrastructure providers. It states that since the establishment of information security policy through the First Strategy, certain goals realized include the strengthening of measures for security and crisis management, the implementation of "accident assumed society" measures, and appropriate handling of new environmental changes.

It further notes that the information security environment changes extremely quickly, and that in the three years since the previous strategy, risks have become increasingly serious, more diffuse and more globalized. "Cyber-attacks" against government institutions and critical infrastructures have become a reality and have become both "national security" and "crisis management" issues. At present, the introduction of the best possible measures for protecting the government institutions and critical infrastructures has become essential. The strategy continues by noting, “we are entering an age, where everything is connected to the internet, called the Internet of Things. This is an age where everything faces information security risks. Risks are also increasing even for control systems which are not connected to the Internet”. It notes that information security has become an issue directly linked to the "stability of people's daily lives" and "economic development".

According to the strategy, Japan is constructing the "world's most advanced IT nation", and the world's most advanced IT nation must realize a "safe cyberspace".

Specifically, it highlights that in the future, the propagation of SDN in telecommunications infrastructure, ITS in transportation infrastructure and smart grids in power infrastructure will result in a variety of social infrastructure always being connected to networks, and managed and controlled by software. There is potential for cyber-attacks targeting vulnerabilities in the software of these systems to directly result in obstruction of communications, transportation disorder, blackouts and other large scale social turmoil and possibly even deaths. A footnote mentions a trend of increasing numbers of incidents each year with SCADA, which carries out system monitoring and control via computers and other types of industrial control systems. Reports of information security incidents resulting in damage both in Japan and overseas are included in the IPA "Report on Critical Infrastructure Control System Security and IT Service Continuance" (March, 2009) and the Ministry of Economy, Trade and Industry "Cyber Security and Economy Research Committee Interim Report".

In particular, it highlights under a section on “more severe risks” that risks which are a threat to national security as well as the lives, bodies, properties and other interests of people. The actualization of threats of targeted attacks is thought to be aimed at the theft of technological and

confidential information from Japanese Government institutions, the defense industry, critical infrastructure providers, research institutions and other entities.

The strategy includes enhancing a risk-based approach. Up until now, Japan has pursued a policy of having each individual actor, including government institutions, critical infrastructure providers, businesses and individuals, exert maximum efforts to each handle their own information security to elevate their capabilities to deal with all cyberspace threats to the highest level in the world.

In these conditions, it finds that it is necessary each individual actor carry out the measures, while also "dynamically implementing and handling with appropriate and timely allocation of resources as a social mechanism for responding to ever-changing risks". Actions such as improving the recognition and analysis functions for incidents related to cyber-attacks, integrating these functions, advancing threat analysis capabilities by promoting information sharing, strengthening cooperation between CSIRT for each actor and among international CSIRTs are all identified as critical, and "it is necessary to strengthen a risk-based approach based on the characteristics of the risks through dynamically responding capabilities brought about by these actions".

The Japan Self-Defense Force (JSDF) Command, Control, Communications and Computer Systems Command is charged with the development of national cyber defense capabilities. Under the command, the JSDF established a Cyber Defense Unit. The defense force is seen as having the necessary structures in place for cyber operations. The JSDF is working to improve its capability, especially through cooperation with the United States, but a shortage of qualified personnel, an inability to respond to attacks, weak capabilities and problems in information sharing within the force remain areas of concern according to ASPI.

The 2013 UNIDIR cyber index report notes that in October 2011, because of attacks on Mitsubishi and other Japanese corporations, METI established the Japan Cyber Security Information Sharing Partnership to facilitate information sharing among manufacturers of core technology and various public and private cybersecurity organizations.

The 2013 national security strategy delineates in the section on "Global Security Environment and Challenges" and "Risks to Global Commons" that "Cyberspace, a global domain comprised of information systems, telecommunications networks and others, provides a foundation for social, economic, military and other activities. Meanwhile, risks of cyber-attacks with the intent to steal classified information, disrupt critical infrastructure, and obstruct military systems are becoming more serious." In Japan, with an increasing level of connecting networks of social systems and various other elements, cyberspace is necessary for promoting both economic growth and innovation through the free flow of information in cyberspace. Protecting cyberspace from the above-mentioned risks is vital to secure national security.

It notes that Japan as a whole will make concerted efforts in comprehensively promoting cross-cutting measures to defend cyberspace and strengthen the response capability against cyber-attacks, so as to protect cyberspace from malicious activities threatening cybersecurity; to ensure the free and safe use of cyberspace; and to guard its critical infrastructure against cyber-attacks, including those in which state involvement is suspected. To this end, Japan will strengthen public-private partnership in the areas of system design, development and operations based on risk assessment, as well as identifying incidents, minimizing damages and their expansion, and analyzing the causes of and preventing similar incidents. In addition, Japan will comprehensively consider and take necessary measures with regard to expanding the pool of human resources in the security field, protection of control systems, and response to the issues of supply chain risk.

Furthermore, Japan will strengthen inter-agency cooperation and define the roles of relevant agencies so that it can reinforce its capability to protect cyberspace and respond to incidents as a nation. At the same time, Japan will promote a range of measures, including enhancing the ability and function to oversee, assess, apprehend, analyse, and internationally coordinate on cyber incidents, as well as reinforcing relevant agencies in charge of those tasks. In promoting these measures, strengthening international partnership in a wide range of areas is essential. For this, Japan will take measures at technical and operational levels to enhance international cooperation. Japan will also strengthen information sharing and promote cyber defence cooperation with relevant economies.

ASPI's report finds that Japan is a highly engaged and capable actor in cyberspace, and the Government has clearly demonstrated its intentions to be proactive on cyber issues, especially by publishing its Cybersecurity Strategy in 2013 and having instituted a wide range of legislation. Japan has some significant challenges to overcome however, primarily at the intra-governmental level, but it has shown clear determination to address these issues. Japan has developed a solid organizational structure for government cyber efforts centered on NISC and the ISPC. NISC secures national security and emergency response systems and drafting standards, recommendations and reports on cyber issues. The Chief Cabinet Secretary chairs the ISPC, which handles cyber policy and works with the NISC and the Government Security Operation Coordination Team to ensure the implementation of policies at the ministerial and agency levels. National Government cyber efforts have benefited from continuity of personnel. The National Police Agency guides cybercrime efforts, while the Japan Self-Defense Force established its Command, Control, Communications, and Computer Systems Command in 2008. However, the report finds that despite a strong organizational structure and wide breadth of cyber efforts, a lack of intergovernmental coordination and fragmentation in government operations has limited Japan's effectiveness. It has demonstrated a clear understanding of its vulnerabilities in cyberspace and what needs to be done to address them. The 2013 Cybersecurity Strategy focuses on building cyber resilience and provides a solid foundation for future cyber efforts. The issue of collective defense as it applies to cyberspace is a serious area of concern for Japan, as

interpretations of its constitutional limitations on the use of force has confused the range of options available to respond to cyber-attacks.

In particular, the report concludes that Japan has a relatively strong cyber relationship with critical infrastructure owners and operators that was set to grow under the 2013 strategy. Japan has a mature understanding and good awareness of private industry cyber risks, as is laid out in the 2013 Cybersecurity Strategy. The Japanese Cyber Security Information Sharing Partnership facilitates information sharing between and among manufacturers and government. Under the strategy, NISC will further efforts for 'organic collaboration' within government institutions and with critical infrastructure providers. In April 2013, Japan launched a cyber team to help companies recover from cyber-attacks.

The 2014 "Basic Policy of Critical Information Infrastructure Protection (3rd Edition)" has specific details outlined for critical infrastructure protection such as the purpose of CII protection, the basic principles for CIIP, stakeholder responsibility, and responsibility of CII operators' executives and senior managers.

Cyber-related policy opportunities and challenges for further consideration:

There still is a challenge in accurately attributing responsibility for a cyber incident. Misappropriation could lead to misunderstanding or an escalation in tensions. This is especially challenging when cybercrime levels are on the increase in the Asia region.

Given the economy's use of nuclear energy, it should continue to monitor closely the nexus between cybersecurity and this sector. The IAEA (as well as several other nation states), for instance, provide guidance for consideration by states, competent authorities, and operators. The aim is to prevent the theft of material or sabotage of plants and facilities.

Regarding multilateral efforts, the UNIDIR 2013 cyber index report notes that in June 2011, Japan and the United States announced a bilateral strategic policy dialogue on cybersecurity issues. The ASPI cyber maturity report in 2014 finds that Japan is heavily engaged regionally and internationally on cyber issues and continues to be a global leader in the digital economy. It is highly engaged with the international community on cyber issues and has a published International Strategy on Cyber Security. As a signatory to the Budapest Convention and a member of the UNGGE, Japan is very engaged in bilateral and multilateral efforts.

In particular, the 2013 International Strategy on Cybersecurity Cooperation delineates that cyberspace has become a driver for social and economic growth due to its openness and availability to all actors. Excessive administration and regulation of cyberspace diminishes the benefits of cyberspace and could impede social and economic growth. Therefore, it is imperative to ensure openness and interoperability of cyberspace without excessively administering or regulating it and to maintain and develop safe and reliable cyberspace in which free flow of

information is ensured. This will ensure freedom of expression and vibrant economic activities in cyberspace, facilitate innovation, economic growth and solutions for social issues and provide positive benefits, which economies around the world can enjoy.

It specifies that as cyber threats are growing in severity, existing measures and initiatives are no longer sufficient to respond to these widespread and globalized risks. Therefore, in addition to existing measures and initiatives, it suggests there should be a new mechanism based on enhanced international cooperation in order to address appropriately the risks associated with the revolution in information and communication technology.

It specifies that rather than absolute prevention "a more realistic approach to cyber threats is to assume that certain risks will occur and trigger incidents, but to work toward a rapid recovery from such incident and to prevent any further damage from it through timely and appropriate allocation of resources and international cooperation." Therefore, one of the most urgent needs for the international community is to establish a mechanism to implement a risk-based approach, whereby risks are quickly and appropriately identified as they evolve and responses are dynamic. All stakeholders in the global cyberspace need to cooperate and assist each other while fulfilling the responsibilities corresponding to their respective roles in the society.

Priority areas include the implementation of dynamic responses to cyber incidents. In implementing the risk-based approach premised on the possibility of cyber incidents, response needs to be prompt and global, and must minimize the impact of the incident while addressing the ever-changing risks. It further outlines that it is critical that each economy has "fundamentals," that is, sufficient basic capacity and response mechanisms to respond dynamically to cyber incidents through international cooperation and mutual assistance. Moreover, considering the global nature of cyberspace, raising the cybersecurity standard at the global level and reducing the number of vulnerable nodes in the realm of cyberspace are essential. Such efforts should also have a consequential deterrent effect on malicious activities carried out in cyberspace.

Drawing on its experience, Japan is providing support for establishing CSIRTs and developing their operational capacity. Japan is also sharing information on measures for cleaning bots, detecting malicious sites, dealing with malware, and on information sharing mechanisms for cybersecurity of critical infrastructure. Japan is also sharing what it describes as "these outstanding cybersecurity measures" when providing support for building of critical infrastructure systems. In addition, when building a framework for cyber hygiene activities, indicators, by which actual cyber-attacks and cybersecurity initiatives in each economy can be quantitatively assessed, are important. Japan is actively contributing to initiatives by the OECD and other organizations for the formulation and measurement of such indicators.

At regional level, it notes that Japan's relationship with ASEAN is particularly important given its existing close ties and increased investment by Japanese enterprises in ASEAN member

states. ASEAN and Japan have cooperated in ongoing initiatives through the ASEAN-Japan Information Security Policy Meeting, as well as the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation. Japan is promoting initiatives such as capacity building for human resources development and for the creation of frameworks for information sharing and critical infrastructure protection. Japan is also a participant at the ASEAN Regional Forum (ARF).

Moreover, Japan is promoting cooperation on cybersecurity technology with ASEAN by promoting the JASPER (Japan-ASEAN Security PartnERship) Project that combines the PRACTICE Project with warnings to computers infected with malware. In addition, under the TSUBAME Project, by cooperating with CSIRTs within the Asia region and installing sensors in CSIRTs, trends of cyber attacks within the Asia region are identified at an early stage and warning and response measures are taken quickly.

Japan-U.S. Security Arrangement is noted as of essential importance for Japan. The two economies have built a cooperative relationship to promote various efforts in the areas of policy consultation, information sharing and cyber incident response through such platforms as the Japan-U.S. Cyber Dialogue and the Japan-U.S. Policy Cooperation Dialogue on the Internet Economy. Japan will continue to deepen this partnership.

Japan is participating in the fourth UN GGE (2014/2015), the fourth Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

6.8.5 Future Cybersecurity Nexus

There is insufficient data on this topic for Japan. This is a potential area of growth for the economy in future cybersecurity nexus.

6.8.6 Smart Grids

Japan has a very clear strategic interest in the smart grid and its strategies outline the link between smart grids and the need to enhance cybersecurity. This must be considered as part of any larger smart grid deployment strategy.

Online reports highlight, for instance, that the blackouts that followed the failure of the Fukushima Daiichi nuclear energy plant plus the threat of future natural disasters is a reason why consumers would invest in home energy storage systems. Many of the HEMS systems also rely on having stored energy from renewable sources as a way to balance the demand/supply needs of the grid.

6.9 Republic of Korea

6.9.1 Economy Energy Resources

The 2014 APEC Energy Overview Study provides an extensive outline of the energy sector in Korea. The report finds that Korea has few indigenous energy resources. It has no oil resources, only 326 million tons of recoverable coal reserves and 3 billion cubic meters of natural gas. To sustain its high level of economic growth, it imports large quantities of energy products.

6.9.2 Smart Grid Initiatives

In 2011, Korea passed the Smart Grid Promotion Act, which provides a framework for sustainable smart grid projects with industry participation. It included a plan for smart grid development, deployment, and commercialization. The Korean Agency for Technology Standards manages the act that also includes the development of a national interoperability standards framework and promotion of international standards activities. The Government is very active in smart grid activities, domestically and internationally. The Government is looking to install smart meters to half of all households by 2016, with the remaining installations scheduled by 2020. Korea has announced plans to implement smart grids nationwide by 2030.

The Government launched a USD 65 million pilot program on Jeju Island in partnership with industry. The Jeju Smart Grid Test-bed is Korea's flagship program. The pilot consists of a fully integrated smart grid system for 6,000 households, wind farms and four distribution lines. Through a public-private partnership, the island of Jeju serves as an ambitious smart grid complex. It has become one of the world's largest smart grid communities, testing advanced smart grid technologies and performing R&D, as well as the development of business models.

The Korea Smart Grid Institute (KSGI) is responsible for managing the Government's Smart Grid Roadmap, and smart grid test-bed, as well as providing policy support for smart grid issues. KGSI is implementing ten Power IT projects aimed at enhancing the power grid system through transmission monitoring, distribution system enhancements, and integration of distributed generation.

The GSGF report of 2012 provides an overview of its main findings related to the smart grid initiatives in Korea.

It finds that because innovating (and exporting) green technology is a pillar of Korean economic strategy, the Government is very active in smart meter / smart grid activities, both domestically and internationally. It has implemented pilot deployments of smart meters and has planned for a broader rollout. In 2011, the Smart Grid Promotion Act (2010) provides a framework for sustainable smart grid projects and a plan for smart grid development, deployment and commercialization. In addition, Korea was designated as a lead economy in smart grid at the Major Economies Forum on Energy and Climate held as part of the July 2009 G8 Summit. The

report finds that what is striking about the Korean example is the level of coordination and support between Government and industry in achieving the objective of economic growth based on green innovation. It finds that the Korea Smart Grid Association plays a critical role as a mediator between government and private-sector stakeholders on the smart grid. It helps develop smart grid projects, conducts standardization work, and engages in important R&D.

Notable projects outlined by the report include:

- Jeju Smart Grid System Demonstration Complex: Organizations KEPCO, Samsung, SDI; Suppliers Secui.com, Hyosung; Demonstration Project; Type Multiple Technologies. The Jeju Smart Grid Demonstration Complex reflects the massive scale of government and industry investment and high level of cooperation in the smart grid space. With funding from the Government and the private sector, together with a host of other companies, KEPCO is responsible for undertaking this smart grid demonstration project on Jeju Island which incorporates distributed renewable generation (wind and solar), distributed automation, a distribution management system, EV infrastructure, advanced metering infrastructure, energy storage, and network monitoring and telemetry. The first phase of the project is complete. In the first phase, the consortium constructed electric vehicle charging stations and installed solar panel rooftops on residences as well as in-home energy storage systems, in-home displays, smart appliances, and/or smart meters. Jeju Island presents a unique opportunity to test smart grid technologies. Notably, the Government and private sector jointly financed this project with the government contributing a little less than a third of total project costs.

- Smart Transportation: Organizations SK Innovation, SK Telecom, Hyundai Heavy Industries, Renault Samsung Motors; Suppliers SK Innovation, SK Telecom, SK Networks, Hyundai Heavy Industries, Renault Samsung Motors, CT&T, DH Holdings ILJIN Electric, EN Tech, KODI-S; Scale 12 consortiums approximately 600 households, 72 EVs, 89 charging stations, 9 home (3 kWh) and building (150 kWh) storage units, and 1 wind power energy storage system; Type Electric Vehicles. In this project, which began in 2009, the project team integrated an electric vehicle infrastructure into the power system and incorporated fast and smart battery chargers, GPS-based charging spots, and emergency information and services. The infrastructure relies on wireless communications. As part of the project, the team developed battery energy storage systems (BESS) for buildings and wind power. The Total Operating Centre (network operating center) conducted data management for the EV infrastructure in the Jeju Smart Grid System Demonstration Complex. This project finished in 2013, with the hope of furthering the consortium's understanding of smart charging and vehicle-to-grid applications.

- Renewable Energy Source Operating System: Organization POSCO ICT; Suppliers LG Chem, Woojin Industrial System, Daekyung Engineering, Korea Institute of Energy Research, Research Institute of Industrial Science & Technology, Chungbuk University, Jeju University; Scale 2 wind generators (750kW), Energy Storage System 2MVA/500kWh, Lead-Acid Energy Storage System 275kW/137.5kWh; Type Distributed Renewable Generation and Network Monitoring & Telemetry. This is a demonstration of a microgrid system that incorporates large-volume wind generation, intelligent output stabilization for this generation, and high volume BESS (2MVA) and various other battery technologies (Li-ion, lead-acid, EDLD, redox flow). It looked at piloting a microgrid system that can operate independently as well as interconnect with other grids.

- Consumer Participating Smart Place: Organization KEPCO; Suppliers Samsung SDI, Hyosung, Omni-system, AID, Rootech, ABB, Secui.com, Millinet, Samsung Electronics; Scale 600 households; Type Consumer Engagement, Demand Response, Advanced Metering Infrastructure, Energy Storage, Electric Vehicles, and Distributed Renewable Generation. The smart grid green place project outfits houses and buildings with integrated energy management services to manage better their energy use. Real-time electricity rates were introduced, and renewable generation sources and energy storage solutions installed at residences together with in-home displays to monitor energy usage. To allow for comparing electricity use across households, smart appliances and EVs were also introduced. The project team also looked at the development of regulations, which could manage the electricity market created by the demonstration project. Electric car chargers, power storage facilities, and photovoltaic systems were built.

The website of the Korea Smart Grid Institute (KSGI) explains that in 2010, Korea took a significant step forward as a player in the global smart grid sector. It is working with the State of Illinois in the United States to jointly develop and test technologies for smart grid for the facility on Jeju Island. Under the plan, technologies that are developed through this partnership and deemed viable for commercialization were to be rolled out both in Illinois as well as in Korean cities. The two sides agreed to launch a business model for the smart grid on Jeju Island and apply it in Seoul and Chicago. The Korea Electrotechnology Research Institute and other related local centers came together with U.S. DOE's Argonne National Laboratory and Chicago University to test and develop technologies.

KSGI launched in 2009 as the secretariat of the Smart Grid Initiative and projects in Korea. The Smart Grid Initiative mainly targets the modernization of electric power systems. Then President Lee Myung-Bak announced Korea's new national vision "Green Growth, Low Carbon" in 2008. KSGI is to implement this vision KSGI by managing the Government's smart grid roadmap;

operating a smart grid test-bed, pilot city; and extending other policy support for smart grid related issues. The First Stage took place from 2010-2012 and the Second Stage is from 2012 to 2020.

This role includes:

1. Reinforcement of Planning Research: a) analyze social and economic cost effects of the building of smart grids; b) conduct qualitative/quantitative data analysis on energy and environment issues; c) identify current status and trends of smart grid projects in Korea and around the world; and d) make proposals on security, standardization, and authentication regarding the roll-out of smart grids.
2. Continuous management of the Korean smart grid roadmap: a) reorganize the roadmap planning committee composed of experts from the domestic industry, academia, and research institutes and hold a regular meeting to make up the existing roadmap; and b) map out in great detail, and implement the roadmap on such issues as technology, legal/institutional systems, standards, and security.
3. Integrate Operation of the smart grid test bed: a) set up a standing task force team (TFT) that serves as the secretarial of the test bed steering committee to supervise the operational progress of the test bed; and b) create working groups to coordinate affairs among providers and gather their views.
4. Smart Grid R&D Project Management: a) evaluate the progress and annual performance of projects; and b) rearrange a HR pool by sector to evaluate performance and enhance people's expertise.
5. In-home Display (IHD) Distribution Project: a) select distribution companies, complete the distribution plan and develop the distribution management system; and b) upgrade a modem and develop a BPL/ZigBee gateway.
6. International Cooperation & Exports: a) build and operate a private-level partnership network with other economies that intend to build a smart grid; Participate in overseas, regional meetings pertaining to the smart grid; b) support Korean companies' entry into overseas smart grid markets; and c) support international cooperation and the development of export tools.

KSGI outlines five sectors for the roadmap:

1) Smart Power Grid: Open power grids will be built to allow various kinds of interconnections between consumption and supply sources. The roll-out of such networks will pave the way for new business models, and the building of a power grid malfunction and automatic recovery system that will ensure a reliable and high quality power supply.
2) Smart Consumer: It aims to encourage consumers to save energy by using real-time information and producing smart home appliances that operate in response to electric utility rates.

3) Smart Transportation: It aims to build a nationwide charging infrastructure that will allow electric vehicles to be charged anywhere. It also establishes a V2G (Vehicle to Grid) system where the batteries of electric vehicles are charged during off-peak times while the resale of surplus electricity takes place during peak times.
4) Smart Renewable: It aims to build a smart renewable energy power generation complex across the nation by rolling out microgrids. This will ultimately lead to the emergence of houses, buildings, and villages, which can achieve energy self-sufficiency through the deployment of small-scale renewable energy generation units in every end-user premise.
5) Smart Electricity Service: With the launch of a variety of energy-saving electricity rate plans, this service aims to improve consumers' right-to-choose by satisfying their different needs. In addition, it wants to deliver a wide array of added electricity services through the marriage of electricity and ICT, and to put in place real-time electricity trading system for the transactions of electricity and derivatives.

Power IT refers to a technology that enables electric power devices and systems to become digital, environmentally friendly, and intelligent through the convergence of electric power technology and ICT. It also creates high added value for electric power services. Korea's Power IT National Program aims to develop Power IT into a driving force behind the nation's economic growth by advancing the Korean electric power and electrical industries. The program also seeks to bring innovation and higher added value to electric power services. To achieve these goals, Korea embarked on a strategic technology development program in 2005 and selected 10 projects, which have since been systematically implemented. In 2009, the implementation of these projects was connected with the Smart Grid Initiative, a core element of Seoul's Green Growth Strategy. The Power IT Program was to help develop the electric power and electrical industries as these two industries play a critical role in propelling national economic growth and delivering innovative and high value-added electric power services. (The ten projects are listed on the KSGI website and were completed in 2012).

The KSGI site further highlights that in 2009, the Leaders of the Major Economies Forum on Energy and Climate (MEF), representing the 17 largest economies of the world, launched the Global Partnership for Low-Carbon and Climate-Friendly Technologies. As an initial step, they requested a set of plans, which now span ten climate-related technologies that together address more than 80 percent of the energy sector carbon dioxide (CO2) emissions reduction potential identified by the IEA. Korea along with Italy led on the smart grid plan.

The "Vision for Accelerated Deployment of Smart Grid under the Global Partnership" is laid out on the KSGI site. It states that MEF leaders should play an active role in overcoming common barriers faced by many economies. Global partnership and collaboration opportunities should be maximized in order to accelerate effective smart grid deployment. Smart grid is a very complex set of solutions and outcomes based on the specific economy and regional drivers, objectives, and benefits wrapped around a diversified spectrum of technologies and applications; therefore,

defining smart grid specific performance-based goals is very complicated and unrealistic. To achieve transformational gains in smart grid deployment, MEF members need to establish a level of measure for smart grid. It then recommends short- and long-term actions to consider, which are fully outlined on the KSGI website. This project became the basis of ISGAN.

Future plans in Korea are outlined. Korea has recognized the necessity of rolling out a smart grid as infrastructure for the low carbon, green industry in preparation for its binding reductions of greenhouse gas emissions. The Government is therefore implementing relevant policies and projects "that can be echoed by the public". In order to implement the smart grid by 2030, the plan is divided into three stages. The first stage is 'the construction and operation of the Smart Grid Test-bed' to test relevant technologies. The second stage is 'the expansion into metropolitan areas' to add intelligence on the part of consumers. The last stage is 'the completion of a nationwide Smart Grid' for all of the intelligent grid networks.

Korea is a member of the GSGF. It became an ISGAN vice-chair in 2011 and hosted the secretariat.

6.9.3 Current Cybersecurity Nexus

Defining critical infrastructure protection

The 2011 National Cyber Security Master Plan, under its section of "Major Imperatives", specifically delineates "Improving the level of security for critical information and facilities" by: a) expanding secret management system and upgrading encryption system to protect confidential information; b) strengthening security measures for information and communications systems in critical infrastructures such as electric power stations and transportation facilities; c) establishing immediate checking system comprising related organizations; d) tightening up security measures and defining clear responsibilities when outsourcing; and e) making it mandatory to establish a system that diagnoses vulnerabilities.

In 2005, there was recognition of a "deepening information system dependency. National infrastructure control systems tend to be connected to the internet. We can predict a paralysis of critical infrastructures from an internet attack" (National Security Research Institute on "Protection of Critical Information Infrastructure in Korea").

In 2009, an inventory study on CIIP in various countries found that the critical information and communication infrastructure plays a crucial role in providing public safety and stable services that are essential for everyday life. In Korea, the following sectors are counted among the critical infrastructures that are heavily dependent on information and telecommunication technologies: E-Government and National Government Administration; National Security; Emergency/Disaster Recovery Services; National Defense; Media Service, e.g., Broadcasting Facilities; Financial Service; Gas and Energy, e.g., Power Plants; and Transportation, e.g., Subways and Airports; and Telecommunication.

Defining cybersecurity

Under the New America compilation of terms and definitions, the following key terms related to existing cybersecurity and information security definitions are delineated for Korea:

Cyber Terrorism: Various forms of cyber terrorism: Hacking, DDoS attacks, denials of service, logic bombs, Trojan horses, Worm viruses, HERF guns etc.

According to the ITU country report for Korea, legislation on cybercrime has been enacted through the Criminal Act (Art. 316(2), Art. 366, Art, 314(2), Art. 347(2), Art. 227(2), Art. 323(2), Art. 140(3), Art 141(1); Act on Promotion of Information and Communications Network Utilization and Information Protection; Personal Information Protection Act; and the Act on the Protection of Information and communications Infrastructure. Legislation and regulation related to cybersecurity has been enacted through the Act on Promotion of Information and Communications Network Utilization and Information Protection; Personal Information Protection Act; and Use and Protection of Credit Information Act - Electronic Financial Transactions Act. The Information Security Management system (ISMS) is the officially approved national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards.

The Korea Internet Security Agency (KISA) provides cybersecurity frameworks in order to foster professionals equipped with information security technology and practical abilities, national qualification. Also SIS (Specialist for Information Security), a private accreditation organization, added promotion of national technical qualifications (information security engineer/ industrial information security engineer) to its work in 2013. KISA has signed MOUs or has partnerships with the: Office of Cybersecurity and Information Assurance (OCSIA UK); Israel National Cyber Bureau (INCB); Microsoft; CERT Australia; CERT Romania (CERT-RO); JP CERT; CN CERT; and the Cybersecurity Institute (STS) of Kazakhstan. The Information Communication Infrastructure Protection Committee is part of the Ministry of Science, ICT and Future Planning, which aims to coordinate policies on critical ICT infrastructure and improve protection of critical ICT infrastructure. Korea has a Private – Public – Military Joint Response Team created by the Ministry of Science, ICT and Future Planning for decision-making on cyber threats, situation monitoring, analyzing of threats and joint investigation.

6.9.4 Cybersecurity Challenges (Issues)

- Geographic differences, legacy issues, regional needs, and consumer education.
- A key challenge is encouraging domestic regulators to know what is going on at the international level, and understand how these standards can be used.

This section identifies the current and planned cybersecurity-energy nexus in Korea.

The 2011 National Cyber Security Master Plan has five action plans that include: 1) establishing a joint response system of private, public and military sectors; 2) strengthening the security of critical infrastructure and enhancing secrets protection; 3) detecting and blocking cyber-attacks at the national level; 4) establishing deterrence through international cooperation; and 5) building cybersecurity infrastructure.

UNIDIR's cyber index report in 2013 notes that in Korea, cyberspace is considered an operational domain, such as land, air, and sea, which needs a state level defense system. The 2011 national strategy for cybersecurity focused on defense, i.e., prevention and detection of, and response to cyber-attack. The National Cyber Security Center is responsible for identifying, preventing, and responding to cyber-attack. It works with the private and military sectors to prevent cyber-attacks, analyses vulnerabilities, and coordinate cyber emergency response activities. The 2008 defense white paper identified cybersecurity as an essential component of national defense. The 2010 white paper outlines cyber-attacks as one of several non-traditional security threats. CERTs at the corps level will oversee the Defense Information Systems. The Ministry of National Defense established the Cyber War Centre in January 2010. Its primary aim is to increase the security of government and financial information networks. The Ministry of National Defense has also created an independent Cyber Warfare Command responsible for defensive and offensive operations in cyberspace. According to the Korea Communications Commission, the National Intelligence Service will play the lead role in cyber issues. The Commission, along with the Ministries of National Defense and Government Administration and Home Affairs, will be tasked respectively with private sector security, national defense, and protecting the safety of the Government's computer systems. The Korea Advanced Institute of Science and Technology established the Cyber Security Research Center, which has assisted in detecting and defending against cyber-attack.

ASPI's report on cyber maturity in the Asia Pacific states that Korea is a leading technological actor in cyberspace and has some of the world's most advanced digital infrastructure. As evidenced by clear governmental organization and a body of legislation on cyber issues, the Government is highly aware of and responsive to all cyber issue areas. It has a highly capable military and advanced digital economy. However, in defining cyberspace primarily as an operational domain, the economy's overemphasis on security comes at the expense of cybercrime and international cyber governance.

The report further explains that Korea has a strong catalogue of cyber legislation and regulation, along with an active critical infrastructure cyber policy. Legislation provides the Government with wide legal flexibility to act in cyberspace, which has led to some international concern about content-control activities. It has strong legislation and robust interaction with critical infrastructure operators.

Korea has seven members of FIRST. The two leading national CERTs are KrCERT/CC, which falls under the purview of the Korea Internet and Security Agency (KISA), and KNCERT/CC, which is part of the National Intelligence Service. KrCERT/CC is an operational member of APCERT and focuses on the private sector, including broadcasting, telecommunications and ICT. Korea has a capable military cyber capacity. The Defense Information Warfare Response Center of the Defense Security Command protects military networks, while the Cyber Command unit handles wider online security. Korea has both defensive and offensive capabilities and in February 2014 announced its intention to develop offensive cyber capabilities. A new Cyber Defense Department launched in May 2014. The new command, to be established under the Joint Chiefs of Staff, will have responsibility for all cyber-warfare missions. It will also include an oversight committee and a whistleblower program.

The report finds that the Government has a very mature relationship with the business sector. KISA oversees the security of private-sector networks. The National Cyber Security Center works with the military and public and private sectors to coordinate information-sharing partnerships, prevent cyber-attacks and coordinate cyber emergency responses.

The 2011 National Cyber Security Masterplan specifies that the national cyber threat joint response team, which began operating in January 2012, comprised of private, public and military sectors under the National Cyber Security Center (NCSC) is to strengthen cooperative ties such as cyber threat information sharing among participating organizations.

It established roles among relevant organizations such as the National Intelligence Service (overall control in times of peace and crisis), Korea Communications Commission (supervision over broadcasting and communications) and Ministry of Public Administration and Security (MOPAS, e-government service to the public, National Computing and Information Agency [NCIA] operating under MOPAS, and support for cybersecurity activities of local governments).

The 2012 Defense White Paper outlines that in response to threats, the military is strengthening its defense of key national facilities in close cooperation with the civil, government, and police authorities. Furthermore, in response to cyber threats and other forms of terrorism, the military is sharing intelligence with relevant agencies. In addition, anticipated threats of provocation such as terrorism against key national facilities and cyber-attacks have been simulated to support the planning efforts to respond effectively to these threats, and training activities to respond with available assets in an integrated and strengthened manner against these threats. In particular, there are integrated protection trainings at key facilities carried out to achieve an integrated civilian-government-military-police defense posture led by local government heads.

The Defense White Paper explains that the recent security environment is seeing an increase in transnational and non-military threats such as terrorism, cyber-attacks and natural disasters, and these threats, if carried out, will not be manageable by a single agency of a government or a single nation. It finds that it is imperative for the military to establish resolute response measures

to counter these threats and the military is building its response capabilities and posture by strengthening not only the whole-of-government cooperation system but also coordination with the international community to prepare against these newly emerging threats.

The MND recognizes cyberspace as an area analogous to territory, territorial waters, and airspace that the nation must protect, and is pursuing the revision of relevant rules and regulations, and the establishment of systems and doctrines to be able to carry out cyber warfare at the national level. CERTs, established in all units above corps level, will monitor the defense information system 24 hours a day and to enable prompt responses. In addition, the MND Information Protection Team expanded and reorganized as the Cyber Defense Policy Team in 2012 to actively respond to increasing cyber threats and reinforce policy functions for cyber warfare. The MND with the Ministry of Knowledge and Economy is making efforts to secure cyber expert personnel by setting up cyber defense departments in civilian universities and recruiting service members with specialty in information protection.

The MND is reinforcing its information protection system to secure the execution of peacetime and wartime operations from various cyber threats such as hacking and computer viruses. In order to respond promptly to cyber threats, the MND maintains a civilian-government-military coordination system and hosts the annual Defense Information Protection Seminar to share knowledge in cyber-attacks and defense expertise.

Cyber-related policy opportunities and challenges for further consideration:

Regarding geopolitical considerations and perceived threats, the 2012 Defense White Paper describes its understanding of the security landscape by explaining that challenges that pose threats to the economy's national security are likely to further increase. While the issues of territorial sovereignty, religion, natural resources, and ethnicity are constant sources of potential regional disputes, non-military and transnational threats such as terrorism and cyber-attacks are increasing. Although Northeast Asia is emerging as the political and economic center of the world in the 21st century, there are tensions in the region.

Under its section on "International Security Threats", it then notes that although the threat of a large-scale war has diminished since the end of the Cold War, traditional sources of conflict such as territorial disputes, competition for natural resources, religious and ethnic conflicts, and separatist and irredentist movements persist, posing a serious threat to global security. Advancements in IT are leading to various forms of cyber terrorism whose resultant damage is rapidly increasing in magnitude. Cyber-attacks are emerging as a new security threat as the entities that carry them out become more organized, targeting key national information networks.

Since it can often be difficult to attribute accurately responsibility for a cyber incident, misappropriation could lead to misunderstanding or an escalation in tensions, particularly in such

an environment. In addition, this is especially challenging when non-state actors could be to blame and contemporary cybercrime levels are on the increase in the Asia region.

Given the economy's use of nuclear energy, it should closely monitor the nexus between cybersecurity and this sector. The IAEA (as well as several nations), for instance, provide guidance for consideration by states, competent authorities, and operators. The aim is to prevent the theft of material or sabotage of plants and facilities.

Regarding international efforts, the ASPI report on cyber maturity finds that Korea has highlighted strengthening international cyber cooperation since its 2011 Cyber Strategy and played host to the 2013 Seoul Conference on Cyberspace. Despite numerous bilateral and multilateral initiatives, Korea's engagement remains somewhat disjointed, with a tendency to focus on security issues over wider cyber issues, such as internet governance.

The Defense White Paper specifies that international cooperation and exchange of information are becoming increasingly important to respond to transnational cyber threats. The MND concluded the 'Memorandum of Understanding on Information Assurance and Computer Network Defense' with the U.S. Department of Defense in 2009, to enhance cooperation between the ROK and the United States in responding against cyber threats and by adopting the 'Terms of Reference of the ROK-U.S. Information Assurance Working Group,' which facilitates the goal of enhanced information sharing in the realm of information. Assurance and Computer Network Defense, has been taking part in the ROK-U.S. Information Assurance Working Group Meeting since 2010. The MND also participates in the International Cyber Defense Workshop hosted by the U.S. Department of Defense twice a year since 2009, to exchange information on cyber warfare and cooperate on information protection technologies. The U.S.-ROK Cyber Policy Consultations, launched as a "whole-of-government" approach, acknowledged that effective bilateral cooperation on cyber-security would require increased cooperation between defense agencies and coordination with the private sector.

Korea is a participant in the ASEAN Regional Forum (ARF).

The "Seoul Framework for and Commitment to Open and Secure Cyberspace" of 2013 outlined that in the preparatory stage of the Seoul Conference on Cyberspace 2013 and the Conference itself, several elements were identified for an open and secure cyberspace. Those elements relevant to the cyber-energy nexus include:

- Governments, business, organizations and individual owners and users of information technologies (cyberspace) must assume responsibility for and take steps to enhance the security of the information technologies. States and relevant regional and international organizations that have developed strategies to deal with cyber security and the protection of critical information infrastructures are encouraged to share their practices

and measures that could assist other Member States in their efforts to facilitate the achievement of cyber security.

- The security of critical information infrastructures is a responsibility Governments must address systematically and an area in which they must lead nationally, in coordination with relevant stakeholders, who in turn must be aware of relevant risks, preventive measures and effective responses in a manner appropriate to their respective roles.
- Capacity Building: States need to enhance efforts to close the digital divide in order to achieve universal access to information and communications technologies and to protect critical information infrastructures by facilitating the transfer of information technology and capacity-building to developing economies, especially the least developed economies, in the areas of cyber security best practices and training."
- Capacity building is of vital importance to an effective cooperative global effort on securing ICTs and their use. Some States may require assistance in their efforts to: improve the security of critical ICT infrastructure; develop technical skill and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridge the divide in the security of ICTs and their use.

Korea participated in the fourth UN GGE (2014/2015), the fourth Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

6.9.5 Future Cybersecurity Nexus

There is insufficient data on this topic for Korea. This is a potential area of future growth for the economy.

6.9.6 Smart Grids

Korea has a very clear strategic interest in the smart grid. However, cybersecurity must be considered as part of any larger smart grid deployment strategy.

For instance, the 2012 GSGF report noted that the Government was actively collaborating with the U.S. Government on energy development, smart grid standard development and on cybersecurity and grid trustworthiness projects, skills training and development, and smart building initiatives. It further found that there had been no notable public reaction to the Government's smart metering or smart grid initiatives. Smart meters and the smart grid do not have much profile with the general population, and electricity tariffs are not highly politicized according to the report. KSGI material outlines that Article 5 of the Act on Promoting SG Establishment and Usage notes the need for development of a professional workforce for the smart grid, for protection and safety of information, and for policy improvement.

6.10 Malaysia

6.10.1 Economy Energy Sectors

According to the 2014 APEC Energy Overview Study, Malaysia is well endowed with conventional energy resources such as oil, gas and coal, as well as renewable energy sources such as hydro, biomass and solar energy.

6.10.2 Current Cybersecurity Nexus

Defining critical infrastructure protection

The CyberSecurity Malaysia CNII Portal is a "portal in which the members of critical infrastructure work together by sharing information on security issues which affect critical infrastructure".

It defines Critical National Information Infrastructure (CNII) as those assets (real and virtual), systems and functions that are vital to the nations so that their incapacity or destruction would have a devastating impact on:

- National economic strength; confidence that the nation's key growth area can successfully compete in global market while maintaining favorable standards of living.
- National image; projection of national image towards enhancing stature and sphere of influence.
- National defense and security; guarantee sovereignty and independence whilst maintaining internal security.
- Government capability to function; maintain order to perform and deliver minimum essential public services.
- Public health and safety; delivering and managing optimal health care to the citizen.

The CNII Sectors identified are: National Defense and Security; Banking and Finance; Information and Communications; Energy; Transportation; Water; Health Services; Government; Emergency Services; and Food and Agriculture.

Defining cybersecurity

The CNII CyberSecurity Malaysia site explains that the National Cyber Security Policy (NCSP) has been designed to facilitate Malaysia's move towards a knowledge-based economy. The Policy was formulated based on a National Cyber Security Framework that comprises legislation and regulatory, technology, public-private cooperation, institutional, and international aspects.

There are eight "thrusts" in NCSP:

THRUST 1: Effective Governance

- Centralize coordination of national cyber security initiatives.
- Promote effective cooperation between public and private sectors.
- Establish formal and encourage informal information sharing exchanges.

THRUST 2: Legislative & Regulatory Framework

- Review and enhance Malaysia's cyber laws to address the dynamic nature of cybersecurity threats.
- Establish progressive capacity building programmers for national law enforcement agencies.
- Ensure that all applicable local legislation is complementary to and in harmony with international laws, treaties and conventions.

THRUST 3: Cyber Security Technology Framework

- Develop a national cyber security technology framework that specifies cyber security requirement controls and baselines for CNII elements.
- Implement an evaluation/certification program for cybersecurity products and systems.

THRUST 4: Culture of Security and Capacity Building

- Develop, foster and maintain a national culture of security.
- Standardize and coordinate cybersecurity awareness and education programmers across all elements of the CNII.
- Establish an effective mechanism for cybersecurity knowledge dissemination at the national level.
- Identify minimum requirements and qualifications for information security professionals.

THRUST 5: Research & Development Towards Self-Reliance

- Formalize the coordination and prioritization of cybersecurity R&D activities.
- Enlarge and strengthen the cybersecurity research community.
- Promote the development and commercialization of intellectual properties, technologies and innovations through focused R&D.
- Nurture the growth of cybersecurity industry.

THRUST 6: Compliance and Enforcement

- Standardize cybersecurity systems across all elements of the CNII.
- Strengthen the monitoring and enforcement of standards.
- Develop a standard cybersecurity risk assessment framework.

THRUST 7: Cyber Security Emergency Readiness

- Strengthen the national CERTs.
- Develop effective cybersecurity incident reporting mechanisms.
- Encourage all elements of the CNII to monitor cybersecurity events.
- Develop a standard business continuity management framework.
- Disseminate vulnerability advisories and threat warnings in a timely manner.
- Encourage all elements of the CNII to perform periodic vulnerability assessment programmers.

THRUST 8: International Cooperation

- Encourage active participation in all relevant international cybersecurity bodies, panels and multinational agencies.
- Promote active participation in all relevant international cybersecurity events, conferences and forums.
- Enhance the strategic position of Malaysia in the field of cybersecurity by hosting an annual international cybersecurity conference.

The National Cyber Security Coordination Committee (NC3) is to:

- Define, communicate and update (when necessary) the national cybersecurity programs to all Critical National Information Infrastructure (CNII).
- To coordinate the national cybersecurity initiatives of various key agencies and organizations.
- To coordinate information security awareness, training and education programs to increase the competency of information security professionals and the industry as a whole at the national level.
- To coordinate the implementation of cybersecurity programmes (in accordance with NCSP).

According to the 2015 ITU country report, specific legislation on cybercrime has been enacted through the following instruments: Communications and Multimedia Act 1998 [Act 588]; Computer Crime Act 1997 [Act 563]; Personal Data Protection Act 2010 [Act 709]; Penal Code [Act 574]; Copyright Act 1987; Digital Signature Act 1997[Act 562]; Financial Services Act 2013; and Electronic Commerce Act 2006 [Act 658]. Specific legislation and regulations related to cybersecurity have been enacted through the following instruments: Communications and Multimedia Act 1998; Financial Services Act 2013; and Digital Signature Act 1997.

Malaysia's officially recognized national CIRT (MyCERT) is operated by Cybersecurity Malaysia. It also has a Government CERT (GCERT), which coordinates knowledge sharing, and exchange programs among MyCERT, ISPs and enforcement agencies. MyCERT is an agency of

the Ministry of Science, Technology and Innovation and is active in APCERT and the Organization of Islamic Cooperation CERT. Malaysia is home to two members of FIRST. MyCERT operates a computer security incident response hotline ('Cyber999') and runs the CyberSecurity Malaysia Malware Research Centre. MyCERT also holds technical workshops throughout Asia and in the Middle East.

The factsheet further outlines that Malaysia has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the following instruments: National Cybersecurity Policy (NCSP); National Security Council directive No. 24 "Arahan 24"; and The Cabinet's Decision in 2010 -Arahan Keselamatan under Chief Government Security Office (CGSO). The Ministry of Communications and Multimedia (KKMM) and the Ministry of Science, Technology and Innovation (MOSTI) monitor and coordinate the implementation of national cybersecurity strategy, policy and roadmap by respective agencies. Malaysia has officially recognized national benchmarking for the national cyber crisis management plan. It has conducted exercises such as the Malaysian Incident Handling Drill. Cybersecurity Malaysia coordinated the first National Cyber Crisis Exercise Cyber Drill code-named X-Maya in collaboration with the National Security Council in 2008. Standards Malaysia is the national standards body and the national accreditation body.

The Malaysian Communications and Multimedia Commission provides various types of awareness programs, industry talks, conferences, training programs and workshops on cybersecurity, for the general public as well as for public and private sector employees.

Malaysia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Malaysia participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014). It participated in the following cybersecurity activities: ASEAN-JAPAN Information Security -APT Cybersecurity Forum; Meridian Conference; Octopus Conference (Cooperation against cybercrime); and JTC 1/SC 27 Meeting.

6.10.3 Cybersecurity Challenges (Issues)

According to the APEC Energy Overview 2014, Malaysia's National Energy Policy, first formulated in 1979, consisted of three principal energy objectives:

- The Supply Objective: To ensure the provision of an adequate, secure and cost-effective supply of energy;
- The Utilization Objective: To promote efficient utilization of energy and to discourage wasteful and non-productive patterns of energy consumption; and
- The Environmental Objective: To minimize the negative impacts of energy production, transportation, conversion, utilization and consumption on the environment.

These three principal objectives are instrumental in the development of Malaysia's energy sector. Subsequent policies are designed to support these objectives and their implementation.

NCSP seeks to address the risks to the Critical National Information Infrastructure (CNII), which comprises the networked information systems of ten critical sectors (listed above) that include the energy sector. MOSTI explains that Malaysia's Critical National Information Infrastructure will be secure, resilient and self-reliant. It explains that the Government must adopt an integrated approach to protect these infrastructures from cyber threats. The NCSP recognizes the critical and interdependent nature of the CNII and aims to develop and establish a comprehensive program and a series of frameworks that will ensure the effectiveness of cybersecurity controls over vital assets. It was developed to ensure that the CNII are protected to a level commensurate to the risks faced. The Malaysia Cyber Security Centre is a one-stop coordination center for national cybersecurity initiatives by adopting a coordinated and focused approach. The center is under the purview of MOSTI, and overseen by the National IT Council for policy direction and the National Security Council in times of national crisis.

The key functions of the Malaysia Cyber Security Center are: NCSP implementation; defines, communicates and updates (when necessary) the national cybersecurity programs to all the CNII; national coordination; closely coordinates cybersecurity initiatives of key agencies and organizations; outreach; and promotes and facilities formal and informal mechanisms for information sharing across the CNII. This role includes promoting cybersecurity awareness, training and education programs to grow the competency of information security professionals and the industry; compliance monitoring; facilitates the monitoring of compliance to cybersecurity policies and standards across the CNII; risk assessment; and assesses and identifies cybersecurity threats exploiting vulnerabilities and risks across the CNII.

CyberSecurity Malaysia hosts annual Cyber Crisis Exercises to assess national capabilities to withstand a cyber-attack.

DAKA Advisory outlines that since 2013, CyberSecurity Malaysia has also provided technical assistance and training services for national cyber crisis management, per Order No. 24 of the Dasar dan Mekanisme Pengurusan Krisis Siber Negara (Policy and Mechanism for National Cyber Crisis Management). This means that the agency helps government ministries or other agencies that need technical cybersecurity assistance, including the National Security Council (NSC). They are the national technical arm for the NSC.

According to the 2013 UNIDIR Cyber Index report, the Ministry of Defense implements IT security policy to protect government and business from cyber-attack. Its missions include ensuring the safety of networks and preventing cyber incidents from having harmful economic effects. According to the 2014 ASPI report on cyber maturity in the Asia Pacific region, the Armed Forces have begun to develop capabilities to protect national assets, including from cyber

threats, and the Malaysian Defense Minister has publicly supported the development of an ASEAN master plan for Southeast Asia's cybersecurity.

The ASPI report concludes that Malaysia has a sound organizational cyber architecture but is weighed down by weak cyber legislation. The economy is very active in the technical elements of international cyber diplomacy and is showing increased interest in the policy aspects. The Government is actively building a structure to manage cybersecurity risks in a coordinated manner through the establishment of CyberSecurity Malaysia and an active CNI protection program. CyberSecurity Malaysia has responsibility for emergency response, security capability, capacity development, outreach, risk assessment and cybersecurity evaluation and certification. However, the full implementation of the strategies outlined in the policy still needs to be seen.

Cyber-related policy opportunities and challenges for further consideration:

Greater connectivity in the region could raise the probability of transnational crime and cross-border cyber-related incidents. With increasing access to high-speed networks, low-level cybercrime has already risen in the ASEAN region. In Asia, policy experts further suggest that the growth of cybercrime could increase. Misappropriation of responsibility could lead to misunderstandings and the possible escalation in tensions or conflict because the accurate identification of those responsible for a cyber incident is not always easy (especially since there is now a wide range of varying threats that may also come from different non-state actors).

A report by DAKA Advisory analyzing cyber threats and responses in Malaysia in 2014 explains that advanced economies are subject to politically motivated cyber-attacks as they have entered a new dimension of ICT capabilities. Since Malaysia is still moving up the ICT value chain, the report finds that it is unlikely to be subject to such activities. A Malaysian CIO explains that regardless of what many people think, sophisticated cyber-attacks are not very common and they have seen very few such serious attacks to the organization (an international offshore oil and gas services provider headquartered in Malaysia). Attacks on critical infrastructures are also rare according to the report and usually target economies that are highly dependent on ICTs or have developed a particular military dependence on them. Therefore, although global threats apply equally in Malaysia, some aspects of the economy's digital development make it more vulnerable to certain types of attacks, and these are primarily financially motivated. The primary cybersecurity concern in Malaysia according to the report is cybercrime.

In 2013, MyCERT showed that the majority of reported incidents were fraud related followed by intrusion attempts and malicious codes. Together, the three categories constituted 85 percent of reported incidents.

Given the economy's oil and gas sector, pipelines and plants, Malaysia should consider possible cyber threats to oil and gas suppliers. Particularly since many major global oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. This could

possibly cause damage but breaches may also cause high damage to corporate assets, public infrastructure and safety, or the wider economy. Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain. Malaysia should monitor cyber issues relevant to oil and gas security as well as the supply chain.

Regarding specific public-private sector considerations relating to cybersecurity and the energy sector. The DAKA Advisory report explains that in broad terms, there are two types of companies in Malaysia: GLCs in which the Government holds a controlling stake and or other private sector companies, including small and medium-sized enterprises. A key question raised for cybersecurity is what happens if the economy liberalizes the role of GLCs in critical infrastructures, such as energy. For instance, the 10th Malaysia Plan calls for "rationalizing the role of GLCs in the economy," including increased privatization. The report finds, however, that interviewees were unconcerned about such potential development, as they do not see a difference regarding preparedness between GLCs and others in the private sector.

The DAKA Advisory report finds though that in light of potential liberalization of critical infrastructures, Malaysia would do well to study other economies' experiences with information sharing and public-private collaboration. It identifies as crucial the need to clarify further roles and responsibilities. The DAKA report finds that in theory the roles and responsibilities of public sector agencies in Malaysia are clear. However, in practice there seems to be overlapping organizational interests. Like most economies, Malaysia has a coordination issue among agencies according to the report.

Regarding international cooperation efforts, at the regional level, Malaysia is a member of ASEAN. Malaysia is also a participant in the ASEAN Regional Forum (ARF).

It participated in the fourth UN GGE (2014/2015), the fourth Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Malaysia is highly active in bilateral and multilateral projects through ASEAN and ITU–IMPACT, with a focus on the exchange of technical data and signatures. In March 2014, Malaysia co-chaired an ASEAN Regional Forum workshop with Australia on confidence building measures in cyberspace.

6.10.4 Future Cybersecurity Nexus

There is insufficient data on this topic for Malaysia. This is a potential area of growth for the economy in the future.

6.10.5 Smart Grids

According to the APEC Energy Overview 2014, Malaysia is considering the potential of implementing a smart grid system to minimize losses, reduce costs and increase reliability.

2014 reports online also outline that some emerging economies, such as Thailand, Malaysia, Indonesia, and the Philippines, are making plans to deploy smart grid technology. While this region is currently behind other global regions in terms of smart meter deployments and regulatory frameworks, its smart grid market is growing. There are already smart grid pilot projects in several economies throughout the region. By 2022, Southeast Asian economies will likely have an electricity demand profile similar to Latin American economies where large-scale smart meter deployments already exist. The region's current electricity consumption rates are among the lowest in the world, while distribution loss rates are comparatively moderate, offering less short-term savings potential compared with other global regions. Additionally, regulatory frameworks remain largely undeveloped in the region. Even in the more advanced economies, deployments are still at the initial pilot level.

These 2014 reports say that investment in Southeast Asia will include smart metering and the modernization of electricity transmission and distribution networks with sensors, communications and software. By 2024, the largest markets will be Thailand, Indonesia, Malaysia, the Philippines, and Viet Nam, according to a recent study by Northeast Group LLC. Southeast Asian economies are modernizing their electric infrastructure. Electrification programs and growth in renewable resources will also drive investment.

February 2015 news articles online report that TNB's smart grid technology is currently in its pilot project stage. It hopes to install smart meters in 8.5 million households within 10 years. The Uniten Smart Grid Laboratory launched in February 2015. The Government tasked TNB to lead the economy's smart grid program. However, material online argues that there are still differing views on the value and relevance of the smart grid for Malaysia.

In April 2013, Silver Spring Networks (a networking platform and solutions provider for smart energy networks) announced an agreement with Masers Energy Malaysia. Under the agreement, Silver Spring Networks was due to coordinate smart infrastructure technology, planning and services for Masers' Smart Grid City Melaka and Special Economic Zone Melaka projects. The Masers Energy Smart Grid City and Green Special Economic Zone are an innovative public-private plan to transform the Melaka region from an agricultural and small-industry zone into the first Smart Grid City in Asia.

In April 2014, TNB signed a smart grid technology memorandum of understanding with smart grid platform company Trilliant. The MOU will provide a framework for collaboration between the two companies to exchange technical information and training, and to explore models to deliver smart grid benefits such as enhanced energy efficiency, improved reliability and energy

security. The smart meter project is part of a wider smart grid initiative. It will see the installment of 1,000 smart grid advance meters in the regions of Putrajaya and Malacca during the one-year period of the pilot project.

Given the interest in the smart grid, enhancing cybersecurity is also essential and should be considered as part of a larger smart grid deployment strategy.

6.10 Mexico

6.10.1 Economy Energy Resources

According to the APEC Energy Overview Study published in March 2014, the energy sector is highly important to the Mexican economy. The oil sector in particular is a central component of the economy with oil exports in 2011 comprising 16 percent of the economy's total exports. In 2013, President Nieto promulgated an ambitious constitutional energy reform to strengthen the capacities of Mexico´s National Oil Company and allow the participation of private investment across the entire value chain of the oil and gas industry.

6.10.2 Smart Grid Initiatives

The state power company, the Federal Electricity Commission (CFE), has started to make significant moves into the smart grid sector. CFE has already integrated Elster's EnergyAxis Management System with its customer information and billing systems.

As the Mexican grid system links to the United States across the Rio Grande via high voltage direct current (HVDC) interconnections, it is expected that there will be similar standards in both economies for smart grid technologies.

An October 2014 reports outlines that the "Smart Grid Model of Mexico" is designed for CFE. According to online sources in 2014, CFE launched a tender offer for smart meters, after the energy law passed Parliament in August 2014. CFE expects up to 40 percent savings from the implementation of smart meters. The state-owned utility also put additional bids out in 2015 and 2016. The energy law includes the opening of the electricity market to independent providers. The new law includes the creation of a wholesale electricity market and the creation of an independent grid operator called CENACE. The power generators, retailers and qualified consumers who participate in the wholesale market will be able to enter into electricity purchase and sale transactions, as well as transactions regarding electricity's related services, electric power, import/export of the products, financial transmission rights and clean energies certificates.

Announcements in 2011 outline that CFE selected Elster for Mexico City's First AMI project. The Mexican Secretaria de Energia (SENER) and CFE were to use the EnergyAxis pilot as a benchmark for evaluating the advantages of Elster's smart grid technologies for potential future deployments. CFE had already deployed nine EnergyAxis systems. Elster was the first and only

AMI provider to have received a Certificate of Compliance from CFE, which certifies the integration of EnergyAxis with CFE's enterprise system. CFE used the project to showcase AMI benefits. CFE also expected to leverage its investment in EnergyAxis to provide smart grid enhancements to other gas and water utilities (Elster is a consortium of utility technology providers on the Mexico City smart grid project including the company's distributor partner in Mexico, Tecnologias EOS. Additional consortium members included ENERI and GIMSA).

Reports from 2013 state Mexico's smart grid technology market is expected to grow 25 percent annually for the remainder of the decade. A report by Zpryme claims that opportunities, including forward thinking energy policies designed to raise the economy's international competitiveness, will drive overall growth for Mexico.

Press releases also highlight that CFE selected Silver Spring for the Loss Reduction Projects on Distribution smart grid project in Mexico City's Central District. In partnership with Tecnologias EOS, under the Megacable and Hola Innovacion consortium, Silver Spring was due to deploy a canopy network across various residential and commercial areas of Mexico City and provide connectivity solutions to cabinets which house a group of centralized meters. The Silver Spring solution aimed to reduce electricity theft for residents and businesses, while Technologias EOS will provide remote indoor displays to help customers monitor power usage. This solution was for approximately 140,000 residential and commercial customers within CFE's Central District in Mexico City that serves approximately 2 million customers in total (Silver Spring Networks is a networking platform and solutions provider for smart energy networks).

Overall distribution losses and electricity consumption rates are average for emerging markets but in some cities theft rates are high. According to CFE, nearly 15 percent of its total electricity production in 2013 was lost due to theft or defaults, and in some areas of Mexico City that increases to more than 35 percent. Several other reports mention the growing issue of electricity theft in Latin America.

For example, reports in 2013 explain that Mexico faces problems such as power outages, electrical theft, and poor energy infrastructure. Therefore, smart grid technology is providing an opportunity for Mexico to improve both functionally and economically. Initially, smart grid investment involve AMI and, as these deployments create a foundation for modernization, new growth will be driven by distributed automation and grid scale energy storage.

According to 2013 reports by Northeast Group LLC, Mexico is steadily developing one of the largest smart grid markets in Latin America. Since 2011, Mexico has nearly doubled the number of AMI meters deployed and began to establish clear roadmaps and deployment targets.

Because transmission and distribution while undergoing deregulation are still quite controlled by the state owned utility CFE, CFE will dictate the pace and scale of smart grid deployments in Mexico. By 2023, Mexico is due to have deployed smart meters to more than half of its

customers and added large-scale investments in distribution automation, wide area measurement, home energy management, and IT.

In 2013, Electric Light & Power explained that Mexico's energy regulator Comision Reguladora de Energia (CRE) developed a smart grid roadmap. CRE allocated spending across 17 smart grid market segments including smart metering, transmission and distribution network infrastructure and IT. The roadmap is being updated in 2016. The Government was working on developing a concrete regulatory framework and political leaders were aiming to reduce electricity prices and incorporate small-scale generators. CFE has been testing smart grid infrastructure for several years and has successfully completed a number of pilot projects using a variety of vendors and technologies.

Mexico is a member of the Global Smart Grid Federation (GSGF) and ISGAN.

6.10.3 Current Cybersecurity Nexus

- The smart grid implementation approach in Mexico focuses on value chain integration as well as system integration using IEC Common Information Model (CIM) standards.

Defining critical infrastructure protection

In 2013, Mexico set its plans for infrastructure development, and its government and private sector came together at the Critical Infrastructure Protection Forum to share knowledge on safeguarding virtual and physical networks. The forum in 2013 focused on supply chain security, extortion, kidnap-for-ransom and cyber defense. Discussions occurred on pipeline protection and supply chain resilience as well as crisis management for major transport hubs and trade routes and cyber-attacks on IT infrastructure. Cargo is vulnerable to attack on the nation’s highways, railways, ports and airports, with attacks ranging from illegal taps of Pemex pipelines to the hijacking and theft of entire trucks and trains. Experts agree that a joint effort is required by both the public and private sectors in order to increase supply chain security.

Another key front in critical infrastructure protection is cyber defense. Mexico repeatedly features as one of the world’s most vulnerable economies to cyber-attacks. While these sources explain that Mexico has yet to suffer a large-scale attack on its critical infrastructure, the advent of more sophisticated malware makes the sector highly vulnerable. Formal efforts to improve Mexican cybersecurity only started in 2012 with the creation of the national CERT. However, the SCT, the interior ministry and the defense ministry still do not have dedicated cyber security units and cyber defense has yet to be elevated to the level of national security policy.

According to a McAfee/CSIS 2012 report on critical infrastructure protection and cyber-attacks, when it came to threat perceptions and responses, Mexico was identified as behind since it had adopted only half as many security measures as leaders like China, Italy, and Japan.

More than 40 percent of the executives interviewed expected a major cyber-attack within 12 months (one that causes severe loss of services for at least 24 hours, loss of life or personal injury, or the failure of a company.) In Mexico, seven out of ten had this expectation. 60 percent felt unprepared for a large-scale DDoS attack against their companies. Two-thirds of the companies also saw their systems as vulnerable to stealthy infiltration.

Defining cybersecurity

According to the 2015 ITU country report, specific legislation on cybercrime has been enacted through the Federal Criminal Code. Specific legislation and regulation related to cybersecurity has been enacted through the Law on Advanced Electronic Signatures. Mexico has a national CIRT known as CERT-MX. In Mexico, compliance with ISO standard 207001's requirements for an information security management system is required of all key government institutions. This is the nationally recognized framework for implementing internationally recognized cybersecurity standards. There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals. The Specialized Information Security Committee (CESI) developed a National Strategy for Information Security (ENSI), which guides all actions to be undertaken by entities of the Federal Government to prevent, identify, neutralize or counteract risks and threats to information security. There is no national governance roadmap for cybersecurity in Mexico. Personnel at the Scientific Division have received and continue to participate in specialized training from the Police Development System of Mexico (SIDEPOL), as well as from numerous other security and law enforcement organizations in countries including Colombia, the United States, The Netherlands and Japan. Government-led efforts to promote increased cybersecurity awareness have included the organization of various conferences for both government institutions and educational institutions.

The exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity is not known for Mexico. There is no information about any framework for sharing cybersecurity assets across borders. Mexico has national or sector-specific programs for sharing cybersecurity assets within the public sector through CESI authorities that have also developed a collaboration protocol between CERT-MX and various agencies of the Mexican Government to respond to cyber incidents. CERT-MX cooperates directly with private institutions. One of ENSI's primary aims includes further increasing and institutionalizing cooperation and information sharing between public/private stakeholders in a more integrated fashion. Mexico is a member of FIRST and the OAS/CICTE. It receives cybersecurity technical assistance through the OAS CICTE cybersecurity program.

According to the 2013 UNIDIR Cyber Index on International Security Trends and Realities, the Mexican Public Security Secretariat has a police unit to investigate cybercrimes. The National Autonomous University of Mexico's CERT works with the Cybercrime Police to provide

support and technical advice to Mexican authorities and shares data with information security professionals.

6.10.4 Cybersecurity Challenges (Issues)

- The challenges for smart grid include renovating existing infrastructure, integrating renewable energy, and reducing the cost of energy.

This section identifies the current and planned cybersecurity-energy nexus in Mexico.

According to the Trend Micro/OAS 2015 report on Cybersecurity and Critical Infrastructure in the Americas, beyond the work done by each country or by the organizations, there is no official information about security incidents in industrial systems or critical infrastructures in the region.

The TrendMicro/OAS report of 2013 on trends and government responses in Latin America and the Caribbean found that Mexican authorities registered a 40 percent increase in the number of cyber incidents in 2012, largely due to hacktivist attacks. Despite having several units tasked with responding to and analyzing cyber incidents, the economy still cites a lack of legislative norms and public awareness as reasons for cyber insecurity. The most serious attacks in 2012 targeted government infrastructures specifically created and employed to support the presidential elections in July. The Mexican Government initially only had one unit in the Secretariat of Public Security tasked to respond to cyber threats. Increased frequency of cyber incidents impelled the creation of a new Coordination Center for the Prevention of Electronic Crimes. The center is responsible for managing cyber incident response, investigating electronic crimes, analyzing digital evidence, protecting critical infrastructures, and responding to digital threats that would affect the integrity of critical networks.

In addition, the National Specialized Cyber Incident Response Team augments government capabilities. Technicians in this team are highly qualified and continuously trained to ensure knowledge of emerging hacking tools and techniques. This group monitors and secures the federal government’s digital assets.

Incident response only represents one area of cybersecurity in which Latin American and Caribbean states have made significant progress. Many are beginning to draft national cybersecurity policies and strategies. With the support of the OAS, Colombia became the first Latin American country to adopt a comprehensive national cybersecurity and cyber-defense strategy. Chile, Peru, Mexico, and others are endeavoring to do the same. Latin American and Caribbean strategies identify key stakeholders, delineate roles and responsibilities, establish coordination and information sharing mechanisms, and prepare strategic action plans for national cybersecurity efforts.

Recent acknowledgment of vulnerabilities in critical infrastructures has spurred several OAS members to adopt initiatives seeking to strengthen their ICS security. Mexico similarly

acknowledged the acute risks that threats to ICS pose and supported specialized training for many of its incident response technicians.

There is however a lack of defined and harmonized terminology. This TrendMicro/OAS report highlights that the term “cyber incident” is not uniformly understood or applied across the region. Some governments interpret a cyber incident as any report or complaint sent to a national response team, while others are more exacting in their classification. In 2012, governments generally noted an increase in the frequency of cyber incidents compared with 2011, even where definitive quantitative data was incomplete or unavailable. Several governments clarified that the numbers they provided did not necessarily reflect real changes in attack frequency, but rather improvements in network monitoring and better-trained personnel, which allowed organizations to detect more system breaches and other illicit cyber activities. Those countries with recently established national CSIRTs reported some of the most significant increases in managed incidents.

According to this report, collecting data to enable a truly comprehensive and detailed picture of the extent of all such incidents and activities in the Americas and the Caribbean, or anywhere else, remains at this point simply impossible. Many private companies and other non-governmental entities continue to be hesitant to report attacks or breaches. A general and persistent lack of collaboration among stakeholders at all levels further complicates the collection of reliable and actionable information on data breaches.

Hacktivism or politically motivated hacking received widespread media attention in 2012 and information provided by OAS members suggests that this form of cyber incident is indeed on the rise in the region. Spyware was found on law enforcement servers in at least one country. Numerous states provided information suggesting that traditional organized crime syndicates have increasingly turned to the internet to extort and launder funds—very much in keeping with observed global trends.

Both OAS and Trend Micro data indicated a rise in the number of attacks against critical infrastructure. A publicly operated national energy utility in one country experienced a spate of cyber attacks, although the national CSIRT was able to minimize damage caused by the breaches. While attacks involving critical infrastructures have not yet caused catastrophic losses or physical damage in the Americas and the Caribbean, they do highlight the need for vigilance and improved resilience, as many critical systems in the region remain exposed.

One of the main impediments to curbing illicit cyber activity in 2012 was the lack of adequate legislation and robust cybersecurity policies. Paired with inexperienced cybercrime investigators and the shortage of prosecutors who specialize in technology-related offenses, many OAS members are facing difficulties deterring and prosecuting hackers and other cybercriminals. In surveys submitted to the OAS, members consistently discussed a need for highly skilled professionals who can secure networks, diagnose intrusions, and effectively manage cyber

incidents as they unfold. Low enrollment in technical-degree programs is a manifestation of this problem. Given the time it takes to acquire cybersecurity skills and expertise, this low enrollment may have a noticeable impact in the coming years.

Mexico's energy reforms have created a number of agencies and reshaped existing ones. ASEA (the National Safety, Energy and Environmental Agency) and CNH (the National Hydrocarbons Commission) are reshaping the regulatory landscape of the oil and gas sector. Some articles argue that the Government still needs to address how it plans to secure pipelines, zones of onshore exploration, and land bases for deep-water development. They recommend that companies develop their own security infrastructure and plans.

Cyber-related policy opportunities and challenges for further consideration:

According to reports in 2013, there has been a lack of attention to the protection of critical infrastructures such as gas pipelines in Latin America. Domestic unrest is present in many Latin American countries and pipelines make easy targets. Labor activism and the remote terrains through which most high-pressure pipelines traverse also add to the risk. Security experts believe that almost all major oil and gas pipelines across the region are vulnerable. Online articles also explain that energy theft is worse than in any other region. An extra layer of difficulty arises in this instance since often it can be difficult to attribute accurately responsibility for a cyber incident.

Given the economy's domestic refineries and natural gas imports, it should closely consider possible cyber threats to oil and gas suppliers. Particularly since many major oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. This could possibly cause damage but breaches may also cause high damage to corporate assets, public infrastructure and safety, or the wider economy. Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain. Mexico should therefore closely monitor cyber issues relevant to oil and gas security as well as the supply chain.

Mexico should also ensure that extensive computer security/cybersecurity measures are in place for its nuclear plant. The IAEA (as well as several nation states) provides guidance for consideration by states, competent authorities, and operators. The aim is to prevent the theft of material or sabotage of plants and facilities.

Regarding international cooperation efforts, at the regional level, Mexico is a member of the Organization of American States (OAS). Mexico is participating in the fourth UN GGE (2014/2015), the fourth Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

6.10.5 Future Cybersecurity Nexus

There is insufficient data on this topic for Mexico. This is a potential area of future growth.

6.10.6 Smart Grids

Given the interest in the smart grid, enhancing cybersecurity is essential and it should be considered as part of a larger smart grid deployment strategy. SmartGrid Mexico could be further explored as a good starting point to leverage its experience in managing stakeholder relationships in this field. It is a nonprofit, public interest association that promotes the development and implementation of technological solutions that increase the efficiency of the energy sector. It prompts the establishment of smart grids and works to integrate the efforts of industry, academia, and the Government. Its mission is to encourage the development and establishment of smart grids in Mexico.

6.11 New Zealand

6.11.1 Economy Energy Resources

The APEC Energy Overview of 2014 provides an extensive outline of New Zealand's energy sectors. The report outlines that due to its remote location, New Zealand has no electricity or pipeline connections to other economies. It is self-sufficient in all energy forms apart from oil and has modest energy resources, including reserves of 79.4 million barrels of oil, 29.2 billion cubic metres of natural gas and 571 million tonnes of coal. In 2012, hydro, geothermal, wind and bioenergy resources met around 73 percent of electricity demand.

6.11.2 Smart Grid Initiatives

Three utilities, Contact, Genesis, and Meridian, are deploying smart meters across the economy. There has been some criticism that meters have not reduced energy usage. The utilities introduced real-time monitoring of energy use when possible but some cases some meters had not been fitted with a home area network (HAN) chip.

A May 2015 report by Northeast Group LLC, "Oceania Smart Grid: Market Forecast (2015 – 2025)", notes that Oceania has one of the most developed power sectors in the world, with well performing utilities, unsubsidized electricity prices, and high rates of electricity consumption. New Zealand (and Australia) is well positioned to continue its existing smart grid projects and develop new ones. The economies' high per-capita income and a number of incentives for clean technology will underpin the sector. New Zealand has nearly completed its AMI rollout. Additionally, it has accomplished its rollout without significant regulations, simply due to the positive business case of AMI.

The Ministry of Business, Innovation, and Employment with the support of the Electricity Networks Association commissioned the New Zealand Smart Grid Forum (NZSGF) in 2014.

The Forum brings together parties from business, scientific and academic circles, policy makers, regulators and consumers. Its objective is to advance the development of smart electricity networks through information sharing and dialogue, supported by analysis and focused work-streams. The forum promotes its objectives to parties involved in smart electricity network development to encourage the active participation of the diverse elements of the power demand and supply chain in its activities; promotes and facilitates a collective understanding of current smart electricity network developments; collaborates and seeks synergies with associated initiatives in areas such as electricity load control, innovation, data sharing, system security and data security, and consumer empowerment; identifies barriers to investment and the means to address those barriers; and develops and communicates a collective understanding of developments in other jurisdictions.

The NZSGF produced its first six-month report for the Minister of Energy in October 2014. According to this report, the NZSGF is unlike similar groups overseas in that it has not been convened to address a specific issue (generally decarbonation and the necessary changes to the electricity system required to accommodate renewable energy sources and greater demand response). The primary objective of the forum is to advance the development of smart electricity networks in New Zealand through information sharing and dialogue, supported by analysis and focused work streams. New Zealand initially established NZSGF for a 12-month period to give members the opportunity to explore the issues facing smart grid adoption and to confirm whether it has a longer-term role and support from the wider industry and stakeholder community. It will report to the Minister every six months and provide recommendations. New Zealand believes there is a considerable advantage in using this broad representative model from across the electricity system.

The first meeting, in April 2014, developed a work plan, which includes the following actions: 1) a stock take of smart grid activity; 2) visions for New Zealand smart grid; 3) management of disruptive technologies on electricity networks; and future sector operating models. The first deliverable was a catalogue of smart grid standards, publications, trials, case studies and activities in New Zealand (November 2014). One of its priorities is to carry out a stock take summary of current and recent smart grid activity as a reference document to inform its work streams. It will also produce reports on models of how the smart grid may evolve in New Zealand in the period to 2050; options and recommendations for managing the impact of disruptive smart grid technologies on the costs and quality of supply from electricity networks; and future operating needs that digital disruption to the electricity system will face.

NZSGF delivered the "catalogue of smart grid standards, publications, trials, case studies and activities in New Zealand in November 2014. It finds that there are were approximately 1.1 million smart meters installed in New Zealand, and estimates for up to 1.25 million by April 2015. New Zealand's AMI rollout has been market-led, which the report explains is rare internationally as large-scale rollouts are typically mandated.

It finds that there are potential issues with the ownership of / payment for data, and privacy (noting that retailers and other parties with access to data are obliged by the Privacy Act 1993 to prevent the unauthorized or unintended use or disclosure of that information). In addition, the New Zealand EMS market is still relatively immature. There are a variety of products on the market such as ZigBee and Nest, which are falling in price; however, uptake by consumers has been slow.

It outlines the following smart grid developments and trials by EDBs: Vector owns the electricity distribution network in the greater Auckland region. In addition to being the largest gas and electricity distributor in New Zealand, 40 percent of Vector's business is in related technology products. Vector sees significant opportunities in renewable distributed generation. It is currently investigating a number of initiatives including testing new renewable and energy management technologies for the home and businesses, many of which Vector is delivering through it's involvement in new technology developments. Vector has launched an installation of solar PV panels combined with battery storage for domestic customers.

Unison Networks views smart grid applications as aligning to three areas: EMS technologies, smart metering, and load control (including systems and communications). Unison developed a strategy for a more aggressive implementation of smart grid applications through the deferment of low risk asset refurbishment that, in turn, releases capital for the application of smart grid technologies.

Powerco is New Zealand's second largest electricity and gas network utility. It connects with networks in Taranaki, Wanganui, Rangitikei, Manawatu, Wairarapa and Wellington. Powerco has identified the opportunity for smart grid technology in major asset replacement projects in the medium term. The company has focused on exploiting smart grid technologies on a small-scale through creating business plans for individual projects. Underlying the whole approach is a focus on improving network reliability. Powerco views New Zealand as fulfilling a 'fast follower' role when it comes to the incorporation of smart grid technologies for distributed generation and electric vehicles. In becoming a fast follower, Powerco is conducting small-scale trials on home management systems and network automation to keep experience and capability within the company for when large-scale investment will be necessary.

As New Zealand networks often do not consider themselves in a competitive environment, there is a strong history of data sharing between Unison and Powerco. To some extent, this broadens both companies' knowledge base and helps prepare for future changes. Powerco will also continue to work closely with the University of Christchurch Green Grid project.

Powerco is undertaking two smart networks research projects: Demand Side Management Technology, and Behavior and Distribution Transformer Monitoring. Project One: Demand Side Management Technology & Behavior: The objective is to bring global research into the New Zealand context and demonstrate different pricing and technology opportunities to reduce peaks

whilst giving consumers better choices. Powerco's project will research consumer and supply chain behavioral factors that influence success of retailers or other parties rolling out new products and services. Project Two: Distribution Transformer Monitoring: This trial assesses the business case of intelligent monitoring or information collection across the distribution network using 250 distribution transformer monitoring units. The project's focus is on the value of information for network monitoring.

Orion uses Demand Response for the purposes of deferring capital expenditure and maintaining compliance with their security of supply standard. The use of Demand Response was an important tool in managing the restoration of supply during the 2010-2011 Canterbury earthquakes. Metering owners have installed approximately 110,000 smart meters, most of which contain inbuilt ripple receivers on the Orion network. Where appropriate, the remainder of the 190,000 network connections have standalone ripple receivers.

The Blue Skin Community Energy Project: The Blueskin Wind Development is led by Blueskin Energy Ltd, a company wholly owned by the Blueskin Resilient Communities Trust (BRCT). It is building three 850 kW wind turbines generating approximately 6.1 GWh for an 'energy community' of 2500-3000 people with a demand of 5.4 GWh annually. BRCT has agreements with OtagoNet. Pioneer Generation, Meridian, Trustpower, DNV-GL Energy, Russell McVeagh, Ethical Power Consulting, the Akina Foundation and Foot Law have provided assistance. The Blueskin Energy Project is in its fourth year of wind monitoring and is preparing a Resource Consent application to build the turbines at a cost of approximately $5 - $6 million. BRCT is in discussions with Oxford University to begin a trial of DIY smart grid initiatives. This study will be part of a wider global research with other sites in South Africa and the United Kingdom.

Variable and Dynamic Line Rating (VLR and DLR) is another tool that Transpower uses to improve capacity utilization of assets, by 'working the assets harder'. The tool changes the rating of transmission lines to reflect likely or actual operating conditions. For example, a line might be able to be rated at a higher capacity on a cold day, thereby avoiding the need for high cost resources to meet regional peaks. This requires either real time monitoring of the local weather along a transmission line or use of detailed historical data. This information feeds into an algorithm that calculates the new line rating. Transpower is using variable ratings based on detailed historic data on six transmission lines already and will begin exploring the use of real time information to lift grid performance.

The Electricity Authority (EA) is an independent Crown entity with the statutory objective of promoting competition in, reliable supply by, and the efficient operation of the electricity industry for the long-term benefit of consumers. The EA's focus for market development is to develop a workably competitive electricity market by reducing barriers to entry, expansion and exit of parties facilitating consumer participation, providing efficient price signals and promoting flexibility and resilience into the market and market systems. The EA's 2014/15 work program

includes several key regulatory projects that support the development of a smart grid, particularly by facilitating consumer participation and by providing efficient price signals. These projects include: Distribution Pricing Review; Retail Data Project; Research Project: Effects of Low Fixed Charges; Time-Of-Use Pricing; Flick Electric; Contact Energy: Peak & Off-Peak Pricing; and Examples of Smart Consumer Participation.

EVs are relevant to smart grids because recharging impacts on demand and grid stability, and EV batteries have the potential to provide useful backup and storage capacity. The greatest impact will be on local distribution networks, especially as the uptake of EVs is likely to be clustered in certain areas – potentially higher socioeconomic areas in cities. Northpower is actively promoting the use of EVs – it has made two standard chargers available to the public, and has installed a fast charger capable of providing 80 percent charge capacity within 30 minutes (compared to the standard eight-hour full charge). New Zealand's Association for the Promotion of EVs (APEV NZ), which is the sister association to APEV Japan, also promotes EVs. APEV NZ's mission is to create financial, environmental, health and energy security benefits for all New Zealanders through facilitating innovation, education, demonstration and collaboration in the EV sector. New Zealand Professors John Boys and Grant Covic have pioneered inductive power transfer technology (IPT). Their technology charges electric vehicles. Developed at the University of Waikato in partnership with HybridAuto, the UltraCommuter is a two-seat battery electric car that uses a lithium-iron-phosphate battery. It is designed for long range.

Meridian's Smart New Zealand Energy Futures report concluded that changes in electricity demand should create a substantial economic case for smart grid opportunities in New Zealand.

6.11.3 Current Cybersecurity Nexus

New Zealand's Ministry of Business, Innovation and Employment has committed $10.6 million to the six-year Security Technologies Returning Accountability, Transparency and User-centric Services (STRATUS) project—a collaboration of Unitec, Waikato University, the University of Auckland, and the Cloud Security Alliance—which will create tools to return the control of cloud-based data to users. The project will utilize Cloud8, the Cybersecurity Lab's cloud computing test bed, which was set up in 2013 so experiments will run in a realistic environment.

Zigbee is the smart meter standard used as it covers a wide-range of wireless applications.

Defining critical infrastructure protection

Under the "Critical 5" document of March 2014, "Forging a Common Understanding for Critical Infrastructure", Annex A provides the definitions of Critical Infrastructure and Associated Sectors for New Zealand.

Infrastructure is as one of the six key drivers of economic growth in New Zealand (in the Business and Growth Agenda 2012). It is defined as "the fixed, long-lived structures that

facilitate the production of goods and services and underpin many aspects of quality of life. Infrastructure refers to physical networks, principally transport, water, energy and communications." To that end, New Zealand expresses its vision that "by 2030 New Zealand's infrastructure is resilient and coordinated and contributes to economic growth and increased quality of life."

New Zealand defines resilient infrastructure as being "able to deal with significant disruption and changing circumstances." The government would like to drive two key ideas through its infrastructure strategy: better use of existing infrastructure and better allocation of new investment.

New Zealand's National Security System, released in May 2011, takes a broad, all-hazards, approach to national security. With regard to critical infrastructure, it highlights "new points of vulnerability" from the integrated and networked character of national and international infrastructures, such as electricity, gas and water grids, telecommunications networks, air, rail and shipping services, and the extent to which daily life depends on their efficient functioning.

New Zealand's Cyber Security Strategy from June 2011 has identified as one of its three objectives the need to improve cyber security for critical national infrastructure and other businesses. New Zealand's Critical Infrastructure includes: Energy; Transportation; Social Infrastructure; Water; and Telecommunications.

The Centre for Critical Infrastructure Protection (CCIP) is now part of the National Cyber Security Centre (NSCS). The Government Communications Security Bureau (GCSB) hosts NCSC.

Under the New America compilation of terms and definitions, the following key terms related to existing cybersecurity and information security definitions are delineated for New Zealand:

> Critical National Infrastructure: A term used by governments to describe assets that are essential for the functioning of a society and economy (e.g. electricity generation, gas production, telecommunications, water supply etc.).

Defining cybersecurity

According to the 2015 ITU country report, legislation related to cybercrime has been enacted through the 248-259 Crimes Act 1961. Legislation and regulation related to cybersecurity has been enacted through the Electronic Transaction Act; Electronic Data Safety Bill; Unsolicited Electronic Messages Act; Electronic Identity Verification Bill; Government Communications Security Bureau Act; and the Telecommunications (Interception Capability and Security) Act. NCSC is the national CERT. Standards New Zealand is the agency responsible for implementing internationally recognized cybersecurity standards.

The national cybersecurity strategy is the New Zealand Cybersecurity Strategy 2011. The GCSB Annual Report and Compliance Report are the nationally recognized benchmarks for cybersecurity. Unitec is home to New Zealand's first Cybersecurity Centre, which is the officially recognized national or sector specific research and development (R&D) program/project for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. GCSB provides various educational and professional training programs in order to raise awareness with the general public, promote cybersecurity courses in higher education and promote certification of professionals in both public and private sectors throughout New Zealand.

According to the UNIDIR Cyber Index 2013, the Ministry of Economic Development is the lead for cybersecurity policy. NCSC, under GCSB, works with government agencies and critical infrastructure organizations to improve cybersecurity and protection against cyber threats. New Zealand's Unitec and Japan's National Institute of Information and Communications Technology established a new cybersecurity research center in order to bolster New Zealand's cybersecurity. New Zealand's 2010 defense white paper discusses cyber-attacks as a growing threat. The New Zealand Defense Force's Statement of Intent 2011–2014 also discusses the threat of cyber attacks and says that New Zealand will increase support operations for its forces.

Under the New America compilation of terms and definitions, the following key terms related to existing cybersecurity and information security definitions are delineated for New Zealand:

- Cyberspace: The global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communication takes place.
- Cyber Security: The practice of making the networks that constitute cyber space as secure as possible against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them.
- Cybercrime: Any crime where information and communications technology is:
    - Used as a tool in the commission of an offence;
    - The target of an offence;
    - A storage device in the commission of an offence.
- Cyber Attack: An attempt to undermine or compromise the function of a computer-based system, access information, or attempt to track the online movements of individuals without their permission.

6.11.4 Cybersecurity Challenges (Issues)

The 2011 Cyber Security Strategy outlines that critical national infrastructure providers, including the banking and finance, telecommunications, transportation and energy sectors, and other businesses, are more and more reliant on digital systems. It explains that cyber-attacks are

becoming more advanced and sophisticated. Incidents reported internationally suggest that attacks are increasingly targeted at intellectual property and other proprietary information held by businesses, as well as at individuals. Many attackers are coordinated, well-funded, and investing heavily in new ways to exploit the digital environment.

It notes that a successful targeted cyber-attack could disrupt the economy's critical services, negatively affecting the economy and, potentially, threaten national security. Cyber-attacks can interfere with the production and delivery of essential goods and services or result in the theft of intellectual property or personal information. New Zealand needs to ensure its cybersecurity activities are as coordinated and effective as possible to be able to identify and mitigate emerging cyber threats. The Government has a responsibility to protect its own systems and assist critical national infrastructure providers. Government units exist to tackle issues such as scams, spam, identity theft, electronic crime and critical national infrastructure protection. The Government also provides support to NetSafe, an independent non-profit organization, to deliver cyber safety education and awareness programs in schools.

It highlights that the threat to New Zealanders and the New Zealand economy from cyber intrusions is real and growing. The key objectives of the Strategy are include: raising the cyber security awareness and understanding of individuals and small businesses; improving the level of cyber security across government; and building strategic relationships to improve cybersecurity for critical national infrastructure and other businesses.

The Government has appointed the Ministry of Economic Development as the lead policy agency responsible for coordinating cybersecurity policy and implementing this strategy. It notes that improving cybersecurity is a shared responsibility. In developing this strategy, the Government sought input from a wide range of stakeholders across government, industry, nongovernment organizations and academia. The Government will continue to build partnerships and work with these stakeholders to implement the initiatives outlined in the Strategy and to explore further opportunities to enhance the economy's cybersecurity response.

The priority areas and key initiatives include: increasing Awareness and Online Security; Protecting Government Systems and Information; and Incident Response and Planning.

Regarding "Incident Response and Planning", the strategy notes that in light of the global growth in significant cybersecurity incidents, emergency preparedness is increasingly important. The Government will revise its cyber incident response plan to ensure New Zealand is prepared to respond to the evolving and increasing cyber threats. Through the establishment of NCSC, the Government will build on New Zealand's existing cybersecurity capability to plan for and respond to cyber incidents. The preparedness of New Zealand businesses to respond to cyber-attacks is critical to New Zealand's cyber resilience. As new and more sophisticated malware and attack tools are developed, it is increasingly important for businesses to have measures in place to identify, assess and respond to incidents and threats. The Government will work with

critical national infrastructure providers and other businesses to further develop their cybersecurity responses.

NSCS provides services to government agencies and critical infrastructure providers to assist them in defending against cyber-borne threats. It is a key element of the New Zealand Cyber Security Strategy (2011). The strategy recognizes that as the use of the internet in New Zealand increases, so too does vulnerability to cyber threats. NCSC explains that countering these threats is a shared responsibility, and government will work in partnership with industry, non-government entities and academia to improve New Zealand's cybersecurity.

NCSC partners with a range of New Zealand organizations including the Ministry of Business, Innovation and Employment; Department of Internal Affairs; NZ Police; Domain Name Commission; Internet NZ; NZ Internet Task Force; Netsafe. International partner organizations include: CPNI; GovCERT Uk; USCERT; CCIRC; CERT Australia; AusCERT; and APCERT.

GCSB contributes to New Zealand's national security by providing information assurance and cybersecurity to the Government and critical infrastructure organizations, foreign intelligence to government decision makers, and cooperation and assistance to other New Zealand government agencies.

Operators of critical power infrastructure developed and agreed to new standards for cybersecurity in March 2014. NSCS and New Zealand Control Systems Security Information Exchange forum developed the voluntary standards, "Voluntary Cyber Security Standards for Industrial Control Systems v.1.0". At the time, the GCSB Director explained that the national and economic security of New Zealand depends on the reliable functioning of critical infrastructure, like electricity networks. He explained that meetings are held several times a year to share information about threats and vulnerabilities in industrial control systems, which allow centralized supervision and control of remote assets such as power stations. It is this commitment to information sharing and collaboration across the industry, which has led to the development of the voluntary standards according to the Director. He explained further that the energy sector forms a key part of New Zealand's critical economic infrastructure and application of these voluntary standards will help increase the resilience of key systems and reduce their vulnerability to cyber-borne threats. The development of these standards is a tangible demonstration of effective collaboration between government and the private sector.

The power sector has developed nine standards, but it is hoped that they can be applied to all industries that operate industrial control systems. They will be a starting point for further development and improvement.

A guide called the New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTS) is also available through NCSC. In addition, the March 2014 "Forging a Common Understanding for Critical Infrastructure" document outlines that the

following narrative represents the shared views of the Critical 5 member nations (Australia, Canada, New Zealand, the United Kingdom, and the United States) with the objective to provide a high-level overview of the meaning and importance of critical infrastructure.

Cyber-related policy opportunities and challenges for further consideration:

Regarding international efforts, the 2011 cybersecurity strategy specifies that the Government is actively working with New Zealand's international security partners on cybersecurity issues and is currently reviewing New Zealand's legal framework in relation to the growing issue of international cybercrime. Internationally, the Government will continue to collaborate with security and trade partners to ensure New Zealand contributes effectively to global cybersecurity initiatives.

At the regional level, New Zealand is a participant at the ASEAN Regional Forum (ARF).

6.11.5 Future Cybersecurity Nexus

There is insufficient data on this topic for New Zealand. This is a potential area of growth.

6.11.6 Smart Grids

Given the interest in the smart grid, enhancing cybersecurity is essential and it should be considered as part of a larger smart grid deployment strategy.

For instance, the New Zealand Smart Grid Forum in its activities now promotes and facilitates a collective understanding of current smart electricity network developments, and it has mentioned the need to find collaborate over issues such as data sharing, system security as well as data security, and consumer empowerment. Its November 2014 report specifically says NZSGF did in fact find that there are potential issues with the ownership of / payment for data, and privacy (noting that retailers and other parties with access to data are obliged by the Privacy Act 1993 to prevent the unauthorized or unintended use or disclosure of that information).

The report also makes note of the voluntary standards for cybersecurity developed and agreed by operators of critical power infrastructure in New Zealand. The NZ standards, based on standards developed by the North America Electric Reliability Corporation (NERC), provide a framework to help relevant organizations recognize and address cybersecurity risks. The CSSIE forum facilitates exchange of information, in a confidential and trusted environment, concerning threats, vulnerabilities and incidents of electronic attack on control systems. Membership includes electricity generation and network companies. New Zealand's electricity mostly is generated in large centralized power stations, which can be a long way from where the electricity is used. It is then moved around the economy through the national grid and then to local distribution networks.

6.12 Papua New Guinea

6.12.1 Economy Energy Resources

According to the APEC Energy Overview Study published in March 2014, the resource industry, which includes minerals, oil and gas, contributes to approximately 80 percent of PNG's export income. In 2011, PNG's net primary energy supply was 2257 kilotonnes of oil equivalent. Light crude oil and petroleum products accounted for 76 percent, gas for 5.7 percent, and hydro and other fuels for the remaining 18.4 percent. PNG hopes to supply 25 percent of its electricity needs from renewable resources including geothermal, wind, and biomass.

6.12.2 Current Cybersecurity Nexus

Defining critical infrastructure protection

Open source searches do not currently produce a list of material related to the definitions of critical infrastructure or critical infrastructure protection in PNG.

The Department of National Planning and Monitoring in the MDTP 2011-2015 refers to "transport infrastructure and other critical infrastructure such as power, water and sanitation".

Defining cybersecurity

According to the 2014 ITU country profile for PNG, it does not have specific legislation on cybercrime; specific legislation or regulations related to cybersecurity; an officially recognized national CIRT; officially recognized national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards. PNG does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals. It does not have an officially recognized national cybersecurity strategy, or a national governance roadmap for cybersecurity.

The National Information Communication and Technology Authority (NICTA) is the officially recognized agency responsible for implementing national cybersecurity strategy, policy and roadmap. PNG does not have any officially recognized national or sector-specific R&D programs or projects for cybersecurity standards, best practices and guidelines for public or private use.

PNG does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors. It does not have any public sector professionals certified under internationally recognized certification programs in cybersecurity. PNG does not have any

certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

According to the ITU factsheet, PNG does not have officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states. It does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector. It is a member of the ITU-IMPACT initiative and it has access to relevant cybersecurity services.

It is among the beneficiary countries of the EU/ITU co-funded project "Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries" (ICB4PAC). It is a member of the Asia Pacific Telecommunity (APT) and participates in the APT organized forum on cybersecurity.

According to a PNG submission to APEC in 2009 on its Counter Terrorism Action Plan, it aimed to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including UN General Assembly Resolutions 55/63 (2000) and convention on cybercrime (2001). It also outlined its aim to identify national cyber-crime units, international high technology assistance contact points, and to create such capabilities to the extent they do not already exist.

According to the 2014 ASPI report on cyber maturity in the Asia Pacific region, cyber awareness among government, business and wider society gained significant momentum throughout 2013–14. The report explains that it is clear that each country surveyed, including PNG, is increasingly cognizant of cyberspace as a critical area.

The report delineates that PNG is developing new cybercrime laws and that it is taking proactive steps to improve its cyber maturity, but a lack of resources and infrastructure has proven to be a limiting factor in this area. The Government has recognized the importance of the issue, joining ITU–IMPACT, pressing for increased investment in digital infrastructure, and calling for a Cyber Cell in its most recent Defense White Paper.

Through international engagement, particularly with Australia, PNG has been strongly involved in addressing cybercrime issues, and similar support in other areas of cyber governance. Building technical capabilities could prove highly beneficial for the economy.

PNG's organizational structure for cyber issues is relatively limited and focused mainly on IT development and cybercrime issues. NICTA is responsible for the regulation and licensing of ICT and aims at 'making ICT services work in PNG's public interest'. It has been proactive in developing its policy and capacity to police cybercrime in an effort led by NICTA in consultation with international partners. Much of PNG's cyber legislation and regulation is developed through the ITU's Capacity Building and ICT Policy, Regulatory and Legislative

Frameworks Support for Pacific Island Countries (ICB4PAC) programs. NICTA has also been proactive in developing ICT regulations and is developing cybercrime legislation.

PNG is making a concerted effort to adopt external frameworks to build domestic cyber legislation and regulation, especially in the area of cybercrime, but the efforts remain ongoing and capacity for implementation is an area for improvement.

PNG has been proactive in reaching out to international partners to develop domestic cyber policies and capabilities. Working with ITU–IMPACT, the Australian Attorney-General's Department, APEC, various development organizations and other actors, it has been strongly engaged in internal capacity building. However, international engagement on governance issues remains limited.

PNG is not home to a recognized domestic CERT. However, it is a member of PacCERT, which covers 22 constituent countries throughout the Pacific.

Despite recent attempts to bolster the strength of the PNG Defense Force, which has limited capabilities and resources, cyber issues have traditionally not been a priority for the economy. The 2013 Defense White Paper references establishing a defensive 'Cyber Cell' to protect a yet to be developed 'Integrated ICT Network', but outlined no timelines or implementation strategies. Clear evidence of military cyber policy and capacity in cyber operations remains limited.

PNG has a limited digital economy, but recent structural reform has increased opportunities in the telecommunications sector. As competition increases in the ICT sector, reduced internet costs and improved accessibility and speed will open new opportunities for the economy's digital economy.

Public awareness and debate concerning cyber issues and the use of ICT have grown quickly within PNG. Connectivity driven by mobile phone use and the spread of social networks has resulted in what many have called the 'PNG Spring'. Forums such as SharpTalk have spurred public discourse of all sorts, including on cyber issues. The Government has also been proactive in increasing cyber safety through the Pacific Islands Chiefs of Police Cyber Safety Pasifika program.

Internet connectivity in PNG is very limited, at only 2.3 percent total internet penetration. However, the rapid adoption of mobile technology potentially will quickly expand internet penetration. While the Government has been actively supporting a national transmission network for the economy, infrastructure and costs are likely to remain the main barriers to improved connectivity for some time.

6.12.3 Cybersecurity Challenges (Issues)

Several opportunities and challenges relevant to cybersecurity issues for further consideration:

About 90 percent of the population has no access to electricity, and the progress in providing electricity to rural areas has been slow. PNG continues to rely heavily on diesel or fuel-oil power plants and generators in spite of the economy's abundant renewable energy resources. Increased access to and improved quality of supply is hindered by a lack of sector planning and the lack of community service obligations payments to PNG Power, in unprofitable areas of the economy.

On the main grids, power outages are becoming increasingly frequent because of insufficient generation and poorly maintained transmission and distribution systems. Therefore, while developing plans, frameworks, and strategies related to cybersecurity is a good starting point on the part of PNG, it is also essential to ensure the implementation and maintenance measures in the energy sector.

Regarding the role of the private sector, according to the 2014 ADB report, the PNG Development Strategic Plan emphasizes the importance of private sector participation in funding energy infrastructure, such as the building of transmission lines and electricity generation capacity. According to the 2014 ASPI report on cyber maturity, there is little evidence of strong official engagement between the Government and industry on cyber issues. However, the report mentions that the Government is actively pursuing efforts with private entities to improve internet accessibility in the economy. NICTA is engaged with the ICT sector for the development of physical infrastructure. Consequently, if there are plans to increase public-private sector participation, specific public-private sector considerations relating to cybersecurity are appropriate.

Capacity building related to cybersecurity issues in this sector should not solely focus on technical capacity building but also on policy as well as legislative, organizational, and law enforcement training. In addition, external offers of capacity building could also be coordinated and capacity building should reflect the unique needs of PNG.

It is also in the interest of PNG as well as the international community that measures be enacted to mitigate possible weak links and havens of vulnerable ICT infrastructures. The fact that PNG is not highly developed in terms of ICT development, and that it has a less developed ICT infrastructure and less connected critical infrastructure means that this could prove to be an advantage. As it becomes more connected, lessons could be applied from the experience of other economies in countering cyber-related threats, best practice policies, and measures implemented. Both security and data privacy by design should be incorporated from inception in the development of ICT and connected critical infrastructures.

According to the 2014 ASPI report on cyber maturity in the Asia Pacific region, despite increased awareness regarding cybersecurity issues in PNG, the report reemphasizes that capacity and implementation remain a problem. For PNG, lack of infrastructure severely impedes growth in cyber maturity. The urban–rural internet penetration gap continues to be an obstacle to full cyber maturity. Lack of infrastructure is the largest challenge to the development of a strong digital economy in PNG. Continued limited investment and by political concerns exacerbate the infrastructure problem, limiting the potential for near-term growth in the digital economy. The recent opening up of the telecommunications sector offers potential for increased connectivity. PNG is limited by government and infrastructure deficiencies. Mobile technologies offer a promising route to increase internet penetration into society and business. With sufficient long-term investment directed at the development of such assets, PNG has the potential to build niches in the digital marketplace.

Given that oil and gas contribute significantly to PNG's export income and that it has several plants and power stations, it should also very closely consider possible cyber threats to oil and gas suppliers. Particularly since many major global oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. This could possibly cause damage but breaches may also cause high damage to corporate assets, public infrastructure and safety, or the wider economy. Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain.

PNG should very closely examine cyber issues relevant to electrical grids, oil and gas security, as well as the supply chain.

At the regional level, PNG is a participant of the ASEAN Regional Forum (ARF).

6.12.4 Future Cybersecurity Nexus

There is insufficient data on this topic for PNG. This is a potential area of future growth.

6.12.5 Smart Grids

When tailoring smart grids to developing economies and emerging economies, reports outline that while advanced economies have well-developed modern grids, many others have grids that do not operate consistently over a 24-hour period, and still others have little electricity infrastructure at all. Developing economies and emerging economies often face high growth in electricity demand, high commercial and technical losses in a context of rapid economic growth and development, dense urban populations and dispersed rural populations. These aspects present both significant challenges and opportunities for economies like PNG.

Reports outline that smart grids can play an important role in the deployment of new electricity infrastructure in developing and emerging economies by enabling more efficient operation and

lower costs. Small "remote" systems – not connected to a centralized electricity infrastructure and initially employed as a cost-effective approach to rural electrification – could later be connected easily to a national or regional infrastructure. As a means to access to electricity in sparsely populated areas, smart grids could enable a transition from simple, one-off approaches to electrification to community grids that can then connect to national and regional grids.

6.13 Peru

6.13.1 Economy Energy Resources

According to the APEC Energy Overview Study published in March 2014, owing to its scarce oil resources, Peru is a net importer of oil. Particularly, domestic production is not only insufficient to meet the economy's demand, but since most crude oil produced is of extra-heavy quality and several of Peru's domestic refineries are unable to process it, a substantial share of domestic production is exported. In contrast, natural gas resources are significant and the economy is a major global gas producer, representing the only source of liquefied natural gas exports in South America.

6.13.2 Current Cybersecurity Nexus

Defining critical infrastructure protection

Open source searches do not currently produce a list of material related to the definitions of critical infrastructure protection or critical infrastructure in Peru.

Defining cybersecurity

According to a 2015 report by Trend Micro and the Organization of American States (OAS) on Cybersecurity and Critical Infrastructure in the Americas, Peru has done work in cybersecurity. Organizations like the Union of South American Nations (UNASUR) and Member States have included cybersecurity and cyber defense in their agenda. They have also organized military conferences in different cities, and analyzed alliances and cooperation initiatives.

According to the 2015 ITU country report, specific legislation on cybercrime has been enacted through the following instruments: Penal Code; Computer Crimes Act; and Incorporating Computer Crimes in the Criminal Code. Specific legislation and regulation related to cybersecurity has been enacted through the following instruments: Protection of Personal Data - Digital Signatures and Certificates Law. The 2014 Symantec/OAS report on Latin American and Caribbean Cyber Security Trends outlines that on the legislative front, the recent passage of three new laws – Incorporating Computer Crimes in the Criminal Code (Law 27309), Protection of Personal Data (Law 29733), and Computer Crimes Act (Law 30096) – has strengthened the economy's legal framework for promoting cybersecurity and combating cybercrime. Additional modification of other existing legislation is under consideration. Peru has an officially

recognized national CIRT known as PeCERT. There is no officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards. There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Peru.

The ITU factsheet explains that Peru has an officially recognized cybersecurity strategy known as Plan Estratégico en Seguridad Informática y de la Información. It does not have a national governance roadmap for cybersecurity. (The 2014 OAS/Symantec report states that one is under development.)

The PeCERT and the Division of High Technology Crimes (DIVINDAT) are responsible for cybersecurity. The 2014 report by OAS/Symantec explains that two agencies serve as the primary leads for cybersecurity and cybercrime-related efforts in Peru. The national CSIRT, PeCERT, is the lead entity responsible for cybersecurity-related matters in Peru, including incident prevention and management. The investigation of cybercrime and corresponding responsibilities falls primarily with the Division of High Technology Crimes (DIVINDAT), within the Directorate of Criminal Investigations (DIRINCRI) of the National Police of Peru (PNP). While PeCERT is an operational CSIRT with national level responsibility, it is currently revising and updating its mechanisms, procedures and policies for incident response.

Peru does not have an officially recognized national benchmarking or referential guide to measure cybersecurity development. There is no program or project for R&D on cybersecurity standards, best practices and guidelines. DIVINDAT and PeCERT actively train their personnel to maintain and develop their capacity to perform their core functions. Internal awareness raising initiatives within their own institutions have entailed a full range of activities to ensure users' understanding of concepts not always associated with but key to cybersecurity such as physical security, security logic, and human security. External awareness raising activities have included media campaigns, and outreach and education for private sector entities including banks, payment processors, and other business and commercial interests.

The OAS/Symantec report explains that DIVINDAT, for example, regularly conducts workshops to update its staff's knowledge of and ability to utilize effectively digital forensics tools. While academic institutions in Peru do offer degree programs with specializations in cybersecurity and cybercrime, no information was provided to indicate whether government officials benefit from the availability of those educational opportunities.

It further outlines that collaboration and information sharing with other economies' competent national authorities has been limited. This is an area where additional steps could occur in the future. Both PeCERT and DIVINDAT reported that they actively work to enhance the security of their constituencies and increase their resiliency and recovery capacity. These efforts have consisted of a combination of preventative and reactive measures. On the preventative side, internal and external awareness raising and education have been a high priority.

Peru does not track the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity. To facilitate sharing of cybersecurity assets across borders or with other nation states, DIVINDAT actively seeks assistance from foreign entities where and when appropriate. It also maintains active partnerships with, and supports the efforts of national and international NGOs, working to combat cyber and other crimes that have utilized ICTs.

PeCERT has initiated a dialogue to increase collaboration with the private sector, particularly ISPs and banks. Peru is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Peru also participates in the OAS Inter-American Committee Against Terrorism (CICTE).

According to the 2013 UNIDIR Cyber Index report, in May 2012, the Government approved Ministerial Resolution 129-2012-PCM, which requires National Information System members to follow common information security standards. Within the President's Council of Ministers, the National Office of Electronic Government and Information Technology is responsible for developing and implementing information security regulations. This Office established the national CERT.

At the regional level, Peru as a member of the OAS, has participated in the OAS CICTE Cyber Security Program, and plans to establish a national CSIRT. Through the OAS program, Peruvian ministries have received technical assistance to develop cybersecurity and CERT capabilities. Peru has reformed its penal code to incorporate crimes committed using IT. The National Police has a High Technology Crimes Investigation Division, which is responsible for investigating crimes committed using ICT.

According to the OAS/Symantec report, Peru showed an increase in 2013 of approximately 30 percent in the number of cyber incidents reported to national authorities. The report identifies the business sector, academia, telecommunications entities, the police, and other public sector institutions as the most affected sectors of the population. Authorities received a wide range of crime reports in 2013. The most common were credit card cloning, identity theft, email threats, intrusion by hacking or cracking, unauthorized access to databases, internet extortion, sexual blackmail, fraudulent financial operations, child pornography, and software piracy. DIVINDAT reported that there were several relatively high impact incidents in 2013 to which they were able to respond effectively.

6.13.3 Cybersecurity Challenges (Issues)

According to a 2015 report by Trend Micro and the OAS on Cybersecurity and Critical Infrastructure in the Americas, there is no official information about security incidents in industrial systems or critical infrastructures in the region.

Another 2013 Trend Micro/OAS report on cybersecurity trends and government responses in Latin America outlines that incident response only represents one area of cybersecurity in which Latin American and Caribbean states have made significant progress. Many are beginning to draft national cybersecurity policies and strategies. With the support of the OAS, Colombia became the first Latin American country to adopt a comprehensive national cybersecurity and cyber-defense strategy. Countries like Chile, Peru, Mexico, and others are endeavoring to do the same. Latin American and Caribbean strategies identify key stakeholders, delineate roles and responsibilities, establish coordination and information sharing mechanisms, and prepare strategic action plans for national cybersecurity efforts. Recent acknowledgment of vulnerabilities in critical infrastructures has spurred several OAS Member States to adopt initiatives seeking to strengthen their ICS security.

There is, however, a lack of defined and harmonized terminology in the region. This TrendMicro/OAS report highlights that it became clear that the term "cyber incident" is not uniformly understood or applied across the region. Some governments interpret a cyber incident as any report or complaint sent to a national response team, while others are more exacting in their classification. In 2012, governments generally noted an increase in the frequency of cyber incidents compared with 2011, even where definitive quantitative data was incomplete or unavailable.

Several governments clarified that the numbers they provided did not necessarily reflect real changes in attack frequency, but rather improvements in network monitoring and better-trained personnel, which allowed organizations to detect more system breaches and other illicit cyber activities. Those countries with recently established national CSIRTs reported some of the most significant increases in managed incidents. According to this report, collecting data to enable a truly comprehensive and detailed picture of the extent of all such incidents and activities in the Americas and the Caribbean, or anywhere else, remains at this point simply impossible.

Information sharing within governments - even those with the most advanced cybersecurity capabilities - continues to come up short, largely due to the practical realities of multiple organizations having to respond simultaneously to an ever-evolving range of threats and targets. In addition, many private companies and other non-governmental entities still are hesitant to report attacks or breaches. A general and persistent lack of collaboration among stakeholders at all levels further complicates the collection of reliable and actionable information on data breaches. The net consequence of all of these factors is a less than adequate awareness of the problem, and the continued vulnerability of critical networks and information systems.

Hacktivism or politically motivated hacking received widespread media attention in 2012 and information provided by the Member States suggests that this form of cyber incident is indeed on the rise in the region. Spyware was found on law enforcement servers in at least one country. Numerous states provided information suggesting that traditional organized crime syndicates

have increasingly turned to the internet to extort and launder funds—very much in keeping with observed global trends.

Both OAS and Trend Micro data indicated a rise in the number of attacks against critical infrastructure. A publicly operated national energy utility in one country experienced a spate of cyber attacks, although the national CSIRT was able to minimize damage caused by the breaches. While attacks involving critical infrastructures have not yet caused catastrophic losses or physical damage in the Americas and the Caribbean, they do highlight the need for vigilance and improved resilience, as many critical systems in the region remain exposed.

One of the main impediments to curbing illicit cyber activity in 2012 was the lack of adequate legislation and robust cybersecurity policies. Paired with inexperienced cybercrime investigators and the shortage of prosecutors who specialize in technology-related offenses, many countries are facing difficulties deterring, prosecuting hackers, and other cybercriminals. In surveys submitted to the OAS, countries consistently discussed a need for highly skilled professionals who can secure networks, diagnose intrusions, and effectively manage cyber incidents as they unfold. Low enrollment in technical degree programs illustrate this problem. Given the time it takes to acquire cybersecurity skills and expertise, this low enrollment may have a noticeable impact in the coming years.

According to the 2014 OAS/Symantec report, private sector entities are not obligated to report incidents to relevant national authorities. However, PeCERT has initiated a dialogue to increase collaboration with the private sector, particularly ISPs and banks. This effort is in part based on the recognition that private enterprises generally have a greater ability to detect unusual traffic and attacks, as well as more mature security management systems, and, as such, are invaluable partners in securing the nation's critical infrastructures.

According to releases on the OAS site, CICTE in collaboration with the Peruvian Ministry of National Defense and the National Office of E-Government and Information (ONGEI) launched a cybersecurity crisis simulation in Peru in 2013. The simulation aimed to test communication channels between the various institutions responsible for protecting Peruvian citizens from cyber threats. Participants faced a wide range of simulated cyber incidents affecting the economy's critical infrastructure. The Director of the ONGEI emphasized that steps are being taken to strengthen PeCERT and said the event would identify actions to improve the team's ability to cope with emerging cyber threats. The exercise included representatives from civil society, the energy sector, the finance sector, ISPs, and other stakeholders from the private sector and critical infrastructure operators, in addition to government participants.

Cyber-related policy opportunities and challenges for further consideration:

According to some reports from 2013, there has been a lack of attention to the protection of critical infrastructures such as gas pipelines in Latin America. Pipelines make fairly easy targets.

Labour activism and the remote terrains through which most high-pressure pipelines traverse also add to the risk. Security experts believe that almost all major oil and gas pipelines across the region are vulnerable. Labor activism is also a cause of concern in economies such as Peru. Online articles also explain that energy theft is worse than in any other region. An extra layer of difficulty arises in this instance since it can often be difficult to attribute accurately responsibility for a cyber incident, misappropriation could lead to misunderstandings or inaccurate identification of responsibility for incidents.

Given the economy's significant domestic refineries and natural gas resources, it should closely consider possible cyber threats to oil and gas suppliers. Particularly since many major global oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. This could possibly cause damage but breaches may also cause high damage to corporate assets, public infrastructure and safety Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain. Peru should closely monitor cyber issues relevant to electrical grids, oil and gas security and the supply chain.

Foreign companies are encouraged, especially in areas involving exports, infrastructure, and services to work with PeCERT. OAS commitments also include continuing to develop comprehensive national cybersecurity strategies and to engage all relevant stakeholders in their development and implementation; the importance of promoting public sector cooperation with the private sector and academia in order to strengthen the security and protection of critical ICT infrastructure; to explore future opportunities to broaden CICTE's efforts to protect critical ICT infrastructure, including by implementing capacity building programs to strengthen all critical components of the global supply chain.

However, according to the 2014 OAS/Symantec report, authorities reported a number of impediments to address to enhance the economy's cybersecurity posture and improve its ability to combat cybercrime. Challenges regarding access to information received particular attention, including the difficulty of getting information from ISPs or other service providers in a timely fashion. Insufficient resources and a lack of willingness to share information and cooperate on the part of other government and private institutions are highlighted as key impediments. It is therefore important that specific public-private sector considerations linked to cybersecurity and the energy sector be further examined.

In addition, capacity building related to cybersecurity issues specifically in the energy sector should not solely focus on technical capacity but also include policy as well as legislative, organizational, and law enforcement training. In addition, external offers of capacity building should also be highly coordinated and capacity building should reflect the unique needs of Peru.

According to the APEC Energy Overview in 2014, although Peru does not use nuclear energy for electricity generation, a government-run nuclear program has been in operation since 1975. In 2009, IPEN presented its Institutional Strategic Plan 2010-2016, which comprises three main objectives, one of them regarding the promotion of electricity generation based on nuclear energy.

Peru should therefore ensure that extensive computer security/cybersecurity measures are in place. The IAEA (as well as several nation states) provides guidance for consideration by states, competent authorities, and operators. The aim is to prevent the theft of material or sabotage of plants and facilities.

At the regional level, Peru is a member state of the OAS.

6.13.4 Future Cybersecurity Nexus

There is insufficient data on this topic for Peru. This is a potential area of future growth for the economy.

6.13.5 Smart Grids

According to the U.S. Department of Commerce's ITA brief, MINEM approved a ten-year plan for the expansion of grid infrastructure, and a number of projects are being developed to strengthen and upgrade inefficient lines in the north and center of Peru. As all transmission activities are in private hands, the upgrade and expansion of the Peruvian grid could generate significant opportunities for investors.

While Peru's smart grid market is in its nascent stages of development, the Government has commissioned system planning and roadmap efforts and remains engaged with international stakeholders on key technical issues like interoperability. Limited opportunities are expected in the near-term – particularly in the areas of renewable supply integration and management – unless technical and regulatory issues are addressed.

Little investment has supported either smart grid or energy efficiency development in Peru to date, although both remain a priority for Peru's National Climate Change Strategy. In 2012, OSINERGMIN tasked the consulting firm Indra to diagnose barriers to smart grid deployment and encourage future smart grid investment. The roadmap is in the process of being finalised. ITA expects smart grid and energy efficiency technology to play a bigger role in the Peruvian electricity market following the roadmap's public release. In the meantime, transmission & distribution equipment suppliers and relevant utility service providers will find opportunities through projects to extend and interconnect Peru's grid.

According to media reports, the proposed plan of action includes the electric system's progressive development towards a new smart grids model. It includes all the agents in the plan

of action's development, based on identifying pilot projects that allow testing functionalities and technologies prior to the final regulatory development for a large-scale rollout.

The ITA report explains that demand for renewable energy technologies, as well as the smart grid products and services that can move electricity from variable power plants in remote areas to consumers is on the rise. It outlines that the limited availability of low cost financing, especially from local banks, has slowed investment and reduced the attractiveness of renewable energy and smart grid projects. The high cost of financing both renewable energy and smart grid projects continues to be a major hurdle for the power industry as technology risk and policy uncertainty have made local financiers reluctant to invest in this sector. Without the involvement of local banks, Peru has relied on international organizations, like the Inter- American Development Bank and the World Bank, to develop large-scale renewable energy projects. This has limited the sector's growth. As new renewable energy and smart grid projects come online, local financiers are expected to develop a comfort level that should support future investment.

Since smart grid and energy efficiency technology will play a bigger role in the Peruvian electricity market following the roadmap implementation, enhancing cybersecurity is also essential.

6.14 The Philippines

6.14.1 Economy Energy Sectors

The APEC Energy Overview of 2014 provides that the economy has modest proven fossil fuel reserves of oil, natural gas and coal. Renewable energy sources provide a contribution of 29 percent to its power generation, from hydro sources and geothermal energy. Of the total primary energy supply in 2011, 55 percent was contributed by indigenous sources and the remainder was imported. Geothermal and other renewable energy resources accounted for 38 percent of the total primary energy supply, while oil and coal, which are largely imported, contributed 33 percent and 20 percent, respectively.

6.14.2 Smart Grid Initiatives

- The Philippines have a "Qualified 3rd Party Program," which includes microgrid projects.
- The USTDA has secured a contract for work in smart grid development.
- Ex-Im Bank has guaranteed $1 billion dollars in financing.

2014 reports find that investment in Southeast Asia will include smart metering and the modernization of electricity transmission and distribution networks with sensors, communications and software. By 2024, the largest markets will be Thailand, Indonesia, Malaysia, Singapore, the Philippines, and Viet Nam, according to a recent study by Northeast Group LLC.

Southeast Asian economies are just beginning on the path of modernizing their electric infrastructure. Electrification programs and growth in renewable resources will also drive investment. 2014 reports online also outline that some emerging economies, such as Thailand, Malaysia, Indonesia, and the Philippines, are making plans to deploy smart grid technology. While this region is currently behind other global regions in terms of smart meter deployments and regulatory frameworks, its smart grid market is growing. There are already smart grid pilot projects in several economies throughout the region. By 2022, Southeast Asian economies will likely have an electricity demand profile similar to Latin American economies where large-scale smart meter deployments already exist. The region's current electricity consumption rates are among the lowest in the world, while distribution loss rates are comparatively moderate, offering less short-term savings potential compared with other global regions. Additionally, regulatory frameworks remain largely undeveloped in the region. Even in the more advanced economies, deployments are still at the initial pilot level.

This Northeast Group study finds that while Singapore is currently leading the region in development, later in the decade the large markets of Thailand, Indonesia, Malaysia, Viet Nam, and the Philippines will account for significant smart grid investment. Several economies in the region have drafted smart grid roadmaps and pilot projects are widespread. Regulatory frameworks are still developing but momentum will grow over the next several years. Both utilities and vendors are already working together to ensure preparedness when regulations are finalised. Many vendors are active across the region. These include ABB, Alstom, Echelon (NES), EDMI (Osaki), Elster, Enverv, GE, Itron, Schneider, Secure, Siemens, Silver Spring Networks, ST Electronics, Trilliant, and other global and local vendors.

Media reports in 2013 outline that the Manila Electric Co. (Meralco) is the economy's biggest distribution utility with more than 25 million people connected with approximately 5 million meters. GE announced that it would be working with Meralco on a prepay smart metering rollout with smart meter networking company Trilliant that is expected to eventually expand to a whole host of smart grid services. There appears to be a preliminary target of 40,000 meters, which could expand depending on customers' take-up of the services. To support prepayment services, Meralco intends to provide customer bill updates, alerts on account balances and pricing information over the internet or via mobile phones. Mobile phones are specifically mentioned as a key device in Asia. Other smart grid networking companies cited include Silver Spring Networks, as well as meter vendors with in-house communications and network technologies like Itron, Sensus, Elster and Landis+Gyr.

In 2013, the Philippines DOE released a circular creating an inter-agency committee to develop a smart grid policy framework and roadmap for the power industry. Meralco has been advocating for the use of smart grid technology.

The circular noted that the policy formulation committee will propose the national strategy for the smart grid for the period until 2030. The committee is composed of members of the DoE, and attached agencies such as the National Power Corp, National Transmission Corp, the National Transmission Corp, the National Electrification Administration, the National Grid Corporation of the Philippines, and the Philippine Electricity Market Corp. Other government offices and private companies will assist in the development of the policy. The committee will prepare the transition policies and guidelines for the effective implementation of the smart grid by power generation companies, transmission companies, distribution utilities, and other network service providers. The committee is also to formulate customer education and information frameworks for economy-wide smart grid awareness and acceptance. It will seek funding from bilateral and multilateral funding institutions willing to finance smart grid initiatives.

The 2013 DOE Circular notes that the DoE's role is to encourage private sector investments in the electricity sector and to promote indigenous and renewable energy sources. It notes that there are some electric power industry participants that have adopted and implemented some level of smart grid initiatives in their operations.

In 2014, the U.S. Trade and Development Agency (USTDA) awarded a grant to Meralco (the largest power distribution utility in the Philippines), to modernize its distribution systems and develop a smart grid design. The feasibility study includes a pilot project for a demand response system, allowing Meralco to balance the grid by integrating control systems and communications infrastructure into its network. These upgrades ultimately should reduce energy losses and manage system peak demand, while optimizing Meralco's sub-transmission and distribution network in and around Metro Manila, which serves 5.2 million customers.

The Department of Energy in its 2012 vision for the Philippines Smart Grid 2012 outlined that with more than 7,100 islands, providing electricity services remains one of the biggest challenges for the Government.

Current smart grid users in the Philippines outlined in this vision included:

1. Transmission/System Operator (NGCP): Energy Management System; SCADA; Automatic Meter Reading (AMR).
2. Distribution Utilities (MERALCO, BENECO, VECO, and DLPC): SCADA (Distribution System): AMR (Pilot only); Customer Information System; Automated Mapping/Facilities Management (MERALCO Pilot only).
3. Market Operator (PEMC): Market Management System.

Smart Grid Development in NGCP: Advanced SCADA Project; Overall Command Center Project; FS for First Smart Grid Substation in Philippines; and Renewable Energy Integration. NGCP and SGCC signed a smart grid strategic cooperation memorandum in 2011.

Meralco is expect to play a key role in driving the nation's journey to a more energized future with the smart grid and through their alliance with PLDT, Smart and Metro Pacific through: a fully-automated home powered by a Home Area Network; maximum control of electricity consumption through pre-paid electricity; and growth in business and the economy with affordable electricity rates.

Future plans cited then included: 1) developing policy and a Regulatory Framework for smart grid by creating an interagency working group (IA-TWG) to conduct policy and technical research and studies; 2) starting a capacity building program (best practices of pioneer economies such as United States, Australia, China, Japan, among others); pursuing international cooperation (APEC and international standards associations such as IEEE and IEC); 3) develop the road map/roll out plan for smart grid implementation by 2013/2014 with a phase-in approach, timelines, and coverage; 4) standards development including interoperability; 5) integration plan e.g., EVs, RETs; 6) IEC program; and 7)continuing R&D activities.

Challenges for the Philippines include its large population of more than 92 million people and 7,107 islands. The DOE has projected that the demand for power in the economy will soon overtake the total installed generation capacity and further investments in the power sector are key to the vitality of the nation's economy.

6.14.3 Current Cybersecurity Nexus

The Philippines follows IEEE standards.

Defining critical infrastructure protection

Twelve key sectors are mentioned in the National Critical Infrastructure Protection Plan (NCIPP): government; food and agriculture; transportation and communication; water; energy; health; emergency response services; manufacturing; banking and finance; strategic commercial centers; and cultural and religious sites and facilities. The NCIPP defines critical infrastructures as comprising two aspects: the physical and cyber.

Defining cybersecurity

According to the 2015 ITU country report, legislation on cybercrime has been enacted through the Cyber Crime Prevention Act - RA 10175. Legislation and regulation related to cybersecurity has been enacted through the: Data Privacy Act of 2012 RA 10173; and Electronic Act of 200 RA 8792. The Philippines' national CERT is PHCert. PH-It is the Philippines' national representative to APCERT. The Philippines has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through iGovPhil services which include a single sign-on facility, and a Public Key Infrastructure for secured online transactions. It does not have an officially approved national

(and sector specific) cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

It has a 2005 national cybersecurity plan. It does not have a national governance roadmap for cybersecurity. The following agencies implement national cybersecurity strategy, policy and roadmaps: The Cyber Crime Unit; Computer Forensic Labs (Zamboanga City, General Santos City and Davao City); and DOST-ICTO Cyber Security Section. The DOST-ICTO Cyber Security Section is responsible for benchmarking and measuring cybersecurity development. It does not have any officially recognized national or sector-specific R&D programs/projects for cybersecurity standards, best practices or guidelines in either the private or the public sector.

The Philippines is a member of the ITU-IMPACT initiative. The ASPI report on cyber maturity from 2014 finds that the Philippines participates in several multilateral cyber-oriented working groups and workshops led by organizations such as APEC, ASEAN and the UN, with a particular focus on the area of cybercrime. However, although involved in these forums and a member of ITU–IMPACT, it often is taking no active role in them. It maintains infrequent bilateral dialogues on cyber issues, mainly with the United States.

According to the UNIDIR Cyber Index 2013, in January 2012, the Philippines passed the Cybercrime Prevention Act to define and penalize internet-related crimes and empower law enforcement agencies in the investigation and prosecution of cyber criminals. The Act created the Office of Cybercrime under the Department of Justice, the National Cyber Security Center under the Department of Science and Technology, and the National Cybersecurity Coordinating Council under the Office of the President. However, this was overturned.

In February 2015, Microsoft announced it is collaborating with the Philippine National Police Anti-Cybercrime Group (PNP-ACG) to address cybercrime. Microsoft will provide readiness programs, knowledge, tools and the necessary technologies to assist in combating cybercrimes. It will work with the PNP-ACG in identifying current requirements, challenges, skills and equipment. Microsoft will also assist the PNP-ACG in developing a readiness program for specific units of the PNP cybercrime group. The PNP-ACG has the primary responsibility of implementing cybercrime laws and anti-cybercrime campaigns of the PNP and government. The PNP-ACG focuses on cybercrime-, computer- and other content-related offences.

Under the New America compilation of terms and definitions, the following terms are cited:

a) Information Weapon: Information resources strategically developed or created for information warfare or to cause damage, confusion or disadvantage and with any other forms of malicious intent.
b) Cyber Crimes or Information Crimes: (i) criminal acts involving elements of information security; and (ii) acts of malicious intent directed at information resources (e.g. techno-vandalism, techno-trespass and superzapping);

c) Information Terrorism: terroristic acts in the context of information security;
d) Information Warfare: actions aimed at achieving information superiority by executing measures to exploit, corrupt, destroy, information resources and telecommunication systems to achieve goals and interests, for example, cyber warfare (information warfare in the defense and military context) or "Internet war" (information warfare in the larger societal context).

6.14.4 Cybersecurity Challenges (Issues)

Official reports cite that one of the key areas of interest identified in the Philippines is energy infrastructure resilience, particularly improving risk assessment, management, and mitigation.

The Philippines' Task Force for the Security of Critical Infrastructure issued the first National Cyber Security Plan in 2005. The Plan called for reducing vulnerabilities, nurturing a culture of cybersecurity among individual users and critical sectors, and strengthening self-reliance on information technology and human resources. The Task Force also created the National Cyberspace Security Coordination Center, tasked with detecting and investigating computer network intrusions and incidents. In 2008, the Commission on Information and Communication Technology in the Office of the President established the National Cybersecurity Coordination Office and appointed an undersecretary as National Cybersecurity Coordinator.

ASPI's 2014 report on cyber maturity in the Asia Pacific outlines that the Philippines has demonstrated an awareness of cyber threats, but a lack of sufficient legislation and capabilities is a clear limitation. As emphasized in the 2011 Digital Strategy, with sufficient investment in infrastructure, the Philippines has the potential to bolster its currently limited digital economy. While there are intentions to improve national cyber maturity, a lack of resources tempers the prospect of significant near-term developments. The Government has shown an awareness of cyber threats and has made some efforts to address them.

In addition, the report finds that critical national infrastructure protection is relatively unorganized. In particular, the report outlines that PH-CERT is a non-profit, voluntary organization that draws its funding from membership fees and sponsorship arrangements. It has faced operational problems due to lack of financial support and low staffing. The Philippines National Police Criminal Investigation and Detection Group has stated that it will revive the Government CERT (G-CSIRT), which was disbanded in 2008, but it is unclear whether that has occurred. The Armed Forces of the Philippines have created a Security Operation Center with a primarily defensive role, protecting military systems. The Task Force for the Security of Critical Infrastructures of the Cabinet Oversight Committee on Internal Security had launched the Government G-CSIRT in 2004 as the focal point for reporting computer attacks intrusions on information and communications system.

Cyber-related policy opportunities and challenges for further consideration:

Greater connectivity in the region could raise the probability of transnational crime and cross-border cyber-related incidents. With increasing access to high-speed networks, low-level cybercrime has already risen in the ASEAN region. In Asia, policy experts further suggest that the growth of cybercrime could increase instability. Misappropriation of responsibility could lead to misunderstandings and the possible escalation in tensions or conflict because the accurate identification of those responsible for a cyber incident is not always easy (especially since there is now a wide range of varying threats that may come from different non-state actors).

The Philippines should closely consider possible cyber threats to oil and gas suppliers. Particularly since many global major oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. This could possibly cause damage but breaches may also cause high damage to corporate assets, public infrastructure and safety, or the wider economy through energy prices. In addition, it could affect the economy's competitiveness. Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain.

The economy should therefore closely monitor cyber issues relevant to the electric grid as well as the supply chain.

Given the Philippines' long-term interest in nuclear energy, the IAEA (as well as several nation states) provides guidance for consideration by states, competent authorities, and operators. The aim is to prevent the theft of material or sabotage of plants and facilities.

The ASPI cyber maturity report in 2014 highlights that while there appear to be mechanisms to aid the growth of the economy's ICT-led industries through the 2011 Digital Strategy, there is little proactive engagement of industry on cybersecurity matters. Specific public-private sector considerations relating to cybersecurity and the energy sector should be carefully examined.

There seems to be a lack of financial resources. In addition, labor resources in cybersecurity are lacking. Consequently, there is a need for more capacity building and skilled professionals in the economy. Capacity building related to cybersecurity issues specifically in the energy sector should not solely focus on technical capacity building but also include policy as well as legislative, organizational, and law enforcement training. In addition, external offers of capacity building should be highly coordinated and capacity building should reflect the unique needs of the Philippines.

At the regional level, the Philippines is a member of ASEAN. It is also a participant at the ASEAN Regional Forum (ARF).

6.14.5 Future Cybersecurity Nexus

There is insufficient data on this topic for Philippines. This is a potential area of future growth.

6.14.6 Smart Grids

Given the interest in the smart grid, enhancing cybersecurity is also essential and it should be more closely considered as part of a larger smart grid deployment strategy.

6.15 Russia

6.15.1 Economy Energy Resources

The APEC Energy Overview of 2014 provides an extensive outline of the Russia's energy sectors. It outlines that the Russian Federation has a vast natural resource base that includes major deposits of coal, natural gas, oil and other minerals. Its major industries include oil and gas production, petroleum refining, and mining, amongst others. The improvement of energy efficiency and energy savings is one of the priority areas of the Energy Strategy to 2030.

6.15.2 Smart Grid Initiatives

- A partnership of Accenture, MSRK and Belgorod is planning to make Belgorod the first smart grid city in Russia.

The APEC Energy Overview Study in 2014 outlines that the Ministry of Energy presented concepts for a program of power sector modernization for the period up to 2020. The central theme of the modernization is to introduce new technologies, both domestic and imported, increasing the reliability of the electricity supply and energy security.

In December 2014, online reports noted that Russia announced plans to modernize its energy infrastructure, expanding its use of the smart grid electrical framework. Smart grid technology is already in use in Russia, but as the current distribution infrastructure loses 12 percent of its transmitted energy, which adds up to a loss of $10 billion per year, there is an incentive to expand the use of the technology. The Russian power transmission and distribution company, JSC Russian Grids, has identified the smart grid as a solution, and has secured partial funding from the National Welfare Fund (NWF). According to a report by Zpryme, Russia's smart grid system is expected to grow from $5.5 billion in 2012 to $15.7 billion by 2017. Russia's smart grid framework will be tested in the Kaliningrad, Yaroslavl and Tula regions, where it seems that there is a particular need to respond to inefficient loss of energy. If the program's first stage is successful, additional regions will adopt the smart grid model.

According to a 2012 "Joint Russian/American Study On Legal/Regulatory, Market, Consumer And Technical Impediments To Smart Grid Technology Deployment", the following major impediments to the deployment of smart grid technology in Russia were identified: Less than Optimal Legislation and Regulation; Unpreparedness of the Grid for Disruptive Smart Grid

Innovations; Weak Smart Grid R&D and Federal R&D Policies; Weak Interactions between Science and Business; and Lack of Federal Leadership in Smart Grid Development. Relating to markets, the report identified: Weak Market Policy of the Government and Administrative "Manual Control"; Unpolished and Inefficient Capacity Market Rules, Favoring Big Generators; Market Oligopoly Structure and Government Policy Supports Large Generation and Depresses Competition; Non-Transparent and Distorted Pricing Mechanism; Regulators are not Ready for Significant Changes in Current Market Rules and Regulatory Framework; Retail Market Rules Impede Distributed Generation Deployment; Lack of Ancillary Service Market Regulations; and Fragmentation of the Power Market Regulatory Framework.

Efficiency issues raised included: Policy Makers' Concerns about Distributed Generation on Generation Efficiency; Inability of "Prosumers" to Sell Excess Energy to the Grid; Grid`s Equipment is Physically and Technologically Outdated, Networks are Poorly Maintained; Insufficient Investment Resources for Monitoring and Accounting Systems and Inadequate Cost-Benefit Analysis; Absence of Proper Data and Data Management Methodology; Insufficiently Developed Regulations and Rules for Implementation of Existing Laws and Norms; Smart Metering Regulation Gaps; Illiteracy, Proper Information and Expert Support for Decision-making on Energy Conservation Solutions; Undeveloped Market of Energy Efficiency Services; Lack of Qualified Personnel, Methodology and Training of Decision Makers on the End Use Side; Problems in Getting Access to Credit Capital for Energy Efficiency Projects; Current Regulations do not Incentivize Consumers to Increase their Load Density; and Lack of Policy Coordination.

Behavioral norms issues identified included: Residential Consumers Lack Understanding of Energy Markets, Efficiency and Smart Grid Benefits; Regulators Lack Understanding of Energy Systems and Smart Grid; Absence of Energy Efficiency Values and Practices of C&I Customers; Absence of Common Terminology in Smart Grid; High-level of Non-payments; Customers are not Incentivized to Deploy AMI and Smart Meters; Regulation and Administrative Provisions Gaps in Smart Meters Installation; Customers are Suspicious on Smart Meter Installations; Regulation Gaps in Smart Metering and Smart Meter Information Ownership; Smart Metering Methodology Gaps; Abuses in Accounting Devices Installation; Lack of Standards and other Technical Regulations for Smart Meters; and Lack of Coordination in Data Reporting and Acquisition; and Unpreparedness to Analyze and Store Future Smart Grid-enabled Data Arrays.

According to the 2013 study, the strategic objective of innovation and scientific-and-technical policy in the energy sector is to set up a sustainable national innovation system in the energy sector providing the Russian fuel and energy system with highly efficient domestic technologies and equipment (including smart grid), as well as innovative scientific and technical solutions necessary to maintain the economy's energy security. Among the priorities of the electric energy industry the following 2030 State Energy Strategy goals: developing highly integrated intelligent backbone transmission and distribution networks of new generation (smart grids) in

Russia's unified energy system; developing power electronics along with devices based on it, especially various types of network controlling devices (flexible alternating current transmission systems, FACTS); developing a highly integrated information and management system of operational dispatch management working in real time mode with expert decision-making systems; and designing automated electricity demand controlling systems.

The study further notes that Russia is pursuing a state policy of innovation activity in the electricity sector. This applies to energy efficiency, renewable energy and smart grids. The 2030 Energy Strategy aims to ensure high energy, economic and environmental efficiency in the production, transport, distribution and demand of electricity. (Smart) meters and accounting systems should be installed at all participants of electricity market and thermal power in power plants and substations, in enterprises. It does not explicitly state that the meters installed must be smart meters, but the focus is on having each grid connection metered and billed. The Russian Energy Agency is also required to develop a smart grid Initiative/Roadmap. The study identified no regional energy policies regarding smart grids. It seems that smart grid related regulations are mainly made on a national level.

Important drivers and focus areas identified by this study included: 1) increasing grid reliability and quality; 2) accommodating decentralized generation; 3) integration of renewables (the study identifies that smart grid technology is a necessary condition for a large share of renewable electricity on the grid); and 4) reduce energy losses (current network infrastructure does not have good protection from non-technical losses in electricity distribution such as electricity theft, but also losses due to poor equipment maintenance, calculation errors and accounting mistakes). According to Federal Grid Company data, smart grid technology will allow the reduction of the energy losses in the grids of all voltage levels by about 25 percent.

A problem identified is the age of the Russian grid. More than half of the grid components (transformers, overhead lines) are over optimal operation time. This might mean that basic replacement of current assets might have priority over smart grids. On the other hand, it might provide opportunities to start with a fresh, smart grid oriented approach according to the study. Energy Law 261 orders energy saving through smart grids. Pilot Projects by the President's Commission for Technological Development of Russian Economy aim to reduce energy consumption of Russia's GDP by 40 percent by 2020 through measures promoting energy saving, improving energy efficiency and improving legal environment. The greatest potential for energy saving is concentrated in the public sector and utilities.

One of the important smart grid implementation directions in Russia is the implementation of demand management systems. The Russian Ministry of Energy developed Methodological Recommendations for technical characteristics of smart equipment and systems, which would be used for electrical energy metering and billing. There is a need identified for a Smart Meter

Centre that can assist in design, purchase and implementation of smart meter and smart grid equipment.

The Russian Ministry of Economic Development introduced the Technology Platform "Intelligent Electric Power System of Russia". It allows for active participation in shaping the market of intelligent power services and occupying leading positions. It is an instrument to stimulate smart grid developments but does not seem to include funding of participants or projects.

There are several smart grid pilot projects identified by the study. There are two high voltage grid restructuring projects consisting of modernization of the transmission grid. The Federal Grid Company of the Unified Energy System (FGC UES) initiated and funded the projects. They includes the installation of digital substations and reactive power control. The main goal is to increase the reliability of the transmission grid.

The first smart grid project identified was a smart meter project in the city of Perm. Five pilot projects (President's Commission for Technological Development of Russian Economy) are in progress in Perm, two are related to future smart grids implementation: "Calculate, Save and Pay" and "Smart Account" as a part of the "Smart Metering". This project includes replacement of more than 50,000 meters by smart meters. The federal budget, IES holding and the local distribution company Permenergo fund it.

The second project was in the city of Belgorod. This Smart City project includes: "Smart metering" and "Smart accounting" – systems of electric energy charge and metering in real-time; "Reliable grids" – reconstruction of distribution grids; "Smart street lighting" – intelligent systems of street lighting; and "Smart House" – automatic consumers' control. The goal of the Smart City project in Belgorod is to increase reliability of power supply, reduce grid losses and reduce cost of electricity for consumers. The Belgorod Smart City project is funded by the distribution company, the Belgorod region and by the Federal Government, based on Federal Law 261. Almost 40,000 meters will be installed.

The third example is from the Astrakhan region. According to energy companies, in the period 2011-2012, smart meters were already installed in more than 4,900 domestic connections, 520 in the industrial sector, as well as 713 in high-voltage substations. All devices are remote connected: 2.4 thousand data transfer devices were installed. Another project is in Moscow. It seeks to develop an electric vehicle charging infrastructure in the Moscow City. The Moscow United Electric Grid Company runs it. This MOESK-EV project installed 24 normal charging stations and 3 fast charging stations in 2012. The goal is to demonstrate the prospects for electric transportation.

According to this report, at that time, Russia was at the initial phase of smart grid deployment, and it noted that there is no national strategy for smart grid, fixed terminology and standards. Additionally there is a lack of analytics.

Other important smart metering and smart grid pilot projects included: the electric vehicle infrastructure development in Moscow (Moscow United Electric Grid Company); digital substation project (JSC R&D Center for Power Engineering); and smart grid implementation at the Elginsky coal complex.

Russia (represented by TP IES (REA) is a participant in ISGAN.

6.15.3 Current Cybersecurity Nexus

Under the New America compilation of terms and definitions, the following key terms related to existing cybersecurity and information security definitions are delineated for Russia:

- Vital Structures: A State's facilities, systems and institutions, deliberate influence on the information resources of which may have consequences that directly affect national security (transport, energy supply, credit and finance, communications, State administrative bodies, the defense system, law-enforcement agencies, strategic information resources, scientific establishments and scientific and technological developments, installations that pose heightened technological and environmental risks, and bodies for eliminating the consequences of natural disasters or other emergency situations).

According to policy research conducted by the Finnish Institute of International Affairs on the evolution of Russian critical infrastructure protection policy, during the nineties, the focus was on 'population and territory'. The threat perception included natural emergencies or technological accidents, and ecological security. In the mid-2000s, the approach was monitoring of 'critically important objects', in other words a sectoral approach and the threat perception included terrorism, and de-modernization. From 2009 until the present day, CIP is a part of the national security strategy (2009). The threat perception includes terrorism, climate change, and cyber-attacks. According to the findings of this research material, the "conceptualization of critical infrastructure in Russia has evolved along lines similar to those adopted in the U.S. and the EU."

In 2012, a report by the Potomac Institute Cyber Center stated Russia has moved to protect its strategic assets. The Security Council of the Russian Federation released a document aimed at creation of a unified government system to detect, warn against and prevent cyber-attacks. The Security Council document takes a step toward implementation of the National Security Strategy of Russia until 2020, which calls for IT infrastructure improvements. In particular, the document calls for protection of the industrial control systems of strategically important facilities—what the report says would be called critical infrastructure. These are defined as assets whose malfunction could negatively affect a region's economy.

According to this report, the plan is to be implemented in three phases: 2012 to 2013, 2014 to 2016 and 2017 to 2020. The first phase involves development of an action plan. During the second phase, Russia would develop legal regulations, specific organizational responsibilities and the means to "liquidate" cyber incidents. The plan for the second phase also calls for establishment of a unified government situation center for detection and prevention of cyber attacks on critical information infrastructure, akin to a national CERT according to the report. The third stage, among other things, involves integration of security systems at the strategically important facilities.

It notes that the Security Council has identified cyber-attacks against critical infrastructure as a national security threat.

Defining cybersecurity:

ITU's country report on Russia provides that legislation on cybercrime has been enacted through the Criminal code (art. 271-273). Legislation and regulation related to cybersecurity has been enacted through the following instruments: Federal Law 152 on Personal Data Protection - regulated by Roscomnadzor (Telecommunications Regulator); Federal Law 139 on Blacklisting and ISP control - regulated by Roscomnadzor (Telecommunications Regulator). Russia has a governmental CERT (GOV-CERT), a joint government project CIRT (RU-CERT), and a CIRT based on Group IB, the leading Russian company in incident response, business CIRT (CERT-GIB). CERT-GIB has partnerships with the League of Safer Internet and the National Coordination Centre. Russia has officially recognized a National Security Concept of the Russian Federation (2000), a concept of the Foreign Policy of the Russian Federation (2013), an Information Security Doctrine of the Russian Federation (2000), Basic Principles for State Policy of the Russian Federation in the Field of International Information Security (2013) and conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (2011). It says the draft of Russia's Cyber Security Strategy is underway. It does not currently have any national governance roadmap for cybersecurity according to the ITU factsheet.

The Russian Federal Security Service (FSB), Federal Protection Service (FSO), Federal Service for Technical and Export Control (FSTEC), Ministry of Internal Affairs (MVD), Ministry of Defense (MoD) and the Foreign Intelligence Service (SVR) are the recognized institutions responsible for implementing national cybersecurity strategy, policy and a roadmap. Each government entity in Russia performs an annual audit of its own networks and systems depending on the requirements of the information. Russia has national or sector-specific R&D programs/projects for cybersecurity standards, best practices and guidelines for either the public or private sector to apply through the ITU-T study group question 17 on security. It does not have any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in

higher education and promoting certification of professionals in either the public or the private sectors according to the country report. The FSB has recognized national or sector-specific programs for sharing cybersecurity assets within the public sector with the following organizations: Federal Service for Technical and Export Control (FSTEC), MoD, Ministry of Internal Affairs (MVD), and the Financial Crimes Unit in Federal Tax Services.

Under the New America compilation of terms and definitions, the following key terms related to existing cybersecurity and information security definitions are delineated for Russia:

- Cyber Space: A sphere of activity within the information space, formed by a set of communication channels of the internet and other telecommunications networks, the technological infrastructure to ensure their functioning, and any form human activity on them (individual, organizational, state).
- Information Area: The sphere of activity involving the creation, transformation or use of information, including individual and social consciousness, the information and telecommunications infrastructure, and information itself.
- Information Space: Activities associated with the formation, creation, conversion, transfer, use, or storage of information that impacts individual and social consciousness, the information infrastructure, and information itself.
- Information Sphere: The present stage in societal development is characterized by an increasing role of the information sphere, which represents an assemblage of information, information infrastructure, entities engaged in the collection, formation, dissemination and use of information, and a system governing public relations arising out of these conditions.
- Cyber Security: A set of conditions under which all components of cyberspace are protected from the maximum number of threats and impacts with undesirable consequences.
- Information Security: Protection of the basic interests of the individual, society and the State in the information area, including the information and telecommunications infrastructure and information per se with respect to its characteristics, such as integrity, objectivity, accessibility and confidentiality.

A situation in which the basic interests of the individual, society and the State in the information area, including the information and telecommunications infrastructure and information itself with respect to its characteristics such as integrity, objectivity, availability and confidentiality, are protected.

By information security, Russian Federation means the state of the protection of its national interests in the information sphere, as determined by the overall balanced interests at the level of the individual, society and the state. The interests of the individual in the information sphere consist of the exercise of the constitutional rights of man and the citizen to information access, to

use of information in the interest of carrying on activities not prohibited by law and physical, spiritual and intellectual development, as well as of the protection of information that ensures personal security.

The interests of society in the information sphere consist of securing the interests of the individual in this sphere, reinforcing democracy, creating a rule-of-law social state, achieving and maintaining public harmony and the spiritual renewal of Russia.

The state's interests in the information sphere consist of creating conditions for harmonious Russian information infrastructure development and for the exercise of the constitutional rights and freedoms of man and the citizen with respect to receiving and using information to ensure the inviolability of the constitutional system, the sovereignty and territorial integrity of Russia, and political, economic and social stability; the interests of the state also consist in the unconditional maintenance of law and order and in the promotion of equal and mutually advantageous international cooperation.

Based on the national interests of the Russian Federation in the information sphere, the state forms its strategic and current domestic and foreign policy objectives for ensuring information security.

- International Information Security: The state of international relations in which global stability is not disturbed nor is the security of the world community endangered in the information space.
- Information Infrastructure: A set of technical means and systems of formation, creation, conversion, transmission, use, and storage of information.
- Information Weapon: Means and methods use with a view to damaging another State's information resources, processes and systems; use of information to the detriment of a State's defense, administrative, political, social, economic or other vital systems, and the mass manipulation of a State's population with a view to destabilizing society and the State. Ways and means used for the purpose of damaging the information resources, processes and systems of a State, exerting an adverse influence, through information, on the defense, administrative, political, social, economic and other vital systems of a State, as well as the massive psychological manipulation of a population in order to destabilize society and the State. Information technology, tools, and methods used for the purpose of information warfare.
- International Information Terrorism: The use of telecommunications and information systems and resources and exerting influence on such systems or resources in the international information area for terrorist purposes.
- Information War: Confrontation between States in the information field, with a view to damaging information systems, processes and resources and vital structures, and

undermining another State's political and social systems, as well as the mass psychological manipulation of a State's population and the destabilization of society.

6.15.4 Cybersecurity Challenges (Issues)

UNIDIR's cyber index report in 2013 outlines that the Russian Federation's Security Council released a national policy in 2012 for fighting cybercrime and the creation of a national system to detect and prevent cyber-attack. The Federal Security Service has responsibility for policy to secure the economy's networks by 2020. In January 2012, the Defense Ministry published its "Conceptual Views Regarding the Activity of the Armed Forces of the Russian Federation in the Information Space". The strategy discusses the principles of information security and different measures to control for interference in information systems. Section 3 of the strategy assesses different rules for deterrence and conflict prevention and resolution. In March 2012, the Russian Federation announced that it was considering establishing a cybersecurity command to secure information for the armed forces. In addition, the Government has drafted a bill to create an advanced military research agency for cybersecurity. The Military Doctrine of 2010 discusses the use of political and informational instruments to protect national interests and those of allies.

The Information Security Doctrine of the Russian Federation specifies that the fourth ingredient of the national interests of the Russian Federation in the information sphere comprises protecting information resources against unsanctioned access, and securing the information and telecommunication systems whether already deployed or being set up on the territory of Russia. Thus, it is necessary to:

- Enhance the security of information systems including communication networks, primarily the security of primary communication networks and information systems in the federal bodies of state authority, the bodies of state authority of the constituent entities of the Russian Federation, credit and financial, and banking spheres, the sphere of economic activity as well as the security of systems and means for informatizing weapons and military equipment, security of troop and arms control systems, and the security of management systems for environmentally hazardous and economically important enterprises;
- Intensify development of the domestic production of information protection hardware and software, along with the methods to control their efficiency;
- Secure data that constitute state secrets; and
- Expand international cooperation by the Russian Federation with respect to the development and secure utilization of information resources and counteraction against the threat of rivalry in the information sphere.

It describes the types of threat to the information security of the Russian Federation by explaining that "according to their general directionality. Of these types, it includes threats to information support to Russian Federation state policy; and threats to Russian information

industry (including informatization, telecommunication, and communication facilities) development, the satisfaction of domestic market requirements with its products and their entry into the world market, and the accumulation, storage reliability, and effective utilization of national information resources; as well as threats to the security of information and telecommunication systems and facilities whether already deployed or being set up on the territory of Russia.

The threats to the security of the information and telecommunication systems and facilities include:

- Illegal information gathering and use;
- Information processing technology violations;
- Insertion into hardware or software products of components realizing functions not envisaged by documentation for these products;
- Development and distribution of programs that upset the normal functioning of information, and information technology systems, including information security systems;
- Destruction, damage, disturbance of, or electronic attack against information processing, telecommunication and communication systems and means;
- Attacks on password key protection systems for automated information processing and transmission systems;
- Discretization of cryptographic information protection keys and means;
- Technical channel information leaks;
- implantation of electronic intercept devices into information processing, storage and transmission hardware via communication channels or into office premises of government bodies, enterprises, institutions or organizations under whatever form of ownership;
- destruction, damage, disturbance or theft of machine processible data carriers;
- interception of information in data transmission networks or on communication lines, deciphering of this information and foisting of false information;
- use of uncertified domestic and foreign information technologies, information protection means and informatization, telecommunication and communication facilities in setting up and developing the Russian information infrastructure;
- Unsanctioned access to information contained in databanks or databases; and
- Breach of the lawful restrictions on information dissemination.

The sources of threats to the information security of the Russian Federation are subdivided into external and internal.

Cyber-related policy opportunities and challenges for further consideration:

Russia should continue to closely consider possible cyber threats to oil and gas suppliers. Particularly since many global major oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. This could possibly cause damage but breaches may also cause high damage to corporate assets, public infrastructure and safety, or the wider economy. Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain.

Given the extremely high significance of the economy's energy sector both to Russia and to the world economy, Russia should continue to monitor cyber issues relevant to the oil and gas sector, the electric grid and the supply chain.

Regarding nuclear energy, in November 2009, the IAEA's Board of Governors adopted a resolution supporting a Russian initiative to establish and maintain in the Russian Federation a stock of low-enriched uranium, and to carry LEU supplies for the IAEA member states. This was a breakthrough in the establishment of an international system guaranteeing reliable nuclear energy plant fuel supplies and lowering the risks of the proliferation of sensitive nuclear technologies. One major concern for world energy development is nuclear safety, which has become a key agenda item after the Fukushima accident. Rosatom's long-term strategy up to 2050 involves moving to inherently safe nuclear energy plants. Construction of 35 reactors in 15 countries are in the pipeline, and seven countries have signed contracts for 19 reactors.

Given Russia's use of nuclear energy, the IAEA (as well as several nation states) provides guidance for consideration by states, competent authorities, and operators. The aim is to prevent the theft of material or sabotage of plants and facilities.

Specific public-private sector considerations relating to cybersecurity and the energy sector should also be carefully examined.

Regarding international efforts in this space, in May 2015 reports outline the signing of "a nonaggression pact in cyberspace" between Russia and China. Under the agreement, the reports note that the two economies have agreed not to hack each other. Both economies also pledged to thwart technology that might "destabilize the internal political and socio-economic atmosphere," "disturb public order" or "interfere with the internal affairs of the state." Additionally, both sides will exchange cyber threat data and information technology. In 2011, China and Russia, with Tajikistan and Uzbekistan proposed to the UN an international code of conduct for information security, followed by a multistate proposal in 2012 to give the ITU greater control over the internet.

At regional level, Russia is a participant of the ASEAN Regional Forum (ARF).

Focusing on prevention and resilience at a conference in 2012, Russian Ambassador Iklódy underlined the importance of protecting critical infrastructure, including from cyber-attack. He explained that the systems and networks that make up the infrastructure of society are often taken for granted, yet disruption to just one of those systems can have dire consequences across other sectors and disrupt the wellbeing of our societies. He continued that it is also impossible to protect all assets of critical infrastructure all the time. They therefore present clear vulnerabilities that various terrorist groups exploit, and effective protection against unconventional security challenges requires a major paradigm shift. He suggested that rather than focusing on defense and deterrence, increasing emphasis must be laid on prevention and resilience, in other words preparing societies, infrastructure, and so on, to receive the blow but then to recover from it quickly. According to this release, many participants agreed with this observation and the fact that the cyber threat to critical infrastructure seems to be ever increasing. There was also general agreement that risks to critical infrastructure need to be assessed in a dynamic way. The conference was organized under the NRC Action Plan on Terrorism, which provides overall coordination and strategic direction of NRC cooperation in this area.

Such illustrations of cooperation in dealing with threats from non-state actors are good examples of where more exchanges could be held among economies on CIP and cybersecurity matters. Regular exchanges of information, consultations, joint threat assessments, civil emergency planning for attacks, as well as dialogue on the role of the military in protecting CIP as well as lessons learned, and scientific and technical cooperation could be a good way in which to establish mutual action points.

Russia is participating in the fourth UN GGE (2014/2015), the fourth Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

6.15.5 Future Cybersecurity Nexus

There is insufficient data on this topic for Russia. This is a potential area of future growth.

6.15.6 Smart Grids

Given the interest in the smart grid, enhancing cybersecurity is essential and it should be more closely considered as part of a larger smart grid deployment strategy.

6.16 Singapore

6.16.1 Economy Energy Resources

APEC Expert Group meeting notes from the 43rd meeting on Energy Efficiency & Conservation in 2014 outline that Singapore's energy policy follows the "Trilemma approach". Singapore focuses on three critical aspects of energy supply: economic competitiveness, energy security, and environmental sustainability. The notes explain that the key challenge faced by Singapore is

a natural resource disadvantage that causes it to be an energy importer for most of its needs, and the small-urbanized geography limits the fuel sources that it can use.

6.16.2 Smart Grid Initiatives

The Intelligent Energy System (IES) is Singapore's smart grid system. It is testing and evaluating smart grid technologies and related applications. Since Singapore has a highly reliable electrical grid, its smart grid targets are slightly different than other economies and are geared towards addressing issues related to the high price of energy and distributed generation. The Intelligent Energy System provides consumers with choices in accessibility and flexibility. The key drivers include retail products and services, management of distributed energy resources, integration of electric vehicles, and integration of the outage management system. The consumer-side demand management includes residential and industrial consumers with time of use (TOU), smart systems, and demand response applications. The benefits include smoothing out demand, incentivizing consumers to manage energy usage, and reducing peak demand. The vision is to have a centrally managed intelligent communications network with interconnected smart grid technologies.

2014 reports say that investment in Southeast Asia will include smart metering and the modernization of electricity transmission and distribution networks with sensors, communications and software. By 2024, the largest markets will be Thailand, Indonesia, Malaysia, Singapore, the Philippines, and Viet Nam, according to a recent study by Northeast Group LLC.

Southeast Asian economies are just beginning on the path of modernizing their electric infrastructure. Electrification programs and growth in renewable resources will also drive investment. 2014 reports online also outline that some emerging economies, such as Thailand, Malaysia, Indonesia, and the Philippines, are making plans to deploy smart grid technology. While this region is currently behind other global regions in terms of smart meter deployments and regulatory frameworks, its smart grid market is growing. There are already smart grid pilot projects in several economies throughout the region. By 2022, Southeast Asian economies will likely have an electricity demand profile similar to Latin American economies where large-scale smart meter deployments already exist. The region's current electricity consumption rates are among the lowest in the world, while distribution loss rates are comparatively moderate, offering less short-term savings potential compared with other global regions. Additionally, regulatory frameworks remain largely undeveloped in the region. Even in the more advanced economies, deployments are still at the initial pilot level.

This Northeast Group study finds that Singapore is leading the region in development but later in the decade, the large markets of Thailand, Indonesia, Malaysia, Viet Nam, and the Philippines will account for significant smart grid investment. Several economies in the region have drafted smart grid roadmaps and pilot projects are widespread. Regulatory frameworks are

still developing but momentum will grow over the next several years. Both utilities and vendors are already working together to ensure preparedness when regulations are finalized. Many vendors are active across the region (these include ABB, Alstom, Echelon (NES), EDMI (Osaki), Elster, Enverv, GE, Itron, Schneider, Secure, Siemens, Silver Spring Networks, ST Electronics, Trilliant and other global and local vendors).

According to the APEC Energy Overview Report of 2014, Singapore under Strategy 2 (Enhance Infrastructure and Systems) of the 2010 ESC Subcommittee report on Ensuring Energy Resilience and Sustainable Growth, is investing in critical energy infrastructure ahead of demand. Enhancing existing infrastructure has helped to make its energy markets more efficient, open new areas for economic development and strengthen energy security.

The Agency of Science, Technology and Research (A*STAR) set up the Experimental Power Grid Centre (EPGC), a program that undertakes R&D activities in areas such as intelligent and decentralized power distribution, control and management of distributed energy resources, and smart and interactive energy utilization. It features a 1 MW experimental power grid, which is designed to create various power network configurations at near grid-like conditions. This facility acts as a platform for researchers, industry and public agencies to develop energy technologies before bringing them to larger-scale test beds or commercialization.

The Energy Market Authority describes Singapore's Smart Community Projects as including: Clean Tech Park (Industrial); Pulau Ubin micro grid test bed; Punggol eco town (residential); Jurong Lake District (business & leisure); and EV test bed (transport).

Key drivers cited include: enabling the management of distributed energy resources including renewable and embedded generation; enabling the integration of new initiatives such as demand response and energy efficiency applications; and supporting the needs of Electric Vehicles. The IDA (the Infocomm Development Authority of Singapore) is cited as responsible for policy and standards; and ADSC and A*Star for security.

A 2011 report from the National Climate Change Secretariat and National Research Foundation on smart grid technology explains that over the years, Singapore Power Group's SP Powergrid Division has been building up its efforts to progressively adopt smart grid technologies, such as self-monitoring and online condition monitoring for network assets using network wide sensors, network mesh topology, adaptive protection schemes and semi-automated self-healing network restoration features. There are also various monitoring and management systems in place in Singapore such as the Electricity management System (EmS), gas monitoring System (gmS), interruptible load (il) monitoring System and distributed generator (dg) monitoring System. These systems include real-time components that enable remote monitoring and control of various elements of the electrical system from generators to loads in the high voltage network.

This report describes the electricity grid as amongst the most reliable and robust in the world with intelligent systems already installed in the generation and transmission network. It highlights that the grid performance of Singapore's electricity network far exceeds that of other cities and economies. Network losses are reported to be only around 3 percent.

The current grid in Singapore is described as already smart by the report, but the grid still employs conventional grid technologies, and the last-mile distribution network could be upgraded to meet: 1) continued growth in demand; 2) the integration of increasing number of variable renewable energy sources and electric vehicles; 3) the need to improve the security of supply; 4) facilitate full retail competition; and 5) enhance delivery of electricity through better communication with households and businesses. This is part of the premise of the Intelligent Energy System pilot, which tests technologies which will be useful in meeting these objectives.

Singapore's electricity grid consists of more than 20,000 km of underground cables interconnecting more than 9,800 substations in the transmission and distribution networks. Intelligent systems are installed in the upstream transmission and distribution systems. Future intelligent systems need to be installed in the last-mile connections and distributed generation (dg) integration systems. The existing grid may have to be upgraded to support greater integration of distributed generation, such as renewable sources.

Smart grid technology research and test-beds in Singapore will enable the implementation of:

A. Advanced metering infrastructure (ami) and demand response as key enablers of consumer-focused grid management;

B. Integration and control of distributed generation and renewables into the grid; and

C. Integration of EV charging infrastructure into the grid.

The report notes that although potential for renewable energy generation may be limited locally in the early years, a demonstration of grid integration capabilities will allow Singapore to emerge as a key technology provider for renewable energy integration systems worldwide.

Singapore appointed Accenture for phase 1 of the iES pilot project. It is working with its selected partners including ST Electronics (info-comm Systems), Oracle, and Hewlett Packard.

The Experimental Power Grid Center (Epgc) has a vision to lead in ushering new technologies for intelligent and decentralized power distribution, interconnection and utilization for Singapore. Epgc contributes to scientific and economic development through collaboration with industry, universities and public agencies to develop new technologies to be implemented both locally and worldwide. Epgc's diverse pool of researchers provides a multi-disciplinary approach to solving complex energy-related problems. It participates in this whole-of-government approach and contributes towards the national agenda of increasing energy resilience through the

enhancement of the energy infrastructure, and supports Singapore's efforts in becoming a "living lab" for new technologies.

Regarding the Pulau Ubin Intelligent Micro-Grid Project, the report notes that many remote areas in the world still lack proper access to electricity and it explains that one major reason is the lack of economic viability to lay power transmission cables due to the modest demand of these remote areas. EMA has embarked on a test-bedding project to develop an intelligent micro-grid infrastructure with clean and renewable energy technologies on Pulau Ubin (Pulau Ubin is a small island), and there is potential for the micro-grid model to be exported and implemented in other remote areas of the region, through rural electrification projects.

In 2014, Singapore Power won the 'Smart Grid Project of the Year' award at the Asian Power Awards 2014 for its program with Silver Spring Networks to deploy a smart infrastructure networking platform with nation-wide coverage. Articles argue that utilities across Asia can look to Singapore Power as a best practice example for how to deploy smart grid services.

The Energy Innovation Program Office (EIPO) has awarded research grants to six research projects focused on smart grid technologies, which focus on reliability and resilience, energy analytics, and control systems, among others.

Singapore is a member of ISGAN.

6.16.3 Current Cybersecurity Nexus

Singapore's cybersecurity initiatives are developed through its cybersecurity Infocomm Security Masterplan I and II (ISMP I and ISMP II). The cybersecurity awareness raising aspect of ISMP I (2005-2007) was a series of outreach programs targeted at the general public and at the private sector. These programs raised awareness about the risks of ill-informed online activities and encouraging organizations to devote sufficient attention and effort in the security upkeep of their information systems. The Government also worked with the various infrastructure owners and operators to ascertain the adequacy of their cyber protection measures, and assessed the adequacy of cybersecurity in the public sector through a series of tests.[8]

ISMP II (2008-2013) built on ISMP I. Its key approach was to ensure that awareness raising and outreach activities are conducted collaboratively by like-minded partners from the public and private sectors. Government and industry formed the Cybersecurity Awareness Alliance. This alliance seeks to build a positive culture of cybersecurity in Singapore, in which users adopt essential security measures such as firewalls and anti-virus software, and encourage the adoption of essential security practices by the public and the private sector.

Defining critical infrastructure protection

[8] APEC Cyber Security Workshop

The National Security Coordination Centre National Security Strategy in 2004 explained in a sub-section on the Protection of Critical Infrastructure and Key Installations that since the September 11 attacks that the Government has enhanced the security of Singapore's critical infrastructure. It instituted a range of security measures at power stations and water networks. A National Critical Infrastructure Assurance Committee formed to study the vulnerabilities of Singapore's critical infrastructure, and to recommend the protective steps to take. On Jurong Island, the site of Singapore's petrochemical hub, Singapore deployed armed personnel, including Singapore Armed Forces (SAF) troops, to increase security.

In 2009, an inventory study on CIIP in various countries found that the new security threats that have emerged in the post-September 11 era emphasize the need for closer cooperation between the military and home front agencies in Singapore. Immediately after the attacks in the United States in 2001, the home front agencies undertook a review of the vulnerabilities and strengths of Singapore's national critical infrastructures from the following sectors: Banking and Finance; Information- and Telecommunications; Energy; Water; Transportation; and Health. Since 2002, the critical infrastructures of these six sectors have been reviewed and assessed, and remedial plans implemented. However, infrastructure protection policies in Singapore have expanded to the following sectors: Food Supply; Aviation Security; and Maritime Security. Even though these sectors have been at the focus of the most recent efforts to prevent terrorism, they do not represent the totality of Singapore's critical infrastructure. Other sectors may well be included in future protection efforts.

The Infocomm Development Authority of Singapore (IDA) under the guidance of the National Infocomm Security Committee (NISC) leads the (third five-year) National Cyber Security Masterplan 2013-2018 (July 2013). It aims to strengthen resiliency against cyber threats through the enhancement of critical infrastructure with the Cyber Watch Centre (CWC) and Threat Analysis Centre (TAC).

The Monetary Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines and Notices (June 2013) is a mandate for financial institutions to ensure monitoring and swift detection of IT incidents. Financial institutions are to report discovery of any IT security incidents within one hour to MAS.

The Computer Misuse and Cybersecurity Act (March 2013) allows the Government to take more effective, timely and proactive measures against cybersecurity threats.

A presentation at the APEC Counter-Terrorism Working Group Workshop in October 2014 on Singapore's Approach to Critical Infrastructure Protection describes the Ministry of Home Affairs (MHA) Counterterrorism Strategy in terms of five layers: 1) Intelligence and International Cooperation; 2) Border Security; 3) Target Hardening; 4) Community Involvement; 5) Crisis & Consequence Management. The third layer, target hardening, is for "at risk

infrastructure" which includes: 1) critical infrastructure; 2) high profile targets; 3) crowded/soft targets; and 4) SSM-related targets.

Critical Infrastructure is the physical infrastructure and assets that are vital to the continued delivery of the essential services upon which Singapore relies, the loss or compromise of which would lead to a debilitating impact on security, economy or public health and safety". The Critical Infrastructure Program (CIP) is the overarching framework for protection of Critical Infrastructure. Objectives include: identify and prioritize CIs; protect and prepare CIs against relevant security threat scenarios; and enhance robustness and resiliency of CIs.

Key Principles of CIP include: protection requirements should be risk calibrated; criticality of infrastructure should guide resource prioritization; CI protection is part of the multi-layered approach; and strong tripartite relationship among Government, Sector Leads and Owners.

Roles & Responsibilities are:

> State: Formulate protection policies and programs; coordinate efforts across Sectors to raise protection level; Work with stakeholders to identify and prioritize CIs; develop standards and guidelines.
>
> Sector: Develop and implement sector-specific protection plans; identify critical facilities, assets and functions for the sector; work with private operators to mitigate threats; conduct exercises to ascertain adequacy of plans & measures.
>
> Asset: Work with Sector Lead to improve security of CI; implement appropriate measures to mitigate vulnerabilities; develop and implement BCP & Contingency Plans.

CI Protection is a Risk-based Approach. The steps are: 1) Set security objectives; 2) Identify critical assets & functions; 3) Identify relevant threats; 4) Identify vulnerabilities; 5) Assess Risk; 6) Prioritize; 7) Mitigate vulnerabilities; and 8) Evaluate effectiveness. This is on a "Review & Monitor (feedback loop)" basis.

Understanding interdependencies is increasingly important for prioritization and protection of CIs. Interdependency Study includes: identify interdependencies and vulnerabilities; uncover concentration risks; and enhance contingency planning and response capabilities.

Policies and measures to enhance protection are described, the first of which is Security-by-Design. This has been a key thrust of the Singapore approach to target hardening since 2006. There is a process requirement to factor in security considerations upstream. It is a threat dependent and outcome based approach.

Operational Measures include high visibility patrols at "at-risk" establishments and high threat locations; Formation of Transport Security Command; and Public Camera Zones (PCZs).

Partnering the Community is listed as including Safety & Security Watch Groups (SSWGs) so as to promulgate good security practices and facilitate sharing of information. This is described as a clustered concept and membership is voluntary. "Singapore takes a risk-based, multi-agency and collaborative approach towards CI protection."

Defining cybersecurity

According to the 2015 ITU country report, legislation on cybercrime has been enacted through the Computer Misuse and Cybersecurity Act (Chapter 50A). "Instruction Manual (IM) 8" specifies government policies, standards, regulations and codes of practice for IT security implemented by government agencies, with which private vendors serving the Government should also comply. All IMs are mandatory for compliance by government agencies and subject to regular audit and assessment for enforcement purposes. Singapore's national CERT is SingCERT. For the Government sector, the Government IT Security Incident Response (GITSIR) team coordinates with government agencies to perform investigations and supports agencies' response to incidents. SingCERT actively engages international counterparts through platforms such as APCERT; FIRST; and the ASEAN CERT Incident Drill (ACID). It is also a participant in the Japan-led TSUBAME Working Group and PRACTICE (Proactive Response Against Cyber-attacks Through International Collaborative Exchange) Project. Internationally recognized cybersecurity standards (such as ISO27000 series) are referenced in the development of Government security policies and standards. For the telecommunications sector, internationally recognized cyber security standards (such as ISO27011) are referenced in the development of the Secure and Resilient Internet Infrastructure Code of Practice. Cybersecurity professionals are encouraged to obtain international certifications such as CISSP and the SANS series of certification. The Association of Information Security Professionals (AISP) aims to transform Infocomm security into a distinguished profession, with a recognized body, qualifications, established career paths and career development programs. The National Cyber Security Masterplan 2018 (NCSM2018) was developed through a multi-agency effort led by IDA and it provides the overarching strategic direction to help Government and organizations in strengthening resilience against cyber threats. It aims to raise the awareness and adoption of cybersecurity best practices.

The factsheet further outlines that the National Infocomm Security Committee is the national-level inter-agency committee responsible for steering cybersecurity strategy and policy in Singapore. The IDA provides Secretariat support. The National Infocomm Security Committee draws its members from the senior ranks of relevant public sector stakeholders. The Singapore Infocomm Technology Security Authority oversees network security. This agency operates under the Internal Security Department of the Ministry of Home Affairs. IDA's Infocomm Security Health Scorecard measures the level of security readiness, assesses the state of info-security health of government agencies in areas such as policies, standards, the security knowledge of public officers, as well as physical and environmental security. The scorecard

helps government agencies to improve their info-security strategies and processes. The Cybersecurity Awareness Alliance amalgamates efforts from its members by bringing together different strengths and resources, to build a culture of cybersecurity in Singapore and to promote and enhance awareness and adoption of essential Infocomm security practices.

According to the 2013 UNIDIR Cyber Index, Singapore amended the Computer Misuse Act in 2012 to help the Government counter cyber-attacks. The amendment gives the Government the ability to order an organization to act against a cyber-attack before the attack happens.

The 2014 ASPI report on cyber maturity finds that the Singaporean public is highly networked and very aware of cyber issues.

The IDA has led the ASEAN CERT Incident Drill since 2006. The authority has also signed information-sharing agreements with government organizations in other advanced economies. The agreements also allow joint training and development opportunities. SingCERT has been active in organizing and hosting ASEAN and APCERT exercises. Singapore hosts seven FIRST members.

The Cyber Security Agency (CSA) of Singapore, launched in April 2015, provides centralized oversight of Singapore's national cybersecurity functions, and focuses on engagement and partnership to ensure the holistic development of Singapore's cybersecurity landscape.

6.16.4 Cybersecurity Challenges (Issues)

- In May 2013, a report by Trend Micro Smart Protection Network showed that over 900 Singapore citizens were victims of online banking fraud in the first quarter of 2013.
- A*STAR has identified issues with NISTIR 7628, which applies to EV charging. They indicate that the standard has some holes that hackers can exploit.[9]

According to the IDA Factsheet on the NCSM2018, this five-year plan will continue to reinforce Singapore's cybersecurity by intensifying efforts in the Government and Critical Information Infrastructure (CII) as well as the wider infocomm ecosystem, which includes businesses and individuals. IDA developed it through a multi-agency effort under the guidance of the National Infocomm Security Committee.

The vision is for Singapore to be a "Trusted and Robust Infocomm Hub" by 2018. It aims to engender a secure and resilient infocomm environment and a vibrant cyber security ecosystem. The three key areas of NCSM2018 are to: 1) enhance the security and resilience of critical infocomm infrastructure; 2) increase efforts to promote the adoption of appropriate infocomm

[9] http://www.smartgridnews.com/artman/publish/Technologies_Security/Smart-grid-security-alert-Singapore-scientists-find-gaps-in-NIST-standards-5817.html

security measures among individuals and businesses; and 3) grow Singapore's pool of infocomm security experts.

The NCSM 2018 Masterplan "Brochure" identifies specifically that, under its focal area of critical infocomm infrastructure, it aims to harden systemically the infocomm systems of critical infrastructure so that they will have a high level of security and resilience against increasingly sophisticated cyber-attacks.

As part of the continuous effort to enhance the protection of CII and improve cross-sector response to mitigate widespread cyber-attacks, the Government will work closely with critical sectors on cybersecurity exercises as well as for high priority critical infrastructure to be assessed for vulnerabilities and ensure that security capabilities and measures are in place to mitigate cyber threats.

The Critical Infocomm Infrastructure Protection Assessment program aims to assess the security of the infocomm systems that are critical to the operation of critical infrastructures in Singapore. Building upon the previous Masterplan, the Government will expand its effort and collaborate with additional critical sectors to ensure high priority CII in each sector remains secure and resilient.

The National Cyber Security Exercise program aims to enhance the readiness and responsiveness to significant cyber-attacks at the national level. It is comprised of exercises conducted within critical sectors to assess the operators' capability and readiness. New cross-sectors exercises will improve the overall resilience of national infrastructure and services.

As part of the continuous efforts to enhance the security and resilience of its infocomm infrastructure, and public sector capabilities, the Government will focus on proactive defense in-depth to mitigate increasingly sophisticated attacks. Such attacks have made the task of threat prevention even more challenging. This includes upgrading of existing detection and analysis capabilities and strengthening preventive and recovery measures at the Whole-of Government level.

The enhanced Cyber Watch Centre (CWC) will provide a wider range of detection capabilities for government agencies with improved correlation capabilities. Apart from continuing to provide and manage security monitoring services for the Government, supported by tested procedures and advanced monitoring technology, the enhanced CWC will leverage tools that are more advanced and techniques to improve the overall security monitoring effectiveness for the public sector.

The enhanced Threat Analysis Centre (TAC) will leverage analytical tools to assess larger volumes of data from a wider range of sources and to identify cyber threats with greater accuracy

and efficiency. This will enable public agencies to receive detailed cyber threat analysis, threat advisories and recommendations and take preventive actions in a timely manner.

The NCSM-2018 Brochure delineates that the Critical Infocomm Infrastructure Security Assessment (CII-SA) appraises the infocomm security readiness of Singapore's Critical Infocomm Infrastructure (CII) and ascertains the adequacy of infocomm protection measures, implemented by infrastructure owners and operators.

The Secure and Resilient Internet Infrastructure Code of Practice (SRII-CoP), aligned with international standards and best practices, has been issued by IDA to designated ISPs. The Code of Practice is incorporated into the telecommunications regulatory framework and sets specific security controls and outcomes to ensure that essential security to mitigate current and emerging cyber threats. IDA conducts periodic audits to ensure that ISPs observe the Code of Practice.

Current efforts will be reinforced to raise infocomm security awareness and adoption amongst users and businesses. This includes the Cyber Security Awareness and Outreach program to augment existing outreach channels (e.g. via online and social media platforms, educational talks, road-shows, seminars, and print advertisements) and explore new avenues that offers wider coverage and reach to users, such as broadcast media.

The NCSM2018 will also include efforts to facilitate information sharing between the Government and private sector, as well as collaborate with industry and trade associations to promote cybersecurity and exchange of threat information.

It outlines that the threat posed by rising cyber-attack sophistication is exacerbated by the shortage of cybersecurity experts. A stronger presence of cybersecurity professionals will put Singapore in a better stead to defend against sophisticated cyber threats and to retain cybersecurity talent given the global shortage and high demand for them. The NCSM2018 will look into developing human and intellectual capital within the infocomm industry to boost cybersecurity in Singapore.

The Defense Science & Technology Agency (DSTA) explains on its site that the physical and cyber infrastructures of Singapore's key installations require protection from external threats. To evaluate the level of protection needed, a systematic vulnerability assessment is required. A multi-disciplinary DSTA team has therefore adapted the Critical Infrastructure Vulnerability Assessment (CIVA) methodology and applied it to assess a key army infrastructure. DSTA is working with the SAF to apply the methodology to other key SAF assets and newer infrastructures using the overarching critical infrastructure protection framework. The methodology provides a way for DSTA to assess a wide range of threats and realize critical infrastructure protection capabilities for the SAF. The Cybersecurity Program Centre develops advanced cyber defense solutions to provide protection and detection, threat sensing and incident

response, as well as trusted vetting and audit capabilities for the Ministry of Defense (MINDEF) and SAF.

The 2014 ASPI report on cyber maturity finds that Singapore has a very strong cyber governance structure, including accompanying legislation that covers both computer misuse and CNI protection. Singapore is very active in international cyber forums and has a very capable CERT team. The military has also established a hub for defending defense networks. Business–government dialogue is very strong. It notes that the National Cyber Security Centre (NCSC) headed by SITSA is likely to enhance Singapore's capabilities in the early detection and prevention of cyber attacks.

It finds that Singapore has successfully implemented legislation, such as the Computer Misuse and Cybersecurity Act, to prevent and respond to cyber issues, including cybercrime and hacking. However, the regulations include provisions that allow the Government to compel organizations to disclose data to the Government for the purpose of pre-emptive cybersecurity. The report finds that Singapore scores highly for its involvement in technical information exchange, anti-cybercrime collaboration and CERT engagement. The SAF have established a Cyber Defense Operations Hub, aimed at protecting domestic military networks. This indicates that there is an awareness of cyber risks and that work is underway to address them. However, there is no publicly available SAF strategy or policy on how the armed forces will engage with cyber threats.

It finds that Singapore has a strong relationship with its CNI providers and private sector engagement is a key aspect of its NCSM.

Singapore has held roundtable, most notably in 2014, on "cyber security in the energy sector" where experts discussed "cyber-attacks" specifically targeted at the global energy sector, namely, the oil, petrochemicals, power generation sectors, as well as intelligent energy systems and smart grids.

In October 2014, A*Star announced new initiatives that contribute towards Singapore's Smart Nation vision, including new partnerships across public and private sectors to strengthen Singapore's capabilities in cybersecurity, energy and transport. A*STAR also announced collaboration agreements between I2R and its partners across regulatory agencies and the private sector to build a greener and safer Smart Nation.

Four new research collaborations were unveiled at ICM Horizons 2014, an annual infocomm technology event hosted by A*STAR's Institute for Infocomm Research (I2R). The event was themed "Innovating for a Smart Nation" and co-organized with the IDA.

A*STAR and IDA signed a Master Research Collaboration to develop innovative technologies in Data Analytics, Cyber Security and Heterogeneous Networks (HetNet). These capabilities will

play crucial roles in providing insights, security and connectivity for citizens, businesses and the government in a Smart Nation.

I2R and ST Electronics (Info-Security) will set up a joint laboratory collaboration to develop advanced security and forensics solutions to enhance the infocomm structure in Singapore. The partnership will support cybersecurity for the nation by developing solutions to prevent cyber threats and attacks. In addition, I2R is setting up a Cyber Security Research Centre.

Renewable energy systems: HDB, I2R, Singapore Power and Narada signed a Memorandum of Understanding to develop energy storage systems for solar-generated power, which will power HDB residences or supply electricity back to the grid. The collaboration will also lead to the development of reliable grid-scale energy storage systems for renewable energy supply.

Intelligent Transport Systems: I^2R, Continental and TUM CREATE have established a joint laboratory to research, study and test-bed a range of communications, information and automotive innovations that improve the safety, efficiency, and performance of transport systems in Singapore.

Urban Mobility Research Centre: A*STAR launched the Urban Mobility Research Centre @I^2R, or UMRC@I^2R. The new center brings together A*STAR's multi-disciplinary research in urban mobile technologies for its Intelligent Transport Systems and Autonomous Vehicle program. The center will function as a one-stop platform for close partnerships and collaboration with government agencies such as the Land Transport Authority (LTA), IDA and the industry.

The CSA focuses on: 1) engagement and outreach - nurturing ties with local and global industry and thought leaders, heightening cybersecurity awareness through public outreach programs, and promoting security-by-design; 2) industry development – developing a robust cybersecurity ecosystem, in other words a vibrant industry equipped with the manpower to respond to and mitigate cyber-attacks; 3) protecting critical sectors – strengthening cybersecurity in critical sectors, such as energy, water, and banking; and 4) operations – ensuring effective coordination and deployment in our response to cyber threats.

Several cyber-related policy opportunities and challenges for further consideration:

Greater connectivity in the region could raise the probability of transnational crime and cross-border cyber-related incidents. With increasing access to high-speed networks, low-level cybercrime has already risen in the ASEAN region. In Asia, policy experts further suggest that the growth of cybercrime could increase instability. Misappropriation of responsibility could lead to misunderstandings and the possible escalation in tensions or conflict because the accurate identification of those responsible for a cyber incident is not always easy (especially since there is now a wide range of varying threats that may also come from different non-state actors).

Given the economy's pipelines and refineries, Singapore should continue to consider possible cyber threats to oil and gas suppliers particularly since many major global oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. This could possibly cause damage but breaches may also cause high damage to corporate assets, public infrastructure and safety, or the wider economy. Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain. Singapore should therefore continue to monitor cyber issues relevant to the electric grid as well as the supply chain.

Regarding international efforts, at the regional level, Singapore is a member of ASEAN and a participant at the ASEAN Regional Forum (ARF).

The NCSM-2018 "Brochure" specifies that the significance of the Meridian Process. It explains that Singapore is a regular participant in the annual Meridian Conference. The conference is a major program of the international Meridian Process, which aims to: build trust and establish international relations with senior government policy makers for Critical Information Infrastructure Protection; share strategic approaches and experiences in CIIP from around the world; and explore benefits and opportunities for cooperation between governments. The Meridian Process provides Governments worldwide with a means by which they can discuss how to work together at the policy level on CIIP.

It also explains that Singapore is an active participant in ASEAN-Japan engagements that range from awareness and outreach, policy research, information sharing to operational co-operation among CERTs/CSIRTs. These engagements are anchored by two annual events, namely the ASEAN-Japan Information Security Policy Meeting and the ASEAN Japan Government Network Security Workshop in which Singapore participates. The Policy Meeting is the platform for deliberation on strategic issues while the Workshop is primarily used to discuss initiatives for collaborations such as the annual Cyber Security Awareness Month. Singapore is a member of the Proactive Response Against Cyber-attacks. Through International Collaborative Exchange (PRACTICE) project, led by the Ministry of Internal Affairs and Communications of Japan, that is trying to establish a global monitoring and analysis framework to protect users from malware infection and malicious activities in cyberspace. Other Japan-led initiatives included the TSUBAME Project, an internet threat monitoring system, and the annual Communications Check Exercises to build closer relationship between ASEAN member states and Japan as well as establish more effective information sharing processes to aid decision making for policy makers. SingCERT represents Singapore in both initiatives. In 2013 and 2014, SingCERT also participated in a Japan-led Communications Check Exercise, to build better relationships between ASEAN member states and Japan, and establish more effective information sharing processes to aid in decision-making for policy makers.

6.16.5 Future Cybersecurity Nexus

There is insufficient data on this topic for Singapore. This is a potential area of future growth.

6.16.6 Smart Grids

Given the interest in the smart grid, enhancing cybersecurity is also essential and should be closely considered as part of a larger smart grid deployment strategy. This is especially true if Singapore decided to export its successful smart technology models.

6.17 Chinese Taipei

6.17.1 Economy Energy Resources

According to the APEC Energy Overview Study published in March 2014, Chinese Taipei has very limited domestic energy resources and relies on imports for most of its energy requirements. There are no coal reserves in Chinese Taipei, but the economy has oil and gas reserves of around 2.4 million barrels and 6.23 billion cubic meters respectively. In 2011, installed electricity generation capacity totaled 41.67 gigawatts. Traditionally, Chinese Taipei is forced by a lack of domestic energy and mineral resources to import nearly all of its energy requirements, with imports accounting for 97.8 percent of its primary energy supply in 2012.

6.17.2 Current Cybersecurity Nexus

Defining critical infrastructure protection

According to an October 2014 presentation on developments in infrastructure protection by Chinese Taipei's Office of Homeland Security (OHS), the National Security Council is responsible for: intelligence, technology, natural disaster reduction, counterterrorism and CIP, and CIIP. The National ICT Taskforce, Office of Information and Communication Security, and Information and Communication Security Technology Centre are involved in CIIP. The Homeland Security Policy Taskforce shares responsibility with OHS for CIP.

The main tasks of the OHS include counter-terrorism, a CIP project, and international coordination and cooperation. The 2014 CIP project's goals are to: a) build a safer, reliable and resilient society; b) prevent, deter, defuse and reduce all threats from natural disasters or manmade attacks on specific major infrastructures; and c) strengthen national abilities of prevention, preparedness, emergency response, and rapid recovery for natural disasters, terrorist attacks or other emergencies. Its strategies are to: 1) collaborate with the private sector and establish joint protection mechanisms; 2) take stock of critical infrastructure and develop protection plans; 3) manage risks for all hazards; and 4) assemble protection resources and maintain government operations. Infrastructure is classified as critical if: 1) the sector is collectively determined by experts and officials based on extensive research; 2) each sector is further divided into sub-sectors depending on its nature and characteristics; and 3) critical

elements are identified. This refers to equipment, operating communications, information, and security systems that are essential to sustain functioning.

Eight critical infrastructure sectors are outlined in the OHS presentation: Energy, Water, Communications/Broadcasting, Government, Emergency Rescue/Hospital, Science Park, Banking/Financial, and Transportation.

It defines critical infrastructure as representing the physical and virtual assets, production systems and networks in the public and private domains that are so vital that impairment or destruction of such infrastructure from man-made or natural causes would impact the operations of government and society, result in losses of life and property, cause economic decline, alter the environment, or harm national security or other interests.

The principles for identifying critical infrastructure include if it can: 1) affect the major missions or functions of a government agency; 2) directly or indirectly affect a large portion of the population; 3) directly or indirectly result in economic losses; 4) can directly or indirectly affect the functioning of other critical infrastructure; and/or 5) is classified as mid-or high-level information systems in the information system classification, grading and assessment mechanism reference manual.

OHS outlines that each agency must adopt appropriate mechanisms to protect against "intolerable" threats. It must also manage an internal control system and perform a self-assessment to identify any flaws in that system. Agencies should each hold their own drills periodically to verify whether they can effectively control every type of threat and whether their prevention plans indeed limit losses from disasters and facilitate quick recovery. In 2014, Chinese Taipei conducted simulations of all-hazard disasters to test three selected types of CIP.

A more flexible method of testing will be needed over the longer term to accommodate the scopes, risk sources and risk analyses of all the different sub-sectors. OHS suggests that when sector/sub-sector critical infrastructure elements are similar in nature—making it easier to develop an accountability system — the sectors should set up councils to coordinate resources among sub-sectors and integrate protection capabilities. The sector/sub-sector classification scheme will require additional modification since it does not currently cover every type of critical infrastructure.

Future plans include: strengthening partnerships by developing a council mechanism for coordinating sectors; engaging in international exchange and cooperation; encouraging participation of local governments and private organizations; studies and legislating for regulations or laws relevant to CIP; innovating risk management by implementing systems for exercises, evaluation and examination; encouraging companies to set up internal compliance programs; promoting resource sharing among government agencies and private sectors; and technology studies and research for risk assessment and sector interdependency.

Defining cybersecurity

According to a draft APEC 2013 discussion document on cyber security submitted by Chinese Taipei, the goals of the Government Information Sharing and Analysis Center (G-ISAC) are to integrate the power of the Government and private sectors, and establish the cybersecurity information sharing and analyze capabilities of the Government agencies and key information security organizations.

The Chinese Taipei Research, Development and Evaluation Commission (RDEC) has operated G-ISAC since 2009. RDEC has invited the Government established ISACs and private industry SOCs such as Government Service Network, Ministry of Education (A-ISAC), National Communications Commission, Ministry of Economic Affairs (EC-CERT), National Police Agency, Ministry of Interior, and Chuinghwa Telecom (SOC Division) to join G-ISAC. By 2013, it had held eight G-ISAC Member conferences to enhance and improve the operating of G-ISAC.

The members of G-ISAC cover approximately 3,000 government sectors. The G-ISAC uses Incident Object Description Exchange Format (IODEF) as the standard exchanges data format, constructs over 45 information security incident type formats and system automation for members to better exchange, analyses, and handle information. During 2012, G-ISAC members exchanged 144,079 information incidents, including 41,895 network attack incidents, 893 Botnet incidents, and 40 Command and Control incidents. REDC wants to extend opportunities in the future using the G-ISAC platform to share cybersecurity information with other international cybersecurity organizations.

According to this draft submission, information security incidents in recent years have indicated the urgent need to improve system and network security. In order to prevent hacker intrusion and further information security events, TWCERT/CC aims to safeguard security and share its experiences of dealing with network security incidents with other national CERTs. Its goals have included: 1) prevention of possible incidents by providing an incident response channel as well as a prevention mechanism for victims to avoid similar events occurring again; 2) handling of real-time incidents by offering an immediate warning and defense force to effectively prevent incidents; and 3) recovery support to reduce damage and protect network security. It provides consultations for incidents and supports recovery operations to reduce damage.

In order to promote network security and reduce damage from intrusion, TWCERT/CC is committed to strengthening security services, publishing latest security issues, providing security documents/tools, vulnerability patch information, and security related documents. It is also actively developing attack/defense technologies.

TWCERT/CC has joined FIRST and APCERT, and acts as the contact point for international coordination in Chinese Taipei. By participating at international forums and conferences,

TWCERT/CC has exchanged security intelligence with emergency response centers and established a transnational defense system to handle international security incidents.

According to a 2013 Jamestown policy brief, there are three major institutional actors in Chinese Taipei's cyber defense infrastructure: NSB, MND, and the Criminal Investigation Bureau. There are currently three units under the MND's Information and Electronic Warfare Command, which was established in 2004, and include 3,000 military personnel who are responsible for countering cyber-attacks. It is reportedly developing a fourth cyber warfare unit to beef up its cybersecurity capability. The lead unit in NSB with the cyber portfolio is the Office for Sci-tech Intelligence and Communication Security. Chinese Taipei has plans for nationwide multi-agency exercises to simulate how the Government would respond in the event of a cyber-attack. The National Information and Communication Security Taskforce (NICST), which was established in 2001, acts as another agency coordinating group for civilian cyber defense and overall situational awareness.

6.17.3 Cybersecurity Challenges (Issues)

According to a 2013 APEC submission by Chinese Taipei, its commitments include countering terrorism by implementing and enhancing CIIP and cybersecurity to ensure a trusted, secure and sustainable online environment. In addition, commitments include enhancing mutual cooperation on countering malicious online activities and engaging in efforts to increase cybersecurity awareness.

Measures undertaken, amongst others, include: 1) effectively identifying what cyber terrorists want to do in cyberspace and how to deal with such activities; 2) the Criminal Investigation Bureau, N.P.A., implementing through the Criminal Investigation Bureau, N.P.AP, a "Working Platform of Cyber Crime Prevention Technology", and hosting conferences to study how to deal with using records; 3) commissioning a research project on regulating of cyber platform providers on retention of internet use records to assess a possible revision of laws (for example: the Telecommunications Act or Communication Security and Surveillance Act); 4) assisting in investigations on the use of domestic servers as a "gangplank" to hack other web servers by the CIB appointing a specific contact point; and 5) establishing of an automated data exchange mechanism among A-ISAC (ISAC for educational networks), G-ISAC (ISAC for governmental networks), and the top 6 domestic ISPs in order to ensure timely responses to cyber incidents.

In order to verify preparedness against cyber-attacks, Chinese Taipei conducted several tabletop exercises on the electricity and telecom industries in 2011. A website backup system and different business systems were established in 2011 to prevent a possible breakdown caused by unexpected disasters. Chinese Taipei also organized security training courses related to e-mail systems and held information security drills on a regular basis to enhance staff competence. Chinese Taipei outsources information security monitoring each year and it has apparently built

up external intrusion and internal abnormality monitoring systems, anti-virus firewall, hardware-based web AP firewalls, and other safeguards to block external attacks.

According to this 2013 APEC submission by Chinese Taipei, future relevant measures planned include, amongst others, trying to predict what terrorists want to do in cyberspace to: a) support their information and military activities, but not directly through an attack; and b) use cyberspace as a means of attacking other targets. The measures planned include tracing the routes of cyber terrorists and cutting the connection of the botnet they built, and securing sensitive targets, both organizations and individuals.

Regarding capacity building, Chinese Taipei believes its ability to implement its commitments to combat cyber terrorism would be strengthened by international cooperation on cross-national judicial issues. It has previously called for international cooperation through APEC to address cyber terrorism. It would like to see "communication meetings" to enhance the cooperation of all APEC members on counter cyber terrorism tasks. Technical training courses to keep up with the evolution of cyber terrorists' attack techniques are mentioned.

According to the 2013 APEC submission, the Special Police Second Headquarter, N.P.A., is mandated to cooperate with each nuclear power plant in order to host an annual nuclear response exercise. It will also host an exercise on nuclear fuel escorting emergency as a part of TPC's yearly training for nuclear fuel transportation (emergency exercise included). Chinese Taipei's CDC will work together with the Ministry of National Defense to maintain emergency response capacity.

The Criminal Investigation Bureau, N.P.A., implemented the "Working Platform of Cyber Crime Prevention Technology" to discuss prevention and control strategy. It is also a contact point for international cooperation. It has established an automated data exchange mechanism among A-ISAC (ISAC for educational networks), G-ISAC (ISAC for governmental networks), and domestic ISPs to ensure timely responses to cyber incidents.

Several cyber-related policy opportunities and challenges for further consideration:

Geopolitical considerations and perceived primary threat actors are important when it comes to how policies might be developed and implemented. The challenge is that since it can often be difficult to attribute accurately responsibility for a cyber incident, misappropriation could lead to misunderstanding or an escalation in tensions. This is especially challenging when non-state actors could also be to blame and contemporary cybercrime levels are on the increase in the region.

Given Chinese Taipei's use of nuclear power, it should especially ensure that extensive computer security/cybersecurity measures are in place. The IAEA (as well as several nation states)

provides guidance for consideration by states, competent authorities, and operators. The aim is to prevent the theft of material or sabotage of plants and facilities.

Chinese Taipei is a chain of islands. Maritime transport and ICT dependencies should therefore be fully considered, particularly since Chinese Taipei is highly dependent on imports for the majority of its energy requirements.

If TPC is privatized and the domestic power market is liberalized, public-private sector considerations relating to cybersecurity will also require closer examination by Chinese Taipei.

6.17.4 Future Cybersecurity Nexus

There is insufficient data on this topic for Chinese Taipei. This is a potential area of future growth.

6.17.5 Smart Grids

Chinese Taipei hosted an APEC Smart Grid Workshop in 2012. In August 2012, the Executive Yuan hosted a series of discussions that promoted smart grid technology, including smart generation, management, transmission and distribution. The Office also outlined that low-voltage smart meters for residential use should also be gradually pushed forward.

Chinese Taipei in documents has noted that the construction of a smart grid plays a vital role in its energy conservation and carbon reduction strategy. Therefore, Chinese Taipei will gradually and steadily replace mechanical meters with a smart metering system.

It intends to expand into overseas markets in order to secure substantial business opportunities. TPC has promoted Advanced Metering Infrastructure (AMI), which entails: drawing up related functional specifications and standards for AMI; establishing an open test platform so as to provide firms with platform testing meters, communication networks, and Meter Database Management System; and data security and availability. The company completed meter installation for 1,200 high-voltage users in 2010, and completed the construction of AMI for all high-voltage users (approx. 23,000) during 2011-2013. 1,200 low voltage AMI meters were deployed from 2010 to 2012 for an AMI demo-site system by the Bureau of Energy, and 10,000 meters in 2012/2013 for a small pilot project by TPC. According to the assessment of the Bureau of Energy and MOEA, it shows a total investment in AMI of NT$95.8 billion dollars over 20 years with a reduction in users' electricity cost of NT$395.4 billion dollars over the same period. It is hoped that will open opportunities for Chinese Taipei metering manufacturers to sell in the international market.

According to a submission document to APEC by the Chair of the Chinese Taipei National Energy Project in 2011 on the development of the smart grid in Chinese Taipei under the "Master Plan of Smart Grid (2011~2030)", a task force includes the following agencies: National Science Council, Ministry of Economic Affairs, Bureau of Energy, Bureau of Standards,

Industrial Development Bureau, Department of Industrial Technology, TPC, Institute for Information Industry, Institute of Nuclear Energy Research, Industrial Technology Research Institute, Smart Grid Industry Association, and the Institute of Economic Research.

Under the section on smart transmission, it mentions the increase of transmission security. As an isolated power system, TPC's is not connected to other power systems. Its strategy is to tie in closely with the smart grid development schedule of TPC to integrate the research abilities of industry and academia to establish the smart grid and to support the power facilities industry in Chinese Taipei. From 2013 to 2017, the plans outlined include: commercializing the promotion of smart meters and electric vehicles; promoting smart home (building) power management technology for household users; and building the first demo site of a smart grid and AMI in Penghu.

The Smart Grid Industry Association's (TSGIA) objectives include: coordinating the development of power system, power electronics and ICT to develop the smart grid industry; and acting as a bridge between industry and government.

Chinese Taipei participates in the APEC ESCI Smart Grid Test Bed Network and Smart Grid Road Maps programs of the Knowledge Sharing Platform. Chinese Taipei is a member of the Global Smart Grid Federation (GSGF).

Given Chinese Taipei's smart grid plans as well as plans to promote smart grid technology, smart energy network systems, energy smart buildings and meters for residential uses, enhancing cybersecurity is essential.

Chinese Taipei should also consider that consumers should be informed about the opportunities as well as the risks associated with smart grid systems.

6.18 Thailand

6.18.1 Economy Energy Resources

The APEC Energy Overview of 2014 provides that Thailand has reserves of oil, natural gas and coal. Notwithstanding its resources, it is highly dependent on energy imports, particularly oil, with more than 85 percent of its oil supply coming from imported stock in 2011. For electricity generation, thermal generation, mostly from natural gas and coal, accounted for nearly all of the power generation (96 percent), with hydropower and others accounting for the remainder in 2011.

6.18.2 Current Cybersecurity Nexus

Defining critical infrastructure protection

Material from the Electronic Transactions Development Agency of the Ministry of Information and Communication Technology specifies the interdependency of critical infrastructures. It describes critical infrastructures as including oil and gas (fuel supply and stations); electric power (power supply and power plant); water; communications; banking and finance; transportation; emergency services; and government services.

It mentions the cybersecurity policy framework includes: cybersecurity governance; cybersecurity emergency readiness; national critical information infrastructure readiness; public private partnership; capacity and capability building; legal measures; R&D; and international cooperation.

Defining cybersecurity

According to the 2015 ITU country report, Thailand's legislation for cybercrime is the Act on Computer Crime B.E.2550 (2007). Legislation and regulation related to cybersecurity has also been enacted through this Act. The Government CSIRT is ThaiCERT. It is a member of APCERT, and the only Thai representative in FIRST. ThaiCERT is operated within the Electronic Transactions Development Agency and engages with regional partners regularly. Through the Office of the National Security Council and the Ministry of Information and Communication Technology (MICT), Thailand has national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards. The approved national certification and accreditation body is the IT Crime Prevention and Suppression Bureau, MICT, and ThaiCERT.

The ITU factsheet specifies that Thailand has a national and sector specific cybersecurity strategy and/or policy through the IT Crime Prevention and Suppression Bureau, MICT, and ThaiCERT. There is a governance roadmap for cybersecurity through the IT Crime Prevention and Suppression Bureau, and MICT. MICT is the official designated agency with responsible for implementing national cybersecurity strategy, policy and roadmaps. It is responsible for national and sector-specific benchmarking exercises, and referential guides used to measure cybersecurity development.

ASPI's 2014 report on cyber maturity in the Asia Pacific also states that MICT is the primary agency responsible for cyber policy. However, the Government has recently raised the profile of cyber issues by launching the National Cyber Security Committee, chaired by the Prime Minister. The Electronic Transactions Development Agency is charged with coordinating the implementation of cyber strategies and measures. It is working with international partners to improve national cyber capacity. The Royal Thai Police are charged with maintaining law online.

Media reports in early 2015 cite that the Cabinet approved a cybersecurity bill to establish the National Cybersecurity Committee and a new state agency, the Office of the National Cybersecurity Committee.

The ITU country report outlines that Thailand does not have any officially recognized partnerships to facilitate sharing of cybersecurity assets across borders or with other nation states. Thailand is a member of the ITU-IMPACT initiatives. According to the UNIDIR Cyber Index 2013, Thailand signed a memorandum of cooperation in 2012 with Symantec to create a national cybersecurity system.

The ASPI report on cyber maturity in the Asia Pacific region in 2014 finds that Thailand has a moderately developed organizational structure for cyber issues and is pursuing positive legislative agendas. The Government and military have made positive moves to develop cyber governance and capability. This includes efforts to increase investment in digital infrastructure, internet connectivity and the ICT sector. If current efforts are continued and backed by much-needed investment, Thailand's cyber maturity outlook is generally positive. There is improving clarity about roles and responsibilities, and Thailand's cyber legislation and regulation are under way. Basic frameworks for national cyber efforts are in place, suggesting a clear understanding and willingness to act on cyber issues. The support structures to further develop policy and implement measures remain a work in progress.

Thailand's international engagement on cyber issues is largely focused on capacity building and less on wider cyber issues, such as internet governance. It has established many international partnerships to improve domestic cyber capabilities, including with the International Council of Electronic Commerce Consultants and the SANS Institute.

The Thai military currently has limited capability and authority on cyber issues, but its leadership has expressed an interest in developing legislation to legalize the operation of a cyber group. Thailand hosted the 2013 USPACOM Cyber Endeavour program, which focused on communications and IT interoperability.

6.18.3 Cybersecurity Challenges (Issues)

A Provincial Energy Authority (PEA) presentation outlined certain challenges in the implementation of the smart grid. These included, amongst others: increase in system operational complexity; large data handling; information security; requirement of accurate forecasting approaches; cost-effecting implementation, including ICT; utilization of Demand Response; and fast analysis tools. Critical issues identified included: interoperability; security; data management; and data integration.

The Annex Power report highlighted that another important factor raised by interviewees on issues that might hinder smart grid development in Thailand was data security. This is apparently still limited due to the lack of knowledge about smart grid. The report argues however, that

official regulations should be prepared and regulations implemented before these concerns grow and cause problems.

Thailand hosted a regional conference in June 2015 on critical infrastructure protection and resilience in Asia. The Department of Disaster Prevention & Mitigation under the Ministry of Interior, the Ministry of Information & Communication Technology and the Electronic Transactions Development Agency co-hosted it. PEA also sponsored the June conference. Topics of discussion included protection, security and cybersecurity of national infrastructure and critical information. The website describes how Southeast Asia has seen a rise in insurgency-related attacks and terrorist activities, creating uncertainty and insecurity on critical national infrastructure. In addition, it cites more extreme weather patterns as creating additional hazards.

Material from the Electronic Transactions Development Agency of the Ministry of Information and Communication Technology on critical infrastructure protection outlines that ThaiCERT has incident drills twice a year [financial institutes, ISPs]. There are information sharing channels between CSIRT and the police, CSIRT and "electricity generating organization".

The ASPI report cites that efforts were underway to upgrade ThaiCERT became a national incident response team in 2014.

Several cyber-related policy opportunities and challenges for further consideration:

Greater connectivity in the region could raise the probability of transnational crime and cross-border cyber-related incidents. With increasing access to high-speed networks, low-level cybercrime has already risen in the ASEAN region. In Asia, policy experts further suggest that the growth of cybercrime could increase instability. Misappropriation of responsibility could lead to misunderstandings and the possible escalation in tensions or conflict because the accurate identification of those responsible for a cyber incident is not always easy (especially since there is now a wide range of varying threats that may also come from different non-state actors).

Given that, Thailand is highly dependent on energy imports, especially with more than 85 percent of oil supply coming from imported stock, it should closely consider possible cyber threats to oil and gas suppliers. Particularly since many major oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. Breaches may cause high damage to corporate assets, public infrastructure and safety, or the wider economy. Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain. Thailand should therefore closely monitor cyber issues relevant to the electric grid as well as the supply chain.

Given its plans for nuclear power, the IAEA (as well as several nation states) provides guidance for consideration by states, competent authorities, and operators. The aim is to prevent the theft of material or sabotage of plants and facilities.

The APEC Energy Overview Study of 2014 finds that the Government is keen to encourage competition and investment in energy businesses by creating a favourable environment for investment, transparent competition and internationally accepted energy-related standards. However, because dialogue between the Thai Government and industry on cyber issues remains fairly limited according to the report by ASPI, specific public-private sector considerations relating to cybersecurity and the energy sector should be carefully examined using mechanisms such as the Cyber Security Operations Center.

The Annex Power report also highlights that smart grid systems mainly include hardware and software systems for supply, transmission, and distribution of electricity. The operation and maintenance of these systems are crucial in the later phase. Capacity building for the future work force for operation and maintenance has to be planned and trained in parallel with other activities.

In addition, material from the Electronic Transactions Development Agency of the Ministry of Information and Communication Technology on critical infrastructure protection outlines cybersecurity challenges. One challenge is that there is not a large enough workforce and certified professionals in cybersecurity. Other challenges include that law enforcement does not have sufficient capacity to fight cybercrime, there is a language barrier and digital divide, and sector-based CSIRT/CERTs are still being built.

Consequently, there is a need for more capacity building and a need for skilled professionals. Thailand, according to reports, is already focusing on international engagement in capacity building. However, capacity building related to cybersecurity issues specifically in the energy sector should not solely focus on technical capacity building but also include policy as well as legislative, organizational, and law enforcement training. In addition, external offers of capacity building should be coordinated and capacity building should reflect the unique needs of the economy.

Given the interest in the smart grid, enhancing cybersecurity is also essential and it should be more closely considered as part of a larger smart grid deployment strategy.

Regarding multilateral efforts, at the regional level, Thailand is a member of ASEAN. It is also a participant at the ASEAN Regional Forum (ARF).

Thailand has expressed support for the ASEAN Regional Forum’s efforts to develop a Work Plan on Cyber Security, according to the ASPI report.

6.18.4 Future Cybersecurity Nexus

There is insufficient data on this topic for Thailand. This is a potential area of future growth.

6.18.5 Smart Grids

2014 reports say that investment in Southeast Asia will include smart metering and the modernization of electricity transmission and distribution networks with sensors, communications and software. By 2024, the largest markets will be Thailand, Indonesia, Malaysia, Singapore, the Philippines, and Viet Nam, according to a recent study by Northeast Group LLC.

Southeast Asian economies are just beginning on the path of modernizing their electric infrastructure. Electrification programs and growth in renewable resources will also drive investment. 2014 reports online also outline that some emerging economies, such as Thailand, Malaysia, Indonesia, and the Philippines, are making plans to deploy smart grid technology. While this region is currently behind other global regions in terms of smart meter deployments and regulatory frameworks, its smart grid market is growing. There are already smart grid pilot projects in several economies throughout the region. By 2022, Southeast Asian economies will likely have an electricity demand profile similar to Latin American economies where large-scale smart meter deployments already exist. The region's current electricity consumption rates are among the lowest in the world, while distribution loss rates are comparatively moderate, offering less short-term savings potential compared with other global regions. Additionally, regulatory frameworks remain largely undeveloped in the region. Even in the more advanced economies, deployments are mostly still at the initial pilot level.

This Northeast Group study finds that Singapore is currently leading the region in development but later in the decade, the large markets of Thailand, Indonesia, Malaysia, Viet Nam, and the Philippines will account for significant smart grid investment. Several economies in the region have drafted smart grid roadmaps and pilot projects are widespread. Regulatory frameworks are still developing but momentum will grow over the next several years. Both utilities and vendors are already working together to ensure preparedness when regulations are finalised. Many vendors are active across the region. These include ABB, Alstom, Echelon (NES), EDMI (Osaki), Elster, Enverv, GE, Itron, Schneider, Secure, Siemens, Silver Spring Networks, ST Electronics, Trilliant and other global and local vendors.

The APEC Energy Overview Study of 2014 finds that strategies under the current 10-year Renewable and Alternative Energy Development Plan (AEDP) 2012–2021 include:

1. Promoting the community to collaborate in broadening the production and consumption of renewable energy;

2. Adjusting the incentive measure on investment from the private sector;

3. Amending the laws and regulations that do not benefit renewable energy development;
4. Improving the infrastructure as system of transmission lines, power distribution lines, including the development of a smart grid system;
5. Public relations and building up comprehensive knowledge for the people; and
6. Promoting research work as a mechanism to develop an integrated renewable energy industry.

2013 reports on the smart grid explain that the government offices and institutions that have studied or planned for smart grid implementation are the Energy Policy and Planning Office (EPPO), Ministry of Energy, Provincial Electricity Authority (PEA), Metropolitan Electricity Authority (MEA), Electricity Generating Authority of Thailand (EGAT), and PTT Public Company Limited. Others may have started similar studies, but have not announced any plans.

The Energy Policy and Planning Office (EPPO) in the Ministry of Energy engaged the Energy Research Institute of Chulalongkorn University to prepare a smart grid implementation plan and roadmap to be the guideline for future investment in smart grid facilities.

The Provincial Electricity Authority (PEA) has developed a smart grid roadmap with the Energy Research Institute of Chulalongkorn University, and has plans to implement Advance Metering Infrastructure (AMI) in Pattaya. The road map is divided into areas of application, such as advanced metering and communication, distribution system automation, substation automation, utility enterprise applications, and system integration. PEA has planned to implement smart grid facilities in three stages. The first stage is "Planning and Pilot Project" (2012-2016). The second stage, will be implemented during 2017-2021, is "Large Scale Expansion", and the last stage is the "Optimal Stage" is planned for 2022-2026. Large investments are planned for the implementation of smart grids.

EPPO and PEA have also supported a demonstration smart micro grid and smart metering system at King Monkut's University of Technology Ladkrabang. PEA plans to implement another demonstration smart grid project in collaboration with King Monkut's University of Technology Ladkrabang at Pattaya City. This would be a micro-grid, which connects the electricity generation from renewable energy (PV), wind simulation and a diesel generator with the main grid.

The Metropolitan Electricity Authority (MEA) has indicated projects that modify and improve the existing facilities in relation to efficiency in operation, customer services, and system security and reliability, such as SCADA for the transfer of information between stations and central control room, will need Energy Management System (EMS) for the analysis of power flow and contingency for the supply side, substation automation, Distribution Management System (DMS), and Automatic Meter Readings (AMR). MEA is now in cooperation with a

research unit in a university for a study on impacts of the connections of VSPPs on the grid for the preparation of future VSPP connections. So far, MEA has announced no concrete timetable for future investment projects in smart grid technologies.

The Electricity Generating Authority of Thailand (EGAT) has utilized modern technologies like SCADA, protection systems, and communication systems, such as power line carrier and optical fiber in overhead ground wire. It has set up a smart grid work group to study future smart grid applications, which includes interoperability standards, renewable energy integration, and effects of electric vehicles (EVs). EGAT's smart grid working group has identified the new technologies to be applied as digitalized substation, Wide Area Monitoring System (WAMS), Special Protection Scheme (SPS), and Automatic Fault Analysis (AFA). However, so far, no concrete timetable for future investment projects in smart grid technologies have been announced by EGAT.

PTT Public Company Limited has an interest in electric vehicle (EV) charging stations, and has set up a demonstration station to verify the applicability of the technology. There is a plan to continue the verification of the technology and to expand the number of EV charging stations, which could be located at PTT gas stations and department stores' parking lots.

The Solar Power Company Group (SPCG) engaged with ENEGATE Co., Ltd., a company from Japan to launch a smart energy management system.

The Annex Power report found the following points were raised as hindering the actual development of the smart grid: 1) lack of knowledge and willingness on the private side; 2) missing regulations and a missing common smart grid plan including budget regulations; 3) unwillingness of the industries due to unknowns and non-visible Key Performance Indicators; and 4) lack of expertise and undeveloped technologies for infrastructure.

The Thai–European Business Association (TEBA) is developing a smart grid development plan in cooperation with the Thai Senate. For that reason, TEBA established a "Smart Grid – Round Table".

6.19 The United States

6.19.1 Economy Energy Resources

The most recent APEC energy review study in 2014 provides an overview of the primary energy sectors in the United States. It finds that the United States is the largest producer and consumer of energy in the world. It is also rich in energy resources. In 2011, the United States had 35 billion barrels of proven oil reserves, 8 800 billion cubic meters of natural gas reserves and 237 billion tons of coal reserves.

6.19.2 Current Cybersecurity Nexus

Defining critical infrastructure protection

Under the "Critical 5" document of March 2014, "Forging a Common Understanding for Critical Infrastructure", Annex A provides country definitions of Critical Infrastructure and Associated Sectors. The United States refers to critical infrastructure as the "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."

According to this March 2014 document, the United States, under the guidance of Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience (2013), is developing a national policy to promote critical infrastructure security and resilience.

The document notes that the nation's critical infrastructure provides essential services that underpin American society, and therefore, critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Resilience and security are both defined within PPD 21, with resilience "meaning the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents" and security referring to "reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters."

U.S. Critical Infrastructure includes: Chemical; Financial Services; Commercial Facilities; Food and Agriculture; Communications; Government Facilities; Critical Manufacturing; Healthcare and Public Health; Dams; Information Technology; Defense Industrial Base; Nuclear Reactors, Materials and Waste; Emergency Services; Transportation Systems; Energy; and Water and Wastewater Systems.

Under the New America study which delineates key terms related to existing cybersecurity and information security definitions, the following citations relevant to critical infrastructure are:

- Critical Infrastructure: As used in this order, the term critical infrastructure means 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.

  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 cybersecurity, national economic security, national public health or safety, or any combination of those matters.

  The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.

  Although governments administer only a minority of the Nation's critical infrastructure computer systems, governments at all levels perform essential services that rely on each of the critical infrastructure sectors, which are agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping.

- Critical Infrastructure and Key Resources: The infrastructure and assets vital to a nation's security, governance, public health and safety, economy and public confidence.

- Cyber Infrastructure: The information and communications systems and services composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. Includes electronic information and communications systems and services and the information contained in these systems and services. For example: computer systems; control systems (e.g., supervisory control and data acquisition SCADA); networks, such as the internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.

- National Critical Infrastructure and Key Assets: The infrastructure and assets vital to a nation's security, governance, public health and safety, economy and public confidence. They include telecommunications, electrical power systems, gas and oil distribution and storage, water supply systems, banking and finance, transportation, emergency services, industrial assets, information systems, and continuity of government operations.

Defining cybersecurity

According to the 2015 ITU country report for the United States, legislation on cybercrime has been enacted through the following instruments: 15 USC Chapter 103; Controlling the Assault of Non-solicited Pornography and Marketing; 18 USC, Chapter 47, § 1029 - Fraud and related activity in connection with access devices; 18 USC, Chapter 47, § 1030 - Fraud and related activity in connection with computers; 18 USC, Chapter 47, § 1037 - Fraud and related activity in connection with electronic mail; 18 USC Chapter 119 - Wire and Electronic Communications Interception and Interception of Oral Communications; 18 USC Chapter 121 - Stored Wire and Electronic Communications and Transactional Record Access. Legislation and regulation related to cybersecurity has been enacted through the following instruments: 44 USC Chapter 35, Subchapter III - Information Security (§3541); Uniform Electronic Transactions Act - Electronic Signatures in Global and National Commerce Act; Homeland Security Act - Cyber Security Research and Development Act; Freedom of Information Act (5 USC § 552) - Privacy Act (5 U.S.C. § 552a); Federal Information Security Management Act of 2002.

The United States has an officially recognized national CIRT, US CERT, and an industrial control systems CERT, ICS-CERT. ASPI's 2014 report on cyber maturity notes that the United States is home to 68 members of FIRST, including the CERT Program at Carnegie Mellon University. US-CERT, under the Department of Homeland Security (DHS), is the leading national CERT and is proactive nationally as well as internationally. The role of the Department of Defense (DoD) in cyberspace is largely concerned with signals intelligence, the defense of .mil domains, and offensive and defensive military cyber operations.

The ITU factsheet specifies that the United States has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the following instruments: NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0; Federal Information Security Management Act of 2002; NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems"; various North American Electric Reliability Corporation (NERC) standards such as NERC 1300 which is a modification/update of NERC 1200; and NIST Special Publication 800-12 provides a broad overview of computer security and control areas. The National Initiative for Cybersecurity Education (NICCS) offers a cybersecurity framework for the certification and accreditation of national agencies and public sector professionals. The National Checklist Program (NCP), defined by the NIST SP 800-70 Rev. 2, is the U.S. government repository of publicly available security checklists (or benchmarks) that provides detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists.

ITU's factsheet further outlines that the NIST Cybersecurity Division (CSD) provides information resources—standards, frameworks, tools, and technologies to enable seamless and secure interactions among homeland security stakeholders and leads the Government's charge in funding cybersecurity R&D. The IT Security Essential Body of Knowledge (EBK) establishes a national baseline of the essential knowledge and skills that IT security practitioners in the public and private sector should have to perform specific roles and responsibilities. The National Cybersecurity Center of Excellence (NCCoE) provides businesses with cybersecurity solution based on commercially available technologies.

The factsheet explains that the White House has an appointed U.S. Cybersecurity Coordinator at the level of Special Assistant to the President to guide Executive Branch efforts. DHS and the DoD are also primary cybersecurity actors and they monitor and coordinate the implementation of national cybersecurity strategy, policy and roadmaps by respective agencies. According to the UNIDIR Cyber Index of 2013, responsibility for cybersecurity is divided among DHS, the FBI, and the DOD including U.S. Cyber Command, with the Departments of State and Commerce leading international negotiations and the development of cybersecurity standards. The DHS National Cybersecurity Division is tasked to "work collaboratively with public, private, and international entities to secure cyberspace and America's cyber interest". It has a number of programs to assist companies in protecting cyber infrastructure from attack.

The DoD established the Defense Industrial Base (DIB) Cybersecurity/Information Assurance (CS/IA) Program that aims to provide cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

UNIDIR's 2013 cyber index notes that the National Cyber Response Coordination Group is comprised of 13 federal agencies and is responsible for coordinating the federal response in the event of a "nationally significant cyber incident". The DHS also has expanded the work of the National Cybersecurity and Communications Integration Center to improve situational awareness and information sharing. The DoD and DHS signed a memorandum of agreement in October 2010 to increase interdepartmental collaboration. Secretary of Defense Leon Panetta, in a speech on 18 December 2012, said that the DoD is exploring ways to strengthen the Cyber Command, which was originally responsible for dealing with threats to the military cyber infrastructure, and will now have broader national cyber defense responsibilities.

The ASPI report on cyber maturity in 2014 finds that the United States is a leading actor in cyber governance and technical capabilities, backed by a strong digital economy, including Silicon Valley and many large and start-up tech communities throughout the economy. The White House doubled down on cyber efforts initiated by the previous administration, but legislative progress is slow. The United States is heavily engaged internationally at all levels of government. It finds that the United States has a strong organizational structure to handle cyber issues, with responsibilities divided among government departments and agencies. Anti-cybercrime

responsibility is generally disseminated among local and state authorities under existing jurisdictional arrangements, with the FBI leading federal efforts.

The report finds however that despite a strong structure in place, the lack of a clear whole-of-government cyber strategy and problems in interdepartmental coordination remain as weaknesses for the Government's cyber efforts. While there is no overarching framework legislation governing cyber issues, the United States does have a strong collection of policies and regulations relating to cyber issues. The Executive Branch has been especially proactive in promoting Federal Government cyber policies as well as public–private partnerships on cyber issues. The United States has a clear and public cyber strategy and a strong ability to implement cyber programs.

Cybersecurity has been identified as a national security priority in the National Security Strategy, and DoD published a Strategy for Operating in Cyberspace in 2011 to guide its cyber efforts. The U.S. military possesses sophisticated capabilities, but internal coordination and governing policies concerning those operations could use further development according to ASPI's report. The DoD published the 2015 DoD Cyber Strategy in April 2015.

According to the ASPI report, the United States is home to some of the largest IT, software, hardware and internet companies in the world, as well as to numerous start-up communities. Knowledge-intensive jobs account for 36.3 percent of the workforce, and the internet economy accounted for 4.7 percent of 2010 GDP. Public awareness of and debate on cyber issues are very high.

Under the New America compilation of terms and definitions, the following key terms related to existing cybersecurity and information security definitions are delineated for the United States:

- Information: 1) Facts, data, or instructions in any medium or form; 2) The meaning that a human assigns to data by means of the known conventions used in their representation; and 3) Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

- Information and Communications Technologies: Any information technology, equipment, or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.

- Information System: The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

- Information Technology: Any equipment or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.

  Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: 1) requires the use of such equipment; or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

- The Internet: The internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB), and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

- Cyber Space: Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work.

  The globally-interconnected digital information and communications infrastructure known as “cyberspace” underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, and public safety.

  A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

  The interdependent network of information technology infrastructures that includes the internet, telecommunications network, computer systems, and embedded processors and controllers.

- Information Environment: Aggregate of individuals, organizations, and/or systems that collect, process, or disseminate information, also included is the information itself.

- Information environment is assessed in the following three aspects: 1) Physical aspect includes command and control systems, supporting infrastructure and soldiers who accomplish operations in physical area; and 2) Information aspect is the information, which is collected, processed, stored, disseminated and protected. Information aspect also includes the cyberspace. This aspect connects physical and cognitive aspects.

- Computer Security: The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems.

  Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

- Cyber Security: The ability to protect or defend the use of cyberspace from cyber-attacks.

- Cybersecurity policy: The strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure.

  The process of protecting information by preventing, detecting, and responding to attacks.

  Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

- Information Security: The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users.

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- Cyber Incident: Actions taken via computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

- Attack: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

- Computer Network Attack: Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

- Computer Network Defense: Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks.

  The actions taken to defend against unauthorized activity within computer networks.

  Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.

- Computer Network Exploitation: Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

- Computer Network Operations: Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

- Cyber Attack: An attack via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

- Cyber Operations: In the NICE Workforce Framework, cybersecurity work where a person: Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.

  The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the global information grid (GIG).

- Cyberspace Operations: The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

- Exploit: A technique to breach the security of a network or information system in violation of security policy.

- Hacker: An unauthorized user who attempts to or gains access to an information system.

- Information Assurance: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

  The measures that protect and defend information and information systems by ensuring their availability, integrity, and confidentiality.

- Information Operations: The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making process, information, and information systems while protecting our own.

- Intrusion: An unauthorized act of bypassing the security mechanisms of a network or information system.

- Malware: Software that compromises the operation of a system by performing an unauthorized function or process.

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

- Threat: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

- Extended Definition: Includes an individual or group of individuals, entity such as an organization or a nation), action, or occurrence.

  Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

6.19.3 Cybersecurity Challenges (Issues)

Media reports in the United States outline that cyber-attacks against energy infrastructure are already a reality. For instance, in 2014, a cyber-attack perpetrated by "Ugly Gorilla" — a hacker alleged to be based in Asia —infiltrated the computers of a U.S. public utility company. The attacker sought to access pipeline schematics and natural gas flow regulation systems, including network areas that allowed remote shutdown of energy infrastructure systems. In 2014, ICS-CERT reported that the largest portion (32 percent) of the 245 cybersecurity incidents to which the organization responded involved the energy sector. In 2013, 59 percent of the 256 cybersecurity incidents responded to by ICS-CERT occurred in the energy sector.

Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience (2013) outlines that U.S. efforts shall address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect this infrastructure's interconnectedness and interdependency. This directive also identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors.

Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience (2013) specifies that the Secretary of Homeland Security shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the nation's critical infrastructure. In carrying out the responsibilities assigned in the Homeland Security Act of 2002, as amended, the Secretary of Homeland Security evaluates national capabilities, opportunities, and challenges in protecting critical infrastructure; analyzes

threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure; identifies security and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors; develops a national plan and metrics, in coordination with SSAs and other critical infrastructure partners; integrates and coordinates Federal cross-sector security and resilience activities; identifies and analyzes key interdependencies among critical infrastructure sectors; and reports on the effectiveness of national efforts to strengthen the nation's security and resilience posture for critical infrastructure.

Additional roles and responsibilities for the Secretary of Homeland Security include:

1. Identify and prioritize critical infrastructure, considering physical and cyber threats, vulnerabilities, and consequences, in coordination with SSAs and other Federal departments and agencies;
2. Maintain national critical infrastructure centers that shall provide a situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact critical infrastructure;
3. In coordination with SSAs and other Federal departments and agencies, provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure;
4. Conduct comprehensive assessments of the vulnerabilities of the nation's critical infrastructure in coordination with the SSAs and in collaboration with SLTT entities and critical infrastructure owners and operators;
5. Coordinate Federal Government responses to significant cyber or physical incidents affecting critical infrastructure consistent with statutory authorities;
6. Support the Attorney General and law enforcement agencies with their responsibilities to investigate and prosecute threats to and attacks against critical infrastructure;
7. Coordinate with and utilize the expertise of SSAs and other appropriate Federal departments and agencies to map geospatially, image, analyze, and sort critical infrastructure by employing commercial satellite and airborne systems, as well as existing capabilities within other departments and agencies; and
8. Report annually on the status of national critical infrastructure efforts as required by statute.

The Secretary of Homeland Security, in coordination with the Office of Science and Technology Policy (OSTP), the SSAs, DOC, and other Federal departments and agencies, provides input to align those Federal and Federally-funded research and development (R&D) activities that seek to strengthen the security and resilience of the nation's critical infrastructure, including:

1. Promoting R&D to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;
2. Enhancing modeling capabilities to determine potential impacts on critical infrastructure of an incident or threat scenario, as well as cascading effects on other sectors;
3. Facilitating initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen all-hazards security and resilience; and
4. Prioritizing efforts to support the strategic guidance issued by the Secretary of Homeland Security.

The 2013 Executive Order, "Improving Critical Infrastructure Cybersecurity", outlines that repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges. The national and economic security of the United States depends on the reliable functioning of the nation's critical infrastructure in the face of such threats.

It further notes that it is the policy to enhance the security and resilience of the nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.

These goals can be achieved through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards. It is the policy of the Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. The Order noted the need for instructions on the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary in collaboration with the Secretary of Defense, shall establish procedures to expand the Enhanced Cybersecurity Services program to

all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities.

The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

The Executive Order called for the creating of a Cybersecurity Framework to incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order. It identified the need for this framework to provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, and any other relevant factors.

The Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure on an annual basis.

The NIST Roadmap for Improving Critical Infrastructure Cybersecurity, the Cross-Sector Roadmap for Cybersecurity of Control Systems and the Roadmap to achieve energy delivery systems cybersecurity provide the national governance roadmap for cybersecurity in the U.S. according to the ITU country factsheet. The DHS Critical Infrastructure Cyber Community C³ Voluntary Program helps align critical infrastructure owners and operators with existing resources that will assist their efforts to adopt the Cybersecurity Framework and manage their cyber risks.

According to the NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, which was then released in 2014, the national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the nation's security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.

The Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. It focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.

It consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business

requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

The Executive Order also requires that the Framework include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. While processes and existing needs will differ, the Framework can assist organizations in incorporating privacy and civil liberties as part of a comprehensive cybersecurity program.

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. It provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today.

In addition, the framework document notes that because it references globally recognized standards for cybersecurity, the Framework can also be used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

To ensure extensibility and enable technical innovation, the Framework is technology neutral. It relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience. By relying on those global standards, guidelines, and practices developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes will scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements. The use of existing and emerging standards will enable economies of scale and drive the development of effective products, services, and practices that meet identified market needs. Market competition also

promotes faster diffusion of these technologies and practices and realization of many benefits by the stakeholders in these sectors.

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to: 1) describe their current cybersecurity posture; 2) describe their target state for cybersecurity; 3) identify and prioritize opportunities for improvement within the context of a continuous and repeatable process; 4) assess progress toward the target state; 5) and communicate among internal and external stakeholders about cybersecurity risk.

The document outlines that the Framework complements, and does not replace, an organization's risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

In January 2015, there was a significant step in the standardization of cybersecurity protocols for the energy sector when the U.S. DOE Office of Electricity Delivery and Energy Reliability issued the Energy Sector Cybersecurity Framework Implementation Guidance. This guidance is intended to help the energy sector establish or align existing cybersecurity risk management programs to meet the objectives of the NIST Cybersecurity Framework. Reports note that the NIST Cybersecurity Framework is one of many emerging cybersecurity benchmarks, and compliance with the framework does not provide a safe harbor for failure to comply with existing cybersecurity requirements. For example, various existing NERC Critical Infrastructure Protection (CIP) Standards are mandatory, which subjects the relevant regulated entities to potential enforcement action and penalty assessment. The CIP Standards relate to critical cyber-asset identification, security management controls, electronic security perimeters, physical security of cyber-assets, among other protocols. The North American Energy Standards Board (NAESB) has developed cybersecurity standards that are mandatory for various segments of the energy industry. In the case of natural gas companies, for example, NAESB's cybersecurity standards mandate the use of digital signatures and self-certification to support mutual entity authentication.

The April 2015 Cyber Strategy of the DoD outlines that the increased use of cyber attacks as a political instrument reflects a dangerous trend in international relations. A disruptive, manipulative, or destructive cyberattack could present a significant risk to U.S. economic and national security if lives are lost, property destroyed, policy objectives harmed, or economic interests affected.

DoD will also work with DHS to improve the Enhanced Cybersecurity Services program and encourage additional critical infrastructure entities to participate, with a particular emphasis on increasing the number of defense critical infrastructure participants.

The Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT) was established in 2009 to provide industry players with up-to-date information about new vulnerabilities, mitigation strategies, and best practices. ICS-CERT has an important role to ensure dialogue and technical exchange between government and the private sector that helps improve the capacity to protect the nation's critical infrastructures.

Reports note that ICS-CERT has made good progress. During the first 6-months of FY 2013, ICS-CERT responded to over 200 reported cyber incidents, exceeding the total number of incidents—198—that were reported during FY 2012. The increase in reported incidents is reported to be a likely reflection of both the continuing presence of cyber-threats as well as better reporting by the private sector to ICS-CERT.

Cyber-related policy opportunities and challenges for further consideration:

The United States should continue to monitor possible cyber threats to oil and gas suppliers, the supply chain, its electric grid, and pipelines.

Many major oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. This could possibly cause damage but breaches may also cause high damage to corporate assets, public infrastructure and safety, or the wider economy. Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain.

Given the economy's nuclear plants, it should continue to closely consider the nexus between cybersecurity and this sector. The IAEA (as well as several other nation states), for instance, provide guidance for consideration by states, competent authorities, and operators. The aim is to prevent the theft of material or sabotage of plants and facilities.

Public-private sector considerations are also important. In this regard, Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience (2013) notes that critical infrastructure security and resilience is a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure. The 2013 Executive Order equally cites the importance of collaboration and recommends a number of initiatives.

ASPI's report also makes note of the fact that the U.S. Government has a strong dialogue with the larger business community, in particular with technology companies, defense contractors,

banks and other big businesses. Informal and formal meetings between government officials and industry representatives occur regularly, and official programs under DHS, the Federal Trade Commission and the Federal Bureau of Investigation's InfraGard program enhance the dialogue. The Executive Branch is seeking to improve cooperation, especially for critical infrastructure security.

Regarding multilateral efforts, the 2014 NIST Framework document specifies that just as the Framework is not industry-specific, the common taxonomy of standards, guidelines, and practices that it provides also is not country-specific. Organizations outside the United States may also use the Framework to strengthen their own cybersecurity efforts, and the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity.

In addition, the March 2014 "Forging a Common Understanding for Critical Infrastructure" document outlines that the following narrative represents the shared views of the Critical 5 member nations (Australia, Canada, New Zealand, the United Kingdom, and the United States) with the objective to provide a high-level overview of the meaning and importance of critical infrastructure.

More generally, at the international level, ASPI's report finds that the United States exhibits a high level of multilayered international involvement on cyber issues, including bilateral and multilateral engagement and participation in international cyber initiatives. The United States has ratified the Budapest Convention on Cybercrime, is a party to the UN Group of Governmental Experts (UN GGE), is heavily involved in the creation of international cyber standards, and regularly takes part in international cyber initiatives. The White House has published an International Strategy for Cyberspace that outlines U.S. priorities and values in the cybersphere.

At regional levels, the United States is a participant at the ASEAN Regional Forum (ARF). The United States also is a member of the Organization of American States (OAS).

The DoD Cyber Strategy 2015 outlines under the section, "Support the hardening and resiliency of Northeast Asian allies' networks and systems", that as a part of its broader cyber dialogue with Asian allies, DoD will work with key allies and partners to improve their ability to secure their military networks and critical infrastructure and key resources upon which U.S. and allied interests depend.

The United States is participating in the fourth UN GGE (2014/2015), the fourth Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

6.19.4 Future Cybersecurity Nexus

There is insufficient data on this topic for the United States. This is a potential area of future growth.

6.19.5 Smart Grids

The U.S. DOE 2014 Smart Grid System Report to Congress provides an overview of smart grid initiatives in the United States. It states in its Executive Summary that the U.S. electric grid is undergoing significant transformation from the application of digital technologies as a result of policies encouraging the growth of renewable and distributed energy resources, emphasis on resilience due to extreme weather events, and increasing involvement of electricity customers and businesses in both managing and producing energy.

Since 2010, large public and private investments of over $9 billion made under the American Recovery and Reinvestment Act of 2009 (ARRA) have advanced smart grid technology deployments, providing real-world data on technology costs and benefits along with best practices. Deployments are delivering results, and the report notes that improvements are being seen in grid operations, energy efficiency, asset utilization, and reliability.

The report notes that smart grid involves the application of advanced communications and control technologies and practices to improve reliability, efficiency, and security, which are key ingredients in the ongoing modernisation of the electricity delivery infrastructure. Progress in smart grid deployment is being made in these areas:

- Advanced metering infrastructure (AMI), which comprises smart meters, communication networks, and information management systems, is enhancing the operational efficiency of utilities and providing electricity customers with information to more effectively manage their energy use. An estimated 65 million smart meters were installed nationwide by 2015, accounting for more than a third of electricity customers.
- Customer-based technologies, such as programmable communicating thermostats for residential customers and building energy management systems for commercial and industrial customers, work with smart meters to make energy usage data accessible and useful to customers. At Oklahoma Gas and Electric, the coupling of AMI with time-based rates and in-home displays is reducing peak demand to an extent that will potentially enable the utility to defer the construction of a 170 MW peaking power plant. Also, utility and state efforts are addressing the privacy concerns of electricity customers, and businesses are offering new energy management services to customers.
- The integration of sensing, communications, and control technologies with field devices in distribution systems is improving reliability and efficiency. Smart grid applications enable utilities to automatically locate and isolate faults to reduce outages, dynamically optimize voltage and reactive power levels for more efficient power use, and monitor asset health to guide maintenance. For example, the City of Chattanooga was able to

instantly restore power to half of the residents affected by a severe windstorm in July 2012 (from 80,000 affected customers to less than 40,000 within 2 seconds) using automated feeder switching. In addition, utilities are upgrading and integrating computer systems to improve and merge grid operations and business processes.

- The deployment of advanced sensors and high-speed communications networks on transmission systems is advancing the ability to monitor and control operations at high-voltage substations and across the transmission grid. For example, synchrophasor technology provides data 100 times faster than conventional technology from the placement of phasor measurement units (PMUs) throughout the transmission grid and permits grid operators to identify and correct for system instabilities, such as frequency and voltage oscillations, and operate transmission lines at greater capacities. In one application, the Western Electricity Coordinating Council has determined that it can increase the energy flow along the California-Oregon Intertie by 100 MW or more using synchrophasor data for real-time control—reducing energy costs by an estimated $35 million to $75 million over 40 years without any new high-voltage capital investments. Public-private ARRA investments in synchrophasor technology resulted in more than 1,000 networked PMUs deployed by 2015, up from 166 in 2009.

The report notes that the rate of smart grid technology adoption varies across the nation and depends largely on state policies, regulatory incentives, and technology experience levels within utilities. It will take time to adequately assess and validate the costs and benefits of the technology for utilities, their customers, and society. Improved efficiencies in operations and energy use and in reliability are already being realised where smart grid technology is deployed. Hence, sharing effective deployment practices and methods for valuation across the industry and government jurisdictions will remain an important task. Deployments are delivering results, where the Government is seeing improvements in grid operations, energy efficiency, asset utilization, and reliability. The smart grid involves the application of digital technologies and information management practices and is a core ingredient in the ongoing modernization of the electricity delivery infrastructure.

A growing number of utilities that have begun successful smart grid deployments and are now grappling with a new set of technical, regulatory, and financial challenges that mark an industry undergoing change. In many cases, utilities have begun with small-scale tests and pilot programs before moving to larger-scale deployments to appropriately evaluate the technology and ensure management and regulatory approval for continued investment. The electricity industry spent an estimated total $18 billion for smart grid technology deployed in the United States during the 4-year period of 2010 through 2013 (BNEF 2014). Smart grid investments under the ARRA accounted for nearly half—approximately $8 billion—during the same time frame (DOE 2014a). As of March 2013, joint federal and private expenditures under ARRA totaled $6.3 billion from the 99 Smart Grid Investment Grants (SGIG), which represent the largest portion of ARRA investments.

Between 2009 and 2015, DOE and the electricity industry jointly invested more than $7.9 billion in the SGIG projects, which involve more than 200 electric utilities and other organizations to modernise the electric grid, strengthen cybersecurity, improve interoperability, and collect an unprecedented level of data on smart grid operations, benefits, and utility impacts (DOE 2013a). In the same time frame, an additional $1.6 billion in cost-shared funding will support energy storage demonstrations and regional demonstrations to assess emerging smart grid concepts (DOE 2014a). Another $100 million in federal funding has supported 52 smart grid workforce training projects in the same time frame (DOE 2014a).

To get a more detailed understanding of current smart grid status, the following sections from the DOE report provide an overview of deployment in four key technology application areas:

- Advanced Metering Infrastructure (AMI): AMI encompasses smart meters, the communications networks that transmit meter data to the utility at regular intervals (hourly or shorter), and the utility office management systems (such as meter data management systems) that receive, store, and process the meter data. Usage data from AMI systems can also be sent directly to building energy management systems, customer information displays, and smart appliances. About 46 million smart meters are in place in the United States today (IEE 2013). An estimated 65 million smart meters will be installed nationwide by 2015 (IEE 2012), accounting for more than a third of the approximate145 million U.S. meters (of all types) in use today (EIA 2013b; FERC 2013). ARRA project deployments contributed more than 16 million smart meters when completed in 2015 (DOE 2013a). Nearly 75 percent of AMI installations to date have occurred in only 10 states and D.C., where on average more than 50 percent of customers now have smart meters (DOE 2013b). AMI investments have been driven largely by state legislative and regulatory requirements for AMI, ARRA funding, and by specific cost recovery mechanisms in certain regions. AMI requires significant investment, and adoption barriers remain for utilities where the business case for AMI is not clear and where prior investments in older metering technology (such as automated meter reading) may present stranded costs.

  Concerns over meter safety, costs, and consumer privacy protections are being addressed, and enhanced consumer education is a key part of the solution.

  Real benefits, such as improved operational efficiencies, are being observed where AMI is deployed. For example, Central Maine Power Company has deployed smart meters to its 625,000 customers and has reduced its meter operations costs by more than 80 percent with annualized savings of about $6.7 million—due largely to fewer service calls, resulting in about 1.4 million fewer annual vehicle miles traveled (DOE 2013a). Projects under ARRA estimate operational cost savings from 13 percent to 77 percent, depending on the nature of legacy systems, the particular configuration of the utility service

territory, system integration requirements, and customer densities per line mile (DOE 2013a).

- Customer-Based Systems: AMI technologies can provide customers with detailed information and greater control over energy usage when coupled with residential customer technologies—including programmable communicating thermostats, web portals, and in-home displays—and business and industrial technologies that include building or facility energy management systems. Customer-based systems enable and support demand-response and time-based rate programs that promote more efficient customer energy use, in alignment with widespread federal, state, and local energy-efficiency policies. Commercial and industrial markets for energy management systems are more established than residential markets, yet they are all expected to grow significantly as advanced technology and greater access to information permit customers to more effectively manage their electricity use and save money. ARRA projects were mostly targeted small-scale, residential deployments of technologies and pricing programs. ARRA project recipients installed 623,000 customer-based devices by October 2013—a small percentage of customers when compared to the 14.2 million smart meters installed at that time (DOE 2013a).

  Time-based rate programs are growing—FERC estimates 2.1 million residential customers participated in 2012, nearly double the 2010 amount—but still reach only a small fraction of total customers (FERC 2012). Pilot programs conducted under ARRA projects aimed to quantify potential savings under time-based rates and determine customer preferences; the Sacramento Municipal Utility District, for example, is shifting all customers to a default time-of-use rate by 2018 based on the success of their pilot program (DOE 2013a, SMUD 2013). For example, Oklahoma Gas & Electric (OG&E) decided to offer a VPP/CPP rate to all its customers based on pilot results that reduced peak demand by at least 70 megawatts (MW) in one year. With a current goal of achieving 20 percent participation, OG&E hopes to reduce peak power requirements by 170 MW and thereby defer the construction of a peaking power plant planned for 2020.

- Distribution System Upgrades: Grid modernisation within the distribution system includes the deployment of sensor, communications, and control technologies that, when integrated with field devices within circuits, permit highly responsive and efficient grid operations. Smart distribution technologies enable new capabilities to automatically locate and isolate faults using automated feeder switches and reclosers, dynamically optimize voltage and reactive power levels, and monitor asset health to effectively guide the maintenance and replacement of equipment.

Industry analysts indicate that investments in distribution automation technology are now exceeding those in smart metering and will continue to grow (BNEF 2014). More than half of the ARRA projects are deploying distribution automation technologies across 6,500 circuits, representing about 4 percent of the estimated 160,000 U.S. distribution circuits (DOE 2013a). ARRA projects have invested about $2 billion as of March 2013 in distribution automation to deploy field devices, such as automated feeder switches and capacitors, and to integrate them with utility systems that manage data and control operations (DOE 2013a). In addition, utilities are beginning to upgrade and integrate their computer systems for managing distribution grid operations including meter operations and customer support, outage management, automated operations within substations and distribution circuits, and asset management. The impetus for advancing and integrating distribution management systems comes from the significant inflow of new data from field devices, such as smart meters and sensors on equipment and lines that provide utilities with enhanced understanding of grid status and new capabilities for planning and operations. As utilities begin to apply this information, increased coordination between departments is becoming possible along with greater collaboration between field operations and business processes, including customer interactions. In addition, advanced distribution systems allow greater degrees of automation, including both centralized and distributed control schemes.

Emerging technologies, such as energy storage and solid-state (power electronics) devices are also being introduced to better manage power flows. These devices along with more sophisticated information management and control systems are needed to provide the flexibility and reliability required to manage distributed energy resources (with two-way flows of power) and to support resilient operations that might incorporate, for example, automated switching and microgrids.

Distribution automation technologies can enhance reliability and resilience while improving operational efficiencies. ARRA projects that deployed automated feeder switches are reporting up to 56 percent shorter and 11 percent–49 percent less frequent outages, with fewer affected customers. The City of Chattanooga was able to instantly restore power to half of the residents affected by a severe windstorm (a derecho) on July 5, 2012 (from 80,000 affected customers to less than 40,000 within 2 seconds) using automated feeder switching; beyond avoiding outage damages to residents and businesses, the utility saved $1.4 million as it was able to restore power more quickly (DOE 2013a). Distribution automation technology can also improve energy efficiency. Many utilities are now beginning to apply smart grid technologies to dynamically optimize voltage and reactive power levels in certain distribution circuits. Where applied specifically to achieve lower voltage levels for conservation voltage reduction (CVR) purposes, smart devices are achieving on average 2.2 percent energy reductions and 1.8 percent peak load reductions per distribution circuit (DOE 2014c). Several ARRA projects are applying CVR within their distribution systems; one utility is expecting to obtain 200 MW in peak demand reduction by automating capacitor banks on their lines (DOE 2012a). Extrapolating from the results observed in CVR projects, it is estimated that significant energy efficiency gains are

possible—by as much as 6,500 MW of peak demand reductions nationally (PNNL 2010). Yet many utilities still face a lack of incentives for applying CVR practices and regulatory cost recovery challenges, as application of the technology results in reduced utility revenues.

Transmission system modernization includes the application of digitally based equipment to monitor and control local operations within high-voltage substations and wide-area operations across the transmission grid. Synchrophasor technology, which uses devices called phasor measurement units (PMUs) to measure the instantaneous voltage, current, and frequency at substations, is being deployed to enhance wide-area monitoring and control of the transmission system. Synchrophasor data are delivered in real time to sophisticated software applications that permit grid operators to identify growing system instabilities, detect frequency and voltage oscillations, and see when the system exceeds acceptable operating limits—allowing them to ultimately correct for disturbances before they threaten grid stability. Additionally, synchrophasor data enable improved coordination and control of generators, including renewable resources (e.g., wind power plants), as they interact with the transmission grid. Since the 2003 Northeast blackout investigation revealed inadequate situational awareness for grid operators, utilities have increasingly deployed synchrophasors to provide real-time, wide area grid visibility. Synchrophasors can provide time-stamped data 30 times per second or faster, which is 100 times faster than conventional supervisory control and data acquisition (SCADA) technology (DOE 2013c). Technology deployments includes phasor data concentrators that combine, time-align, and verify data from multiple PMUs; communication networks that deliver synchrophasor data; and information management, visualization, and other analytical tools to process synchrophasor data and support new data applications for grid operators.

The ARRA projects included a total public-private investment of about $330 million that increased U.S. synchrophasor coverage from 166 networked PMUs in 2009 to more than 1,000 networked PMUs deployed by the 2014-2015 time frame (DOE 2013c). As PMUs are deployed, transmission owners and reliability coordinators are working to develop suitable applications, build out high-speed data networks, improve data quality, and share synchrophasor data between transmission owners and operators across large regions. Utilities are already using synchrophasor data to improve the engineering models that simulate and explain how individual power plants and large system interconnections perform. Engineers design and operate the grid using mathematical models that predict how a power plant or other transmission assets will operate under various normal and abnormal conditions, and use these models to set grid operating limits and manage real-time operations and contingencies. These models are intended to prevent the high costs of potential power plant damage or large regional blackouts. Synchrophasors can provide historical data on actual grid performance under a variety of conditions to improve models, along with real-time data on current system operating conditions to allow operators to safely operate the grid closer to operational limits.

For example, the Bonneville Power Administration will use synchrophasor data as the basis of automated controls that will increase the operational capacity of the California-Oregon Intertie (COI). The 4,800-MW COI runs between the Pacific Northwest and northern California and frequently operates below capacity due to various system constraints. The COI energy flows can be increased by 100 MW or more using synchrophasors to take real-time control actions as needed—reducing energy costs by an estimated $35 million to $75 million over 40 years without any new high-voltage capital investments (WECC 2013). In another example, the Bonneville Power Administration used historical synchrophasor data on the actual performance of the 1,100 MW Columbia Nuclear Generating Station to validate and calibrate the plant's dynamic model, negating the need to take the plant offline for manual tests every five years to meet reliability criteria standards requirements. Energy Northwest, the organization that owns and operates the power plant, saved up to $700,000 from not having to take the plant offline for model validation (WECC 2012). More importantly, the model for the plant's behavior has been significantly improved, resulting in more accurate predictions of power system performance and more precise operating limits that are neither too conservative nor too optimistic.

In addition, the report outlines that utilities are applying various types of communications systems to meet their needs with respect to bandwidth, latency, reliability, and security. The application of smart grid technologies—such as AMI, distribution automation, customer systems, and synchrophasors—poses increased data communication challenges for legacy utility systems. To meet these challenges, utilities are investing in a range of technologies with varying bandwidth, latency, reliability, and security characteristics. Each smart grid application has unique bandwidth and latency requirements, often requiring utilities to use a combination of different communications technologies. These technologies can be deployed over either an existing public network (e.g., cellular and radio frequency [RF] mesh), which is often economical and readily available, or a licensed private network (e.g., communication over fiber, licensed RF mesh, or microwave links). Cost, reliability, performance, and technology longevity impact a utility's decision-making on communications technologies. While some utilities implement private communications networks, lower costs and increased technical support are causing public networks to gain momentum for utilities. Recently, public cellular carriers have lowered the per-megabyte cost of AMI communications, making wireless broadband technology (e.g., 2G/3G and 4G LTE networks) more popular with utilities. However, certain applications, such as feeder switches and synchrophasors, require higher speeds than what cellular networks can offer. RF-based mesh networks have emerged as the leading technology for AMI and distribution automation deployments in North America, although fiber optic cable is also used. Many U.S. municipal utilities also use microwave or Wi-Fi wide-area communications for AMI backhaul and distribution applications. To meet the high-speed, high security communication needs of its utilities, the Western Electricity Coordinating Council is using a secure, fiber-optic, wide-area network—built to the same standard as the nation's air traffic control network—that sends PMU data in less than 30 milliseconds to grid control centers.

Government and industry experts are also actively advancing interoperability through standards development, testing, and supporting policies. Yet solutions often lag industry needs, and continued coordination for standards identification and independent testing is needed to define the rules of the road and streamline new technology integration. Interoperability is the capability of two or more networks, systems, devices, applications, or components to connect effectively and share information securely with little or no disruption to the system or the operator. Interoperability is an essential enabler of grid modernization, allowing service providers and end users to integrate an expanding number of technology solutions and capabilities while maintaining reliable operations.

NIST formed the public-private Smart Grid Interoperability Panel (SGIP) in 2009 under a new effort to accelerate interoperability. SGIP engaged nearly 800 organizations and 1,900 individuals by 2013, when it became an independent, member-funded organization. Over this period, NIST leveraged the SGIP to develop and update the Framework and Roadmap for Smart Grid Interoperability Standards, which identifies agreed-upon standards and gaps for future development. SGIP actively works to address gaps and vet new standards, and has so far accelerated standards for exchanging energy usage data with consumers (Green Button); defined energy schedules, price, and demand response signals (used in OpenADR); and was instrumental in extending the SEP2 information model (a common vocabulary for messages) to support electric vehicle charging (CSEP). The report explains that the challenge is often not a lack of standards, but rather choosing common standards among diverse stakeholders, determining which products support them, and ensuring standards are consistently interpreted across a global marketplace of energy technologies. Even with strong coordination, standards alone do not achieve interoperability. SGIP and industry consortia support independent testing and certification programs that verify the ability of products from multiple technology suppliers to connect and work. Best practices and lessons learned from integration experiences are also being collected to educate the smart grid community and identify new gaps where progress on new standards, guides, and testing can simplify integration and maintenance.

It will take time to validate the full costs and benefits of smart grid technologies, especially as many utilities begin to leverage new data and information technology (IT) applications that will generate additional value from deployed smart grid systems. Utilities and their state and local regulators have widely varying experience with smart grid technologies and differing views on costs and benefits. As a result, investment decisions and deployment rates are determined at the local level—shaped by individual state energy goals, regulator views on allowable investments, and the level of smart grid maturity and experience at individual utilities. DOE has teamed with EPRI to develop a consistent, step-by-step framework for utilities to estimate project costs and benefits based on past demonstrations (EPRI 2012). This methodology continues to evolve as new performance data emerges and additional benefits are generated by adding enabling

technologies to existing smart grid systems. Improving interoperability and systems integration will enable utilities to realize new synergies among smart grid technologies.

The IT and communications infrastructure that support smart grid devices creates capabilities, costs, and integration challenges that are largely new to utilities, and difficult to value. The effort and time needed to integrate new networks and systems is difficult to predict; the lifecycle of digital devices and systems is largely undetermined; and the full range of new functions and operational capabilities will only be realized over time. Utilities do not yet know the extent to which IT and communications infrastructure may need to be upgraded and maintained as technologies evolve. Systems integration issues have challenged many demonstration projects, though several utilities have also realized large operational savings. Those utilities and regions with higher smart grid technology and IT adoption rates are facing the next level of smart grid technical and policy challenges more quickly.

Utilities and regulators are considering new benefit streams for valuing the technology and making investment decisions. For example, some utilities are now providing estimates of avoided customer costs of outages, rather than applying the traditional reliability indices (that merely provide the duration and frequency of outages) when submitting cost/benefit analyses of smart grid technology to their regulators. These value-of-service (VOS) estimates help utilities and regulators understand the customer-related and societal benefits of applying automated feeder switching and other system upgrades for improving reliability. This valuation approach will allow utilities and regulators to understand the true costs of power interruptions and help prioritize investments that lead to improved reliability and resilience.

Growing environmental concerns and decreasing technology prices are leading to greater adoption of distributed energy resources (DERs). These include distributed generation (e.g., rooftop solar and combined heat and power), electric vehicles, demand-response practices, and energy storage. DERs account for an extremely small percentage of U.S. generation capacity. However, installations will increase in scale and pace over the next decade (EPRI 2014), particularly in regions where policies and renewable portfolio standards are encouraging and rewarding adoption: 29 states, D.C., and two territories have renewable portfolio standards (RPS) that set percentage targets for renewable generation, and 17 states have mandates for solar and other DER (DSIRE 2014). 45 states have net metering policies, which credit the energy that consumers produce on site against the utility-provided energy they use (IREC and VSI 2014). 7 states, as well as utilities in other states, have established feed-in tariffs, which offer long-term contracts for energy producers with pre-established rates to encourage investment in distributed generation (EIA 2013a).

Subsidies, rebates, tax incentives, and financing incentives also promote DER adoption. Decreasing costs and local incentives for photovoltaic (PV) solar arrays spurred a 41 percent growth in adoption in 2013, and installations provided 12.1 GW system-wide by the end of 2013

(SEIA 2014). Non-utility (customer-based) solar arrays added 1,904 MW in 2013 (SEIA 2014) as system costs became competitive with retail power for some consumers (EPRI 2014). DER adoption will require more fast-acting, finer control of distribution grid operations to integrate variable, intermittent generation resources while maintaining high reliability. The future grid presents a complex set of relationships among new market entrants and third-party power producers with highly distributed energy resources that will need to be optimally managed in real time. DER technologies are being adopted at different rates across regions. High-adoption states like California, Arizona, New Jersey, and Hawaii (EPRI 2014) are on the frontline to address new challenges from effectively integrating intermittent, variable resources. In Arizona, for example, net metering laws spurred rooftop solar development by providing needed support for solar owners, but resulted in lost revenues for its utilities. As the number of rooftop solar customers increased, the Arizona Public Service Company (a distribution utility) asserted that non-solar customers now had to bear a higher amount of the costs for maintaining the grid—by as much as $1,000 per installed solar system—because such costs are built into the kilowatt-hour (kWh) rate. To ease this cross-subsidization issue, the Arizona Corporation Commission ruled in November 2013 to institute a fixed charge of $0.70 per kW per month. Also, growing adoption of renewable resources that provide variable power into the grid, like rooftop solar, may require energy storage systems to effectively balance quickly changing patterns of generation and demand. For example, in October 2013 the California Public Utilities Commission (CPUC) established an energy storage target of 1,325 MW for three investor-owned utilities with installations required no later than 2014. The purpose of the CPUC mandate is to optimize the grid (including peak reduction and deferment of upgrades), integrate renewable energy, and reduce greenhouse gases to meet California's goals (CPUC 2013).

In 2010, 663 U.S. electric utilities had 20,334,525 smart metering infrastructure installations, approximately 90 percent of which were residential customer installations. In 2011, the national average penetration rate for smart meters was about 14 percent, with rates in seven states exceeding 25 percent. Other than a major influx of investment through the ARRA, much of the cost of these deployments is recovered in the retail tariffs paid by consumers.

The smart grid is a topic with a lower popular profile than that of smart meters according to the GSGF report. In 2003, the U.S. DOE formed the Office of Electric Transmission and Distribution (now called the Office of Electricity Delivery and Energy Reliability) to lead a national effort to modernize and expand the electricity grid. In January 2004, the Office produced the National Electric Delivery Technologies Roadmap, which articulated an ambitious vision of a smart grid branded "Grid 2030". Grid 2030 envisaged intercontinental power transfers, real-time information flow from consumers, near-zero economic losses from power outages and disturbances, and open competitive markets in all segments of the electricity industry. Since then, the Federal Government has made significant commitments and funding available to stimulate smart grid activity. Support for the smart grid was codified in the federal

Energy Independence and Security Act of 2007. The DOE manages an R&D and demonstration program for smart grid technologies that matches funds for qualifying investments.

The GridWise Alliance is a smart grid stakeholder organisation that facilitates dialogue across the electricity sector and academia on matters pertaining to smart grid developments. The following projects are a sample of smart grid initiatives: Pacific Northwest Smart Grid Demonstration Project; Milto-Freewater City Light and Power; Flathead Electric Cooperative; NorthWestern Energy; Peninsula Light Company; Houston Smart Grid.

According to reports, the electricity grids of Canada and the United States are highly interconnected. There are at least 33 major transmission interconnections between them. They have formed the Electricity Grid Working Group focused on bilateral collaboration to facilitate the transition to a modernised electric grid. The Clean Energy Dialogue (CED) was also formed to enhance joint collaboration on the development of clean energy science and technologies to reduce greenhouse gas emissions.

The United States is a member of ISGAN.

Smart Grid-Cybersecurity Issues/United States:

Given the interest in the smart grid, enhancing cybersecurity is also essential and it should continue to be considered as part of a larger smart grid deployment strategy.

The 2012 GSGF report on the smart grid and country case studies noted that it is anticipated that over the next decade, smart grid activities in the United States will continue to attract federal attention in the areas of critical infrastructure and cybersecurity.

According to the 2014 DOE Overview on the Smart Grid, the increasing severity of weather-related events has sparked a growing interest in modernizing the electric grid to improve both reliability and resilience. With 11 weather events each exceeding $1 billion in damages—including Hurricane Sandy at $65 billion—2012 was the second costliest year (as determined since 1980) for disasters, which included storms, droughts, floods, and wildfires (NOAA 2013). Political support from New York and New Jersey governors for infrastructure hardening and upgrades following Superstorm Sandy in 2012 have since triggered regional utilities to develop billion-dollar investment plans. For example, the Public Service Electric and Gas Company (PSE&G) in New Jersey has proposed the Energy Strong program, which would invest $3.9 billion over 10 years to raise and harden vulnerable substations ($1.7 billion), add smart grid technologies that improve problem detection and response ($454 million), and strengthen or bury distribution lines ($60 million), among other upgrades (PSE&G 2013).

The DOE report further outlines that resilience and sustainability concerns have also increased interest in developing microgrids to provide dedicated power and islanding capabilities (i.e., rapidly connect/disconnect from the surrounding grid) during emergencies. Industry analysts

predict North American microgrid capacity may reach almost 6 gigawatts (GW) by 2020, up from 992 MW in 2013 (Navigant2013). However, optimal grid-to-microgrid interactions and microgrid functions will require more sophisticated, intelligent systems that apply advanced sensing, switching, and control technologies and effectively integrate distribution automation technologies and distributed generation. End-users such as military installations, hospitals, and university campuses with critical needs or favorable economics will likely be early adopters of microgrids.

The DOE report notes specifically that progress is also being made in instituting cybersecurity measures and advancing interoperability among devices and systems. Government and industry are actively developing tools, guidance, and resources necessary to develop robust cybersecurity practices within utilities. Government and industry experts are also advancing interoperability through standards development, testing, and supporting policies. It notes that continued coordination for standards and independent testing is needed to streamline new technology integration. As of March 2013, joint federal and private expenditures under ARRA totaled $6.3 billion from the 99 Smart Grid Investment Grants (SGIG), which represent the largest portion of ARRA investments. Between 2009 and 2015, DOE and the electricity industry will jointly invest more than $7.9 billion in the SGIG projects, which involve more than 200 electric utilities and other organizations to modernize the electric grid, strengthen cybersecurity, improve interoperability, and collect an unprecedented level of data on smart grid operations, benefits, and utility impacts (DOE 2013a). In the same time frame, an additional $1.6 billion in cost-shared funding will support energy storage demonstrations and regional demonstrations to assess emerging smart grid concepts (DOE 2014a). Another $100 million in federal funding has supported 52 smart grid workforce training projects in the same timeframe (DOE 2014a).

The 2012 report on country case studies by the GSGF noted for instance that public reaction to these deployments had been mixed. For utilities that articulated the benefits of smart metering, the consumer reaction has been positive, such as the deployments for Oklahoma Gas & Electric, San Diego Gas & Electric, as well as CenterPoint Energy in Texas. In other areas there has been major consumer pushback, fueled mostly by health and privacy concerns and a negative response to the increased electricity costs that have accompanied the smart meters. Class action suits were launched against Pacific Gas & Electric in California and against Oncor in Texas alleging health and privacy infringements, as well as overbilling. The suit against Oncor was dismissed in August 2010. As a result of these developments, the political profile of consumer sensitive issues related to smart meters is higher in the United States according to the GSGF report. In response, there have been a series of initiatives from government and industry to address these concerns. For instance, the Smart Grid Consumer Collaborative was formed by private sector companies, utilities and advocacy organizations to focus on smart grid messaging and educational tools for consumers. In California, legislation was enacted protecting the privacy of consumer energy consumption data, and the California Public Utilities Commission ruled that customers must be allowed to opt-out of smart meter installations (for a fee).

The 2014 DOE Report to Congress also highlights that concerns over meter safety, costs, and consumer privacy protections are being addressed, and enhanced consumer education is a key part of the solution.

The report further notes that while the application of customer-based technologies and time-based rate programs generally lags the deployment of smart meters, many utilities are beginning to actively engage their customers as smart meters and AMI make new information on electricity usage available to consumers (DOE 2013d). However, the availability of this personal electricity usage data has raised consumer concern over privacy and protection of their individual data. NIST, the Smart Grid Interoperability Panel (SGIP), and several states are addressing privacy policies and practices that more adequately secure personal data. At least eight states have now adopted rules governing third-party access to customer usage data (FERC 2013). In addition, industry organizations are now working with NIST, DOE, and their states to make smart meter energy usage data available to customers in a standard, usable format. Standardizing the format of usage information paves the way for new customer services, such as energy management cell phone applications and web tools or home energy-efficiency reports. DOE, NIST, and the White House Office of Science and Technology Policy (OSTP) launched Green Button, now an industry-led effort to simplify and standardize smart meter data and provide it in a secure and easy-to-read format. Currently, 48 electricity suppliers committed to provide Green Button data to more than 59 million homes and businesses (OSTP 2013). Some utilities have partnered with third-party service providers to develop customer "apps" that use energy use data to alert customers to potential cost savings from efficiency improvements or alternative rate programs (FERC 2013). Based on a December 2013 Presidential Memorandum, federal agencies are now required to use Green Button, where available (OSTP 2013). The executive summary of the report outlines that utility and state efforts are addressing the privacy concerns of electricity customers, and businesses are offering new energy management services to customers.

The DOE report to Congress in 2014 specifically outlines cybersecurity measures under cross-cutting technology efforts. It states that though cybersecurity remains a critical challenge, government and industry are actively developing the tools, guidance, and resources necessary to develop robust cybersecurity practices within utilities. In response to Executive Order 13636, NIST released the Framework for Improving Critical Infrastructure Cybersecurity in February 2014 to offer a prioritized, flexible, repeatable, and cost-effective approach to manage cyber risk across sectors (NIST 2014). This effort built upon NIST's collaborative work with industry to develop the NISTIR 7628 Guidelines for Smart Grid Cyber Security (NIST 2010). In the same month, DOE released a second version (1.1) of the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), which uses a self-evaluation methodology to help grid operators assess their cybersecurity capabilities and prioritize actions and investments for improvement (DOE 2014b). The ES-C2M2 provides a complementary, scalable tool for NIST Framework implementation. To date, 104 utilities covering 69 million customers have downloaded the ES-C2M2 toolkit. Combined with the Risk Management Process that DOE

released in 2012, and upcoming cybersecurity procurement language, utilities now have a holistic view of cybersecurity best practices across business processes (DOE 2012b).

In addition, DOE required each recipient of SGIG funding under ARRA to develop a Cybersecurity Plan that ensures reasonable protections against broad-based, systemic failures from cyber breaches. DOE followed up with extensive guidance on plan implementation, annual site visits to the 99 recipients, and two workshops to exchange best practices. As a result, recipient utilities are instituting organizational changes and leveraging new tools to strengthen organization-wide cybersecurity capabilities.

Advanced technologies with built-in cybersecurity functions are now being developed and deployed across the grid. For example, research funded by DOE has led to advancements in secure, interoperable network designs, which have been incorporated into several products, including a secure Ethernet data communications gateway for substations, a cybersecurity gateway (Padlock) that detects physical and cybersecurity tampering in field devices, and an information exchange protocol (SIEGate) that provides cybersecurity protections for information sent over synchrophasor networks on transmission systems. In addition, the University of Illinois developed NetAPT, a software tool to help utilities map their control system communication paths, allowing utilities to perform vulnerability assessments and compliance audits in minutes rather than days.

The United States is also a member of the GSGF.

6.20 Viet Nam

6.20.1 Economy Energy Resources

According to the APEC Energy Overview Study published in March 2014, Viet Nam's territory has a significant endowment of fossil energy resources such as oil, gas and coal, as well as renewable sources such as hydro, biomass, solar and geothermal. It has become a net energy exporter, mainly of crude oil and coal. Oil is still the most important energy source in Viet Nam. Its gas reserves are more promising than its oil reserves. While gas resources are found in many parts of Viet Nam, nearly all of the largest reserves are found offshore.

6.20.2 Current Cybersecurity Nexus

Defining critical infrastructure protection

Open source searches do not currently produce a list of material related to the definitions of critical infrastructure protection or critical infrastructure in Viet Nam.

Defining cybersecurity

According to the 2015 ITU report on Viet Nam, specific legislation on cybercrime has been enacted through the Law on Information Technology. Specific legislation and regulations related to cybersecurity has been enacted through the following instruments: 1) Law on e-transactions - Decree No. 90/2008/ND-CP against Spam 2) Intellectual Property Law - Technology ended by Law No. 36/2009/QH12; 3) Law on Telecommunications - Circular. 12/2008/TT-BTTTT(12/2008) on Anti-Spam; 4) Decree on Information Technology Application in State Agencies' Operations; and 5) Decree No. 63/2007/ND-CP Providing for Sanctioning of Administrative Violations in the Domain of Information. Viet Nam has an officially recognized national CIRT known as VNCERT. The national CERT, a unit within the Ministry of Information and Communication, was established in 2005. Its tasks include the coordination of cyber incident response and the development of computer network security. It does not have an officially approved national cybersecurity framework for implementing internationally recognized cybersecurity standards. There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals. It does not have an officially recognized national or sector-specific cybersecurity strategy. There is no national governance roadmap for cybersecurity in Viet Nam. The Ministry of Posts and Telematics and Ministry of Information and Communication coordinate cybersecurity. There is no information on any framework for sharing cybersecurity assets across borders with other nation states. There is no information on any framework for sharing cybersecurity assets between the public and private sector. Viet Nam is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services.

According to the 2013 UNIDIR Cyber Index on International Security Trends and Realities, Viet Nam’s Ministry of Public Security has proposed the establishment of a high command to provide electronic and cybersecurity for the military, citing the “eventuality of cyber wars” as a key impetus for a cyber-military organization. The Director of the Department of Information Technology within the Ministry of Public Security has been an advocate for improving operational cyber capabilities.

The General Department of Logistics and Technology of the Ministry of Public Security, the national CERT, and the International Data Group continue to draft plans for information security advancements throughout the next decade. Viet Nam is planning to invest $42 million to secure sensitive information and to establish a National Centre for Technology and an Agency for Information Security. As part of this investment, it approved a national master plan to secure domestic cyberspace for the period of 2010–2020 and created the National Network Security Technical Centre to develop a system for monitoring, early warning, and incident response, to be operational within two years.

According to input in July 2013 from the Information Technology Industry Council (ITI) on Viet Nam’s Draft Law on Information Security through which the Government is trying to improve

cybersecurity, ITI believed certain proposed actions in the draft law, if not revised or implemented carefully, would present serious challenges. In particular, it cites concern over certain provisions relating to personal information that might hinder the ability of industry to innovate and to engage in the necessary transactions to offer optimal products and services.

The law's provisions touch on cybersecurity, personal information, and content/filtering. Viet Nam generally describes what is often termed as cybersecurity to be "information security". The draft law requires individuals and organizations to report any information security "infringement or incident" to related competent authorities. Article 6 on the state's policies on information security emphasizes training, human resources, growing the market for information security product and service imports, and creating a competitive environment for information security activities, including R&D.

6.20.3 Cybersecurity Challenges (Issues)

Open source searches do not currently produce material related to the current and planned cybersecurity-energy nexus in Viet Nam.

Several cyber-related policy opportunities and challenges for further consideration:

Geopolitical considerations and perceived threats that should be considered. The challenge is that since it can often be difficult to accurately attribute responsibility for a cyber incident, misappropriation could lead to misunderstanding or an escalation in tensions. This is especially challenging when non-state actors could be to blame and contemporary cybercrime levels are on the increase in the region.

Greater connectivity in the region could raise the probability of transnational crime and cross-border cyber-related incidents. With increasing access to high-speed networks, low-level cybercrime has already risen in the ASEAN region. In Asia, policy experts further suggest that the growth of cybercrime could increase political instability.

In terms of nuclear power development, according to the APEC Energy Overview in 2014, the Government is carefully reviewing the safety issues and considers them the first priority for review. In June 2010, the Prime Minister approved a plan to build and develop a nuclear technology industry but after the Fukushima nuclear power plant accident, safety issues in the development and operation of nuclear power plants became a top priority and the programme's timeframe and the amount of capacity to be developed over the long term are under careful review.

Given these plans for nuclear power, Viet Nam should also seek to ensure that extensive computer security/cybersecurity measures are in place. The IAEA (as well as several nation

states) provides guidance for consideration by states, competent authorities, and operators. The aim is to prevent the theft of material or sabotage of plants and facilities.

Given the economy's dependence on oil and gas as well as planned projects for oil refineries and gas pipelines, it should also very closely consider possible cyber threats to oil and gas suppliers particularly since many major global oil and gas producers have fallen victim over recent years to cyber-attacks or had their networks infected. This could possibly cause damage but breaches may also cause high damage to corporate assets, public infrastructure and safety, or the wider economy. Analysts have noted that while intrusions previously focused on the theft of IP and business strategies, recent malware attacks reflect a change towards attacks with the potential for causing physical disruptions to the oil and gas supply chain.

According to the 2015 ITU profile on Viet Nam, the Ministry of Information and Communication has signed a memorandum of understanding with Microsoft, for example, for both parties to cooperate on bolstering cybersecurity, cloud infrastructure and application development, and infrastructure management skills in Viet Namese businesses.

Therefore, for capacity building related to cybersecurity issues specifically in the energy sector, should not solely focus on technical capacity building but also include policy as well as legislative, organizational, and law enforcement training. In addition, external offers of capacity building should also be coordinated and capacity building should reflect the unique needs of Viet Nam.

It is in the interest of Viet Nam as well as the international community that measures be enacted to mitigate possible weak links and havens of vulnerable ICT infrastructures. Viet Nam is not highly developed in terms of ICT development, and given that it has a less developed ICT infrastructure and less connected critical infrastructure means that this could prove to be an advantage for the economy. As it becomes more connected, lessons could be applied from the experience of other states in countering cyber-related threats, best practice policies, and measures may be implemented. Both security and data privacy by design could be incorporated from inception in the development of ICT and connected critical infrastructures.

According to the APEC Energy Overview 2013, Viet Nam Electric Power Group (EVN) is a state-owned utility founded in 1995. The group is engaged in the generation, transmission and distribution of electricity for the whole of Viet Nam. Apart from EVN, other companies are also responsible for much of this, supplemented by the Build–Operate–Transfer and independent power producer schemes run in partnership with private investors. In 2010, companies other than EVN owned over 53 percent of the power supply system. In addition, Viet Nam's gas and oil upstream sector is open to all, while the downstream functions such as transmission, distribution (except that for petroleum products), and marketing are almost all within the PVN monopoly. PVN and private companies, including foreign companies and joint ventures with PVN, carry out oil and gas production but all are required to sell through PVN.

Consequently, specific public-private sector considerations relating to cybersecurity and the energy sector should be further examined.

Regarding multilateral efforts, at the regional level, Viet Nam is a member of ASEAN and a participant at the ASEAN Regional Forum (ARF).

6.20.4 Future Cybersecurity Nexus

There is insufficient data on this topic for Viet Nam. This is a potential area of future growth.

6.20.5 Smart Grids

2014 reports online outline that some emerging countries, such as Thailand, Malaysia, Indonesia, and the Philippines, are making plans to deploy smart grid technology. While this region is currently behind other global regions in terms of smart meter deployments and regulatory frameworks, its smart grid market is growing. There are already smart grid pilot projects in several countries throughout the region. By 2022, Southeast Asian countries will likely have an electricity demand profile similar to Latin American countries where large-scale smart meter deployments already exist. The region's current electricity consumption rates are among the lowest in the world, while distribution loss rates are comparatively moderate, offering less short-term savings potential compared with other global regions. Additionally, regulatory frameworks remain largely undeveloped in the region. Even in the more advanced countries, deployments are still at the initial pilot level.

These 2014 reports say that investment in Southeast Asia will include smart metering and the modernization of electricity transmission and distribution networks with sensors, communications and software. By 2024, the largest markets will be Thailand, Indonesia, Malaysia, Singapore, the Philippines, and Viet Nam, according to a recent study by Northeast Group LLC. Southeast Asian economies are just beginning on the path of modernising their electric infrastructure. Electrification programs and growth in renewable resources will also drive investment. Singapore is currently leading the region in development but later in the decade, the large markets of Thailand, Indonesia, Malaysia, Viet Nam and the Philippines will account for significant smart grid investment. Several countries in the region have drafted smart grid roadmaps and pilot projects are widespread. Regulatory frameworks are still developing but momentum will grow over the next several years. Both utilities and vendors are already working together to ensure preparedness when regulations are finalized. Many vendors are active across the region (these include ABB, Alstom, Echelon (NES), EDMI (Osaki), Elster, Enverv, GE, Itron, Schneider, Secure, Siemens, Silver Spring Networks, ST Electronics, Trilliant and other global and local vendors).

According to a 2013 report on the market potential for smart grid technology in Viet Nam, the Viet Namese power system is still in distributed form, not connected into a unified system and lacks many important elements.

The “Electricity Master Plan Number 7”, which was implemented and approved in July 2011 for the period 2011-2020 outlines plans including generation, power transmission and distribution, power grid linking with other regional economies. It also gives solutions and indicates tasks of ministries, local and relevant units as well as a list of power projects and power transmission network to be constructed and renovated. In this decision, the Prime Minister assigned MOIT to organize the development of a “Roadmap of Smart Grid Development in Viet Nam” proposal for approval.

Regarding grid development, the decision highlighted:

- Research on implementation of smart grid technology to enable the interaction between households using electricity with the power grid in order to reduce grid development costs and improve the stability of the power grid; and application of modern technologies to improve the quality of distribution grids, step-by-step put the power grid into underground infrastructure in large cities to limit its influence on landscape and environment. Utilise modern technology in investment, operation and management to reduce power losses. These activities are oriented towards building Smart Grid, Smart Communities in order to reduce power losses and improve energy efficiency.

The Proposal on Roadmap of Smart Grid Development in Viet Nam (motivated by Decision 1208/QD-TTg) was developed by ERAV/MoIT and approved in October 2012. This is the most important document related to smart grid development in Viet Nam. It outlines the plan for Viet Nam's electricity sector for 2011-2020 and proposes short-term, medium-term and long-term goals for the development of the Viet Namese smart grid, as well as the master plan for deploying smart grid in Viet Nam.

According to the roadmap, the targets of smart grid development in Viet Nam include: 1) the implementation of smart grid is aimed at promoting energy conservation as well as encouraging the development of clean energy technologies and supporting industries. The targets and the road map have been split into three phases. According to this report, current smart grid activities/projects in Viet Nam include: 1) TOU meter program; 2) Research program load (Load Research). EVN in cooperation with ERAV perform these activities for deployment in Hanoi Power Corporation and Ho Chi Minh Power Corporation. The program was implemented in 2011 and 2012. In the program, 1100 smart meters, transmission lines, a server, and software were installed. EVN is the project administrator, which manages the database and perform measurements and conducts load research; 3) Project "10-Years Road Map for Smart Grid Distribution in Viet Nam". EVN Northern Power Company commissioned this 10-year road map from the U.S. Brattle Group. The project focuses on smart grid applications in distribution grid and considers the implementation of a demand side management program at Power Companies. The proposed project contains the following components - smart metering, customer programs, and distribution automation; 4) Project SCADA/ EMS. This investment project by the

Moderation Systems Center National Implementation is to equip the new SCADA/EMS system for four new Operating Centers supported by a loan from the World Bank. The project was awarded in 2012; 5) Project Installation of Electronic Meters. This project of the EVN Central Power Cooperation is a DEP project of the World Bank to install approximately 10,000 electronic meters.

Regarding future pilot programs and projects, in order to implement the smart grid development plan, ERAV-MoIT proposes five main programs and two pilot programs:

- Program 1: Improvement of Operational and Managerial Efficiency of the Power Grid:
    - For the transmission grid:
        - Investment in remote system monitoring, data collection & processing (SCADA / EMS).
        - A capacity building project for the Electric Regulatory Centers, National Power Transmission Corporation (NPT).
        - Deploy applications to improve transmission grid efficiency.
    - For electricity distribution networks:
        - Step-by-step development of infrastructure monitoring and control systems (SCADA/DMS).
        - Training and capacity building for the General Power Companies and Power Companies.
        - Develop "Performance standard indications" for the distribution grid to monitor operational efficiency.
        - Upgrade the grid, narrow radius of power supply and perform the management measures to reduce energy loss.
        - Research distribution grid structures capable of integrating distributed generation sources, including renewable energy focus.
- Program 2: Installation of AMI Infrastructure:
    - Perform pilot projects to research and evaluate the effectiveness of modern ICT infrastructure (including smart meter, communication lines, data acquisition, storage and process).
    - Step by step deployment for customers according to the approved financial mechanisms.
- Program 3: Encouragement of Customers' Participation in Energy Usage Management:
    - Develop and issue the legal framework allowing smart grid applications to give permissions to customers.
    - Deploy the application for customer's participation, based on load management; billing applications, information provision for customers, power cut management, etc.
- Program 4: Integration of Renewable Energy:

    - Research and promulgate policies to encourage use of renewable energy at both centralized and distributed levels.
- Program 5: Green Transportation:
    - Establish the mechanism for the development of electric vehicles and car charging stations.
    - In the short term (2012-2016), some pilot programs should be deployed early in order to evaluate their effectiveness to serve as the basis for extension.

Two prioritized projects are:

1. Installation of AMI Infrastructure: Installation of smart meters for large customers in the General Power Corporation Ho Chi Minh City along with transmission lines and server systems for data collection and data processing. Implementation of selective applications on the AMI platform. The purpose is to test ICT infrastructure and smart grid applications and the organizers are ERAV and General Power Corporation of Ho Chi Minh City.
2. Integration of Renewable Energy: Installation of ICT infrastructure between small hydro power plants (connected to the medium voltage grid) connected to the SCADA/DMS of the Central Power Corporation (CPC); training and capacity building for operational staff; study the effects of the operation of small hydropower plants to the operation of CPC distribution grid. The organizers are ERAV and CPC.

In the context of Viet Nam, smart grid is a platform that includes: 1) the grid infrastructure including distributed generation, transmission, distribution, and customer grid that contain smart elements (such as SCADA, automated substation control, etc.) to optimize and increase grid stability, power quality, and reduce loss; 2) distributed generation with renewable energy; 3) Advanced metering infrastructure for large customers; and 4) a platform to encourage the culture of energy saving and conservation, and stimulate the integration and development of renewable energy.

Currently, the investors in smart grid include the Government, the World Bank, the Asian Development Bank, and several foreign banks that are investing in grid extension and upgrading, like German KFW. In the short and mid-term, the focused smart grid technologies are transmission automation and AMI for large customers. Other technologies will have much smaller shares.

According to this report, the most serious barriers to smart grid in Viet Nam include the difficulty in financing; lack of expertise; no clear policies from EVN and MOIT; low public awareness, especially among electric authorities, power companies and customers on the benefits of smart grid; and a legal framework for smart grid deployment and smart grid applications is under development.

Regarding smart grids, reports outline that they can play an important role in the deployment of new electricity infrastructure in developing countries and emerging economies by enabling operation that is more efficient and lower cost. Small "remote" systems – not connected to a centralized electricity infrastructure and initially employed as a cost-effective approach to rural electrification – could later be connected easily to a national or regional infrastructure. As a means to access to electricity in sparsely populated areas, smart grids could enable a transition from simple, one-off approaches to electrification to community grids that can then connect to national and regional grids.

This is significant given Viet Nam's schemes for rural electrification and increasing the proportion of rural households with access to electricity. About 70 percent of the economy's 86 million people live in rural areas with about 4 percent of households in those regions lacking access to electricity in 2012 according to the 2014 APEC Energy Overview.

7 Challenges

Critical infrastructure entities in the energy sectors face the likely event of a brute force attack on their internet-facing control systems. Anything that is connected or integrated through the internet could be attacked at some point. Most recently, exploitation techniques and readily available tools have been successful in compromising company networks.

Although attack methods and techniques could be similar from one sector to another, this may also not always true for every attack case. In FY12 in the United States for example, the DHS ICS-CERT group responded to 198 cyber incidents across all critical infrastructure sectors. Of the 198 incidents, 41 percent were in the energy sector and ranged from a wide variety of threats. The incidents involved weak cybersecurity configurations or defaulted credentials. In comparison, for the first half of FY13, ICS-CERT responded to 204 incidents across all critical infrastructure sectors; 54 percent of the incidents were in the energy sector [39]. Figure 19 illustrates the number and percentage of incidents in each sector that reported incidents during the first half of FY13. The majority of the incidents involved attack methods such as water holing, SQL injections, and spear-phishing attacks [38].

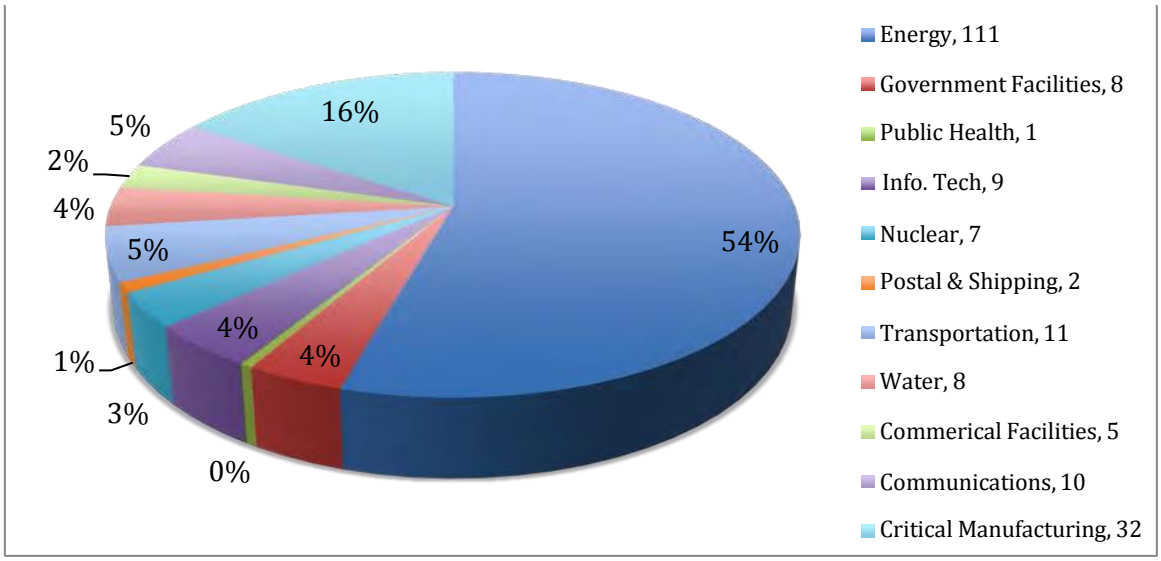

Figure 19. Incident Reports during First Half of Fiscal Year 2013

The motivation and origin of an attack can vary, ranging from gaining information on intellectual property, data thefts, and exploiting vulnerabilities to manipulating control devices to create disruptive and/or catastrophic events. Threats do not originate only from the outside; they also originate from an insider (either with intention or unknowingly initiating an attack) within the company.[39] The threats' range includes (but is not limited to) the following:

- **Nation-States:** Conduct IP theft and espionage. A nation-state's intelligence, security and military services bring the most sophisticated and best-rounded tools and resources to conduct cyber intrusions against the energy industry.

- **Hacktivist:** Seeks to expose and embarrass energy companies. Hacktivists target energy sectors to protest environmental and other similar issues. An individual or groups of individuals seek unauthorized access to computer files or networks in order to further social or political ends.

- **Opportunistic Criminals:** Focus on stealing customer information, identities, payment data, and other sensitive information, which can be quickly converted for financial gain.

- **Malicious Insiders:** Conducts espionage, sabotage, or unauthorized disclosure of information. May include an employee, consultant, or other trusted partners with authorized access to sensitive information that can inflict harm. Insiders can act alone or in collusion with an outsider.[44]

As the smart grid technology continues to grow and gain momentum, an increase of new energy systems will be connected to the internet, which will introduce new security vulnerabilities because of the countless connected devices. Modern systems continue to increase in complexity; they may include SCADA or ICS systems that sit outside the traditional security walls interconnected to the main facility. [39], [40] Furthermore as the systems become more complex, regulations and requirements will become more stringent with regard to compliance with current/new standards.[44] In addition, many economies have also started to open the energy market, adding smaller contributors to the electric power grid (i.e., private water power plants, wind turbines, or solar collectors), which can also have an effect on power outages on the larger grid if they are improperly managed due to the lack of available IT staffing support. Private contributors may also deploy new technology that may have gone untested or contains other known vulnerabilities, ultimately exposing the integrity of the whole power grid. [39], [40]

In July 2014, it was reported that more than 1,000 energy companies in Europe and North America had compromised by an Eastern European hacking group. Eighty-four countries were affected, with the most targets in the United States, Spain, France, Italy, Germany, Turkey, and Poland. Since 2013, a group known as Dragonfly has been targeting electric, water, oil, and gas organizations that use ICS systems. Furthermore, cyber espionage groups aim at energy grid

operators and industrial equipment suppliers as a way to breach the security walls and access the infrastructure's network. Targets against ICS systems are the biggest threat to critical infrastructure; cyber-attacks are expected to increase because industrial networks offer a relatively easy way into heavily protected network systems. Also, attackers are becoming more sophisticated in the ways that they steal and gain access into infrastructure networks. [40] [41] Table 5 provides a list of some of the publicly reported cyber-security related incidents in the APEC Economy Region.

Table 5. Examples of Cybersecurity-Related Incidents in the APEC Economy Region [24] [42] [43] [49] [50] [51] [52]

Economy	Nature of cyber incident	Month and Year
Brunei Darussalam	IT Protective Security Services recorded more than 2,000 cyber-attacks in 2010-12 (62 percent virus attacks, 26 percent spam, 7 percent defacement, and 4 percent scams).	November 2012
Canada	Telvent Canada (now Schneider Electric), an energy technology firm whose systems help run oil and gas pipelines, had a security breach because the company never received the federal agency warning about hackers targeting critical infrastructure six months prior to the incident. Telvent stated it never received the alerts because it is a vendor that builds systems for energy companies and is not an infrastructure company. Records show the Canadian Cyber Incident Response Centre sent out four alerts to technology experts in critical infrastructure in the month before the breach. The alerts warned of hackers sending malicious emails disguised as internal messages to staff, and outlined preventative steps to take to protect themselves. The hackers installed malicious software and stole project files related to Oasis SCADA.	September 2012
Indonesia	A group called Anonymous Indonesia defaced over 12 government websites following the arrest of Wildan yani Ashair, who was accused of hacking the president's website. In three years, government websites have been attacked over 36.6 million times.	January 2013
	Serious online fraud schemes involving losses over $500K accounted for 40 percent of the 176 cybercrime cases reported during the first four months of 2013.	April 2013

Republic of Korea	Computer systems at a South Korean nuclear power plant were hacked. Documents belonging to KHNP (part of the stat-run utility Korea Electric Power Corporation) were leaked online.	December 2014
	South Korea financial institutions as well as the Korean broadcaster YTN had their networks infected in an incident said to resemble past cyber efforts by North Korea.	March 2013
Malaysia	Police recorded 24 cases of hacking between January and September 2012, with estimated losses of $1.1 million.	November 2012
	Hackers posted a statement on the Department of Information website that Prime Minister Datuk Seri Najib Tun Razak was resigning.	February 2013
	Alternative radio stations for the opposition and the news portal Sarawak Report claimed to be targeted by distributed denial of service attacks. AFinSpy sample – part of the remote intrusion and surveillance software FinFisher, distributed by Gamma International – appeared to be specifically targeting Malay speakers.	March 2013
The Philippines	Chinese hackers in connection with the South China Sea dispute allegedly defeated several government websites. Philippine hackers retaliated by launching similar attacks against Chinese websites.	June 2012
	Anonymous Philippines attacked prominent commercial entities, civil society organizations, and the Government in protest over the contentious Cybercrime Act.	September 2012
	Anonymous Philippines hacked the president's website for allegedly mishandling the Sabah conflict and accused the Government of allowing Malaysian troops to kill Filipino citizens.	March 2013
	After the Philippine Coast Guard shot a Chinese Taipei fishing boat, Chinese Taipei and Filipino hackers conducted a "cyber battle" using the Chinese Taipei and Philippine Government websites.	May 2013
Singapore	A report by Trend Micro Smart Protection Network showed that over 900 Singapore citizens were victims of online banking fraud in the first quarter of 2013.	May 2013

Thailand	The Turkish Agent Hacker Group compromised McDonald's Thailand, releasing the contact information of 2,000 users. The same group claimed responsibility for an attack on the Red Cross Thailand website, protesting disrespect of the prophet Mohammad accompanied by a Turkish flag. The group previously defaced the website of Pepsi Hungary with the same message.	October 2012
	From January to May 2013, there were 1,475 intrusions into government sites and hundreds of malware attacks and phishing incidents.	June 2013
United States	In May 2014, DHS ICS-CERT reported an attack by a sophisticated hacking group against a U.S. public utility. The hacking group compromised its control system through an internet portal that enabled operators to access the utility's control system, but there was no evidence that the utility's operations were affected.	May 2014
	In fiscal year 2014, there were 79 hacking incidents at energy companies in the U.S.; 145 reported incidents the previous fiscal year.	FY 2013 & FY 2014
	DOE's Pacific Northwest National Laboratory shut down internet access and email services following a sophisticated cyber-attack. The attack seemed to be similar to a spear-phizing attack that occurred earlier in the year in April 2011 at Oak Ridge National Laboratory. Officials shutdown most computer services for employees, including email, SharePoint, wireless network and internet access immediately after discovering the breach.	July 2011
	A 'Trojan Horse' malware was inserted by hackers penetrated software that runs much of the nation's critical infrastructure. The hacked software is used to control complex industrial operations like oil and gas pipelines, power transmission grids, water distribution and filtration systems, wind turbines and even some nuclear power plants.	November 2014
Viet Nam	The Viet Namese version of Badu, a Chinese search engine, apparently infected computers with spyware and adware that, once downloaded, allowed compromised computers to be controlled remotely, have data extracted, and be used as "zombies" for distributed denial of service attacks.	July 2012

8 Recommendations

Included here are recommendations from private and government-related sectors for making the cyber-energy nexus secure, efficient and interoperable.

8.1 Edison Electric Institute Recommendations and Initiatives

Edison Electric Institute provides its initiatives to protect a nation's grid from cyber threats. For the electric power industry, protecting a nation's electric grid and ensuring a reliable supply of energy are the top priorities. In the electric power industry, cybersecurity has been a growing priority and the electric energy sector has been applying threat mitigation actions to preparations, prevention, response, and recovery in its operations in the United States. The electric power industry partners with federal agencies, including the Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and the DOE to improve sector-wide resilience for cyber threats. The industry also collaborates with the NIST, NERC, and federal intelligence and law enforcement agencies to strengthen its cybersecurity capabilities.

8.1.1 Threat Scenario Project

In 2011, the Edison Electric Institute, in conjunction with private sector experts and its member utilities, initiated the Threat Scenario Project to identify cyber threats and practices to mitigate the threats. Identified threats included coordinated cyber-attacks, as well as blended physical and cyber-attacks. The project established common elements for each threat scenario, including a description, likely targets, potential threat actors, specific attack paths, and likely impacts of a successful attack. The project continues to evolve as the threat landscape changes in order to keep the industry prepared to identify and defend against emerging cyber threats. [37]

8.2 U.S. National infrastructure Advisory Council (NIAC) Recommendations

In October 2010, NIAC issued a report, "*A Framework for Establishing Critical Infrastructure Resilience Goals*," with nine recommendations. The recommendations are:

1) The White House should initiate an executive-level dialogue with electricity and nuclear sector CEOs on the respective roles and responsibilities of the private and public sectors in addressing high-impact infrastructure risks and potential threats, using an established private sector forum for high-level, trusted discussions between industry executives and government leaders. Both senior public and industry private sector leaders need to better define respective roles and responsibilities in preparing for and recovering from major events, including frequency events. This recommendation calls for new public-private dialogue that uses an existing executive-level forum of public leaders and private sector CEOs to focus on high-level policy issues; creation of a framework for public-private collaboration on defining roles

and responsibilities; and, finally, recommendations to strengthen overall resilience for high-impact and low-frequency risks [35] [36].

2) The nuclear and electricity industry should each develop an emergency response plan that outlines a coordinated industry-wide response and recovery framework for a major nationwide disaster. Currently the nuclear and electricity industries have robust emergency response plans and exercise them regularly, but there is no industry-wide plan to address major national disasters. Relationships between companies and their State, regions, and communities exist and are established, but relationships, roles, and responsibilities at the national level are not very well defined. NIAC recommends that coordination and development of emergency response plans be led by CEOs in each sector and aligned with the National Response Framework and National Incident Management System. The emergency response plan should include and clearly identify the types of disasters that will activate the plan and identify who makes that decision; clarify roles and responsibilities within the electricity industry and between various public and private sectors for specific functions; set priorities and actions to take place when decisions are made; describe expectations at the federal and state government levels for certain types of disasters; and, finally, provide a structured communication plan with appropriate protocols. The responsibilities to coordinate and develop emergency response plans should be determined by the leadership of each sector. [36]

3) DHS and other federal agencies should improve information sharing with the private sector by providing focused, actionable, open-source information on infrastructure threats and vulnerabilities. DHS and other government agencies should work to develop more effective ways to share classified information with the electricity and nuclear sectors, or translate it into useful non-classified information. [36]

4) All critical infrastructure sectors should consider adopting the industry self-governance model exemplified by the Institute of Nuclear Power Operations (INPO) and the North American Transmission Forum (NATF) to enable the private sector to collaborate on industry-wide resilience and security issues outside the regulatory compliance process. This recommendation will help share evaluations, issues, and solutions with the sectors in an honest and trusted environment, but outside the regulatory process. The self-governing model clearly addresses transmission reliability and resilience issues across the electrical sector and also improves overall accountability, communication, and performance. Adopting this model can provide regular evaluation of the resilience and security of sector assets and systems, establish performance objectives, train and educate sector employees, and create CEO accountability for any shortcomings in performance. [36]

5) Promote the use of NIAC-developed framework for setting resilience goals in Critical Infrastructure and Key Resources (CIKR) sectors and for providing a common way to organize resilience strategies within federal and state governments and CIKR sectors. This process enables a critical infrastructure to recognize its resilience goals and also to uncover gaps in sector resilience to develop options to address them. The process is intended to establish a baseline of current practices, develop high-level resilience goals, test the sector's resilience in a high-impact scenario, and address gaps and layers through a public-private dialogue. [36]

6) DHS should support modeling and analysis studies of the cross-sector economic impacts of CIKR failures using tools such as input-output analysis. Many CIKR sectors are interconnected, which can help resilience, but at the same time can create new opportunities to cascade across sectors, regions, and economic systems. As infrastructure become more interconnected, it is important to understand the impact of sector failures and their overall effects. [36]

7) Federal and state agencies should allow cost recovery for utility investments that increase infrastructure resilience. Investments in reliability and resilience beyond those required by existing regulations must be justified as benefiting the customers because ultimately they will be who pays for them. To encourage the private sector to invest in the resilience of transmission and distribution systems, government agencies should modify their processes for allowing rate adjustments. [36]

8) Electricity industry and government leaders should pursue options to mitigate supply chain vulnerabilities associated with extra-high voltage transformers. This recommendation suggests that the Government should providing incentives to encourage additional domestic manufacturing of extra-high voltage transformers and also standardizing transformer designs and development of a recovery transformer. [36]

9) The Federal Government should work with owners and operators to clarify agency roles and responsibilities for cybersecurity in the electricity sector, including those for cyber emergencies and national-state threats. To avoid confusion and duplicating and/or conflicting actions, government and private industry leaders should work to coordinate responses and declare the need for emergency action. It is recommended that public leaders work with electricity sector CEOs to clarify public and private roles and responsibilities in management cyber risks that could compromise the integrity of the bulk power systems. [36]

8.3 Pricewaterhouse Coopers (PWC) Recommendations

PwC outlines an integrated approach to assessing cyber threats and protecting assets. Although there is no failsafe method to ensure absolute security, the Chief Information Security Officers (CISOs) and the security team can take action to create a security program that enables an

organization to prepare for and quickly detect attacks, protecting its most valuable data and system's operations.

8.3.1 Take Charge of Your Cybersecurity

A successful cybersecurity program will define the role and assign who is responsible for the organization's cybersecurity and other security. The CISO and the overall corporation executive leadership team must commit to cybersecurity as a business imperative. Energy companies that introduce and execute a security program into strategic decision-making across the business are better able to recognize current and future security risks, navigate the threat landscape in pursuit of business opportunities, and allocate security resources more effectively. With a well-defined cybersecurity program, the company is able to clearly explain cybersecurity strategies to all stakeholders (i.e., shareholders, investors, employees, regulators, and others).

8.3.2 Know What You Need to Know

Understand your adversary and how they relate to your organization. The cyber threat may change on a daily bases. Keep in mind where you do business, how you conduct business, and with whom you do business with. The security team needs to understand what their cybersecurity strategy is protecting, from whom, and what their role is in protecting an asset. Without a proper understanding, the most valuable asset can be left vulnerable and unprotected. The cybersecurity strategies must also consider and take into account the company's relationships such as supply chain vendors, service providers and strategic partners, employees, and all customers. Each plays a part in both risks and opportunities for the company.

8.3.3 Have a Smart, Proactive Action Plan

An effective cybersecurity plan is both threat-based and asset-based. Successful energy companies make comprehensive security resource investments based on informed risk assessments, rather than just from compliance requirements and/or standards. Also having an integrated security strategy is an important business model, which considers all levels of business as well as the full scope of security (cyber, physical, personnel, technical, and non-technical) in the security model. Having a public-private partnership strategy is another important element to keep in mind. An increase in government focus and collaboration on corporate cybersecurity is believed to be an opportunity to further enhance your protection. Successful companies implement a security information-sharing plan that includes enterprise ecosystems, industry peers, cross-industry groups, and government agencies.

8.3.4 Be Informed, Proactive, Secure, and Ahead of the Market

Energy companies with a successful cybersecurity strategies focus on: 1) Prioritizing corporate resources and protecting those things that are of value to both the company and the adversary; 2) proactively implementing cybersecurity practices that not only protect the business, but also move them ahead in the global market; and 3) effectively engaging with policy makers and

regulators, preparing to answer inquires in regard to current and future cybersecurity initiatives. [44]

8.4 Security Think Tank Recommendations

A security think tank has outlined the following three steps to effective incident response, indicating how organizations can take steps to protect themselves from a very plausible attack.

1) Develop a Plan. A simple initial planning process will reveal gaps in areas of communication, policy, technical capabilities, roles, and responsibilities that may require urgent attention. A plan must include working with multiple departments in the company (i.e., information security, legal, human resources, communications, and vendor management) headed by a core team consisting of representative personnel from the multiple departments. The core team should take the lead in responding to incidents.

2) Practice and Perform Exercises based on Scenarios. Cyber-attack will impact numerous departments, and all must be prepared to respond quickly. Performing a simulation exercise can prevent confusion and help set clear expectations, post-breach actions, and responsibilities.

3) Respond Decisively. Quick response to compromised systems is crucial; accurate documentation of response activities is necessary for legal and law enforcement purposes. Once evidence has been collected, the initial forensics investigations are complete, and basic facts have been established, the organization has a responsibility to communicate to customers and partners. Clear communication is essential during a breach/attack situation. [45]

8.5 Sandia National Laboratories Recommendations

8.5.1 Protection against Lifecycle Attacks using Trust Anchors

The top priority is to secure critical infrastructure systems vulnerable to physical and cyber-attacks from adversaries who take advantage of compromised critical systems at every stage of the systems' lifecycles. Typically, the main focus is to secure the operational phase of the critical system and ignore the other important aspects of the IT lifecycle. For these reasons, Sandia National Laboratories proposes implementation of trust anchors that enable the use of functional elements developed through trustworthy processes and introduced into process control systems to provide critical security services that cannot be influenced by malicious content. Furthermore, trust anchors address the lifecycle threats of the process control system and, coupled with Sandia's secure obfuscation technology, renders them tamper proof in a cryptographically secure manner. [46]

Trust anchors provide: (a) verification that systems function correctly; and (b) a foundation for additional, independent security services. Sandia's cryptographically secure obfuscation technology ensures both that trust anchors are tamper-proof and that an adversary cannot derive the critical system's function. Keeping in mind a critical system's security can never be at 100 percent, the use of trust anchors increases the risk to an adversary attempting to insert malicious functions. [46]

Trust anchors address the four components in the following threat model:

- Hardware and software supply chains must be assumed to be untrustworthy.
- Routine system administration, configuration, and updates cannot be proven trustworthy.
- Unbiased measurement of operational system components is currently impossible.
- Systems are too complex to reliably analyze . [46]

The two core services that trust anchors provide are unbiased monitoring and unimpeded control, which provide the flexible foundation for multiple security services. The unbiased monitoring enables the trust anchors to independently verify the system function, reveal deceptive malicious functions, independently confirm the system state, and verify the correctness of system tests. The unimpeded control makes it possible to implement trusted control functions, remove discovered malicious content, execute system tests, and conduct experiments on and analysis of a suspected compromise. A trust anchor at a minimum provides a root of trust (additional trust anchors can be promoted dynamically) and has several other important security properties to enable them to serve as an effective security tool. The other properties of a trust anchor are provided by Sandia's secure obfuscation technology, which ensures that an adversary cannot:

- Be aware of what the device is measuring.
- Understand the function or modify it.
- Sabotage the system, as any modification will be immediately evident [46].

These three capabilities greatly increase the risk to an adversary who intends to introduce malicious functions into critical infrastructure systems [46].

Sandia's secure obfuscation technology is a mathematically provable obfuscation that enables some of the trust anchor's most important capabilities. The obfuscation technology uses a customized compiler to obfuscate a software program, which hides the program's functionality and ultimately prevents reverse engineering. The obfuscation code can then be executed with an oracle. The oracle is a small tamper-protected device, which interprets the obfuscated code and ensures its integrity. Because the oracle derives the function of the obfuscated code, it must be protected. The obfuscated code can be executed only when it is in communication with the oracle. Regardless of whether the code is in the process of executing or not, the code remains obfuscated. Figure 20 illustrates the obfuscation model. [46]

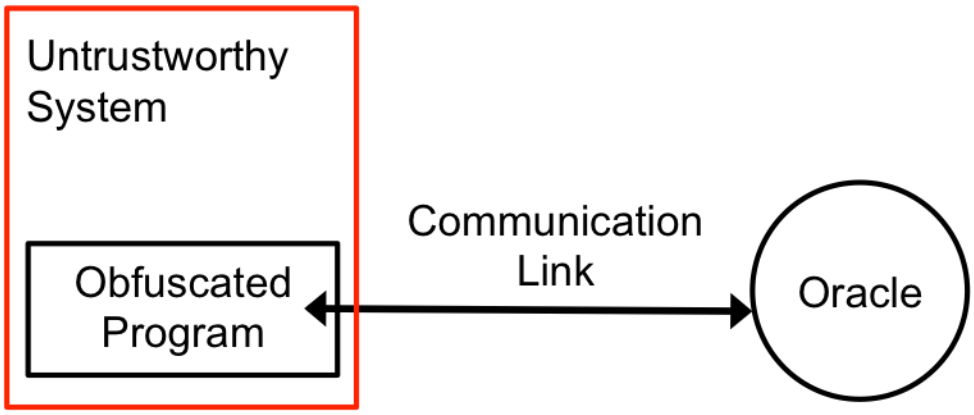

Figure 20. Obfuscation Model [46]

The oracle computations are very simple, require minimal storage space independent of the size of the obfuscation code. The oracle computations can be implemented on a variety of platforms such as a network server, USB drive, crypto card, and/or smart card. The system is also scalable; a single oracle can be made to execute a variety of obfuscated programs [46].

Effective use and programming of obfuscation can provide a significant advantage in safeguarding information systems that protect national security assets. Sandia's obfuscation technology has been mathematically proven to be secure. Under the developed model, the adversary is allowed to make requests to the oracle (tamper-protected device) and view its outputs, but the adversary is not allowed to view its internal computations. The model proves and satisfies the two most important security properties:

- The obfuscated code behaves as a true black box, assuming the oracle is protected.
- The original algorithm will at most only see a polynomial time slowdown; internal testing has shown linear slowdown with a coefficient of two. [46]

8.5.2 Threat Analysis Framework

Sandia developed a threat analysis framework to address the need to protect national critical infrastructure integrated with the commodity-based IT into the control system architectures. IT systems provide a great set of capabilities and commonality critical to energy infrastructures (i.e. oil, gas, and electric power), but at the same time they also introduce vulnerabilities to other expansive sets of threats. To reduce this new set of risks in the energy sector, a continuous evaluation of the adversary attack risk is necessary. The threat analysis framework can be used to identify the elements required to quantify threats against critical infrastructure assets and apply appropriate action to the critical infrastructure entities for the asset protection. A comprehensive threat analysis can assist critical infrastructure providers, utility owners, and operators how best to apply their limited resources in protecting their infrastructure from an adversarial attack. This

threat analysis framework defines the critical elements associated with identification, impact, and mitigation of a possible threat. [47]

The threat analysis framework identifies and describes five key elements to provide a comprehensive analysis of a threat. The five elements are:

1. Identify the adversary through various intelligence organizations.
2. Identify adversary characteristics and develop threat profiles that describe the adversary capability and level of threat. This element can include developing a threat profile matrix to characterize the adversary.
3. Identify generic attack paths that can be pursued by an adversary against a system under evaluation.
4. Discover associated adversary activities that may indicate and provide an early warning of the adversary's intent to discover vulnerabilities against a critical infrastructure asset under evaluation.
5. Develop cyber-based threat scenarios (at the local, regional, and national level) and identify the best strategies for mitigation and reduction of the overall risk against the compromised critical infrastructure. [47]

Applying and executing these five elements helps develop a comprehensive threat analysis by those in the energy sector. The process helps by better defining and analyzing the threat against the control systems and provides the following benefits:

- The ability to bring national attention to the potential risk of a cyber-attack against the nation's critical infrastructure.
- A tool for ranking mitigation actions to be performed.
- A technical threat analysis capability.
- A method for providing unclassified, actionable risk information to control system owners and maintainers.
- A greater understanding by the energy sector stakeholders of the impacts of sophisticated and changing threats.
- The ability to communicate objective information to industry. [47]

The threat framework also aids in responding to questions from government on security for the critical infrastructure system and from industry on capabilities and mitigation strategies to protect against the threats. [47]

8.5.3 Security Framework for Control System Data and Protection

Sandia presents a data classification process for utility administers, control engineers, and IT personnel in an effort to help meet new regulatory requirements and recommendations developed since 9/11. Such requirements and recommendations include data authentication and data

exchange integrity, network security and secure network management, compartmentalizing communication, and blocking access to resources and services. The goal is to make critical infrastructure control systems less vulnerable to malicious attacks and enable effective implementation of security techniques and technologies so the control system continues to function as required in an attack. The data classification framework for controls systems comprises four main components: data type identification, data classification, data protection profile, and implementation guide. Figure 21 illustrates the overall structured approach to data classification and protection. [48]

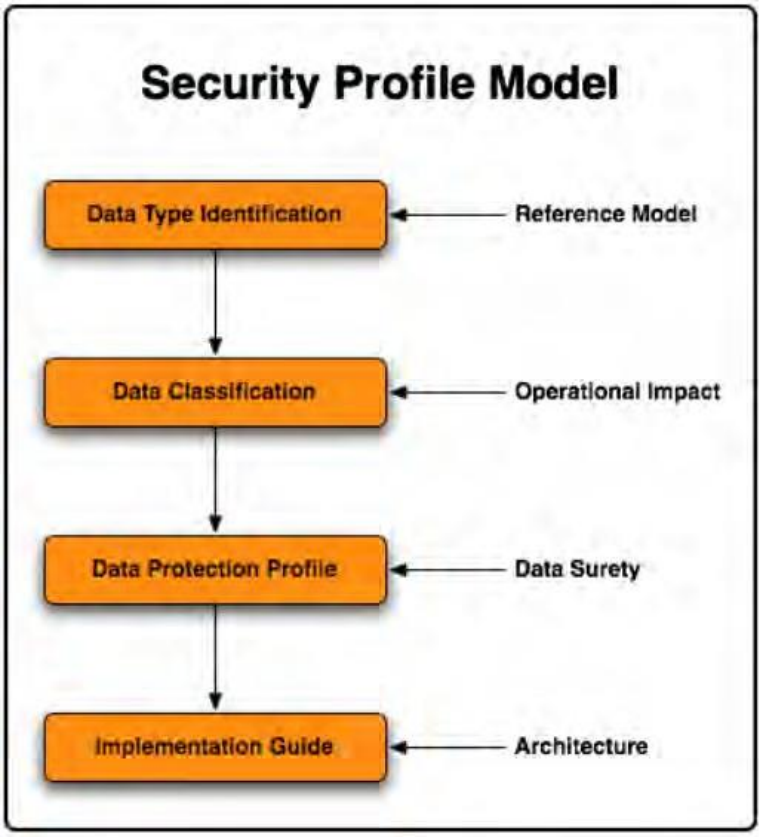

Figure 21. Security Profile Model [48]

The first step is to identify/determine the data type associated with the control system. A reference model for the data types must be identified or developed. The reference model helps the utility owner identify the different types of data being analyzed from their control system. The reference model must be able to identify the types of data based on function or purpose with association to the overall operation of the control system. After the different types of data are identified, the classification for each data type needs to be determined based on the data type's importance to maintaining operations. This classification not only determines the criticality of the role the data type plays in the main operations, but also determines the common characteristics that govern its interaction. [48]

The second step in the data classification process is data classification, which can become overly complex. To maintain a manageable and flexible classification, the technique must be able to accommodate changes in operational requirements and infrastructure. The approach for this classification requirement is to align with the service offerings on the control system network. The criticality of the data should be determined by the service it supports and the overall service value it provides to the control system. Figure 22 demonstrates this concept. To create the system priority tiers, descriptive information about the process control system must be collected for use in developing the system's data structure. This information must include all the groups that use the data, maintenance technicians responsible for troubleshooting and repairing equipment, master control personnel monitoring and analyzing activity, IT staff responsible for the network, and the business units that process the data on the Local Area Network (LAN). To properly and accurately create the tiers, all responsible elements for proper operations of the control system must be taken into account. [48]

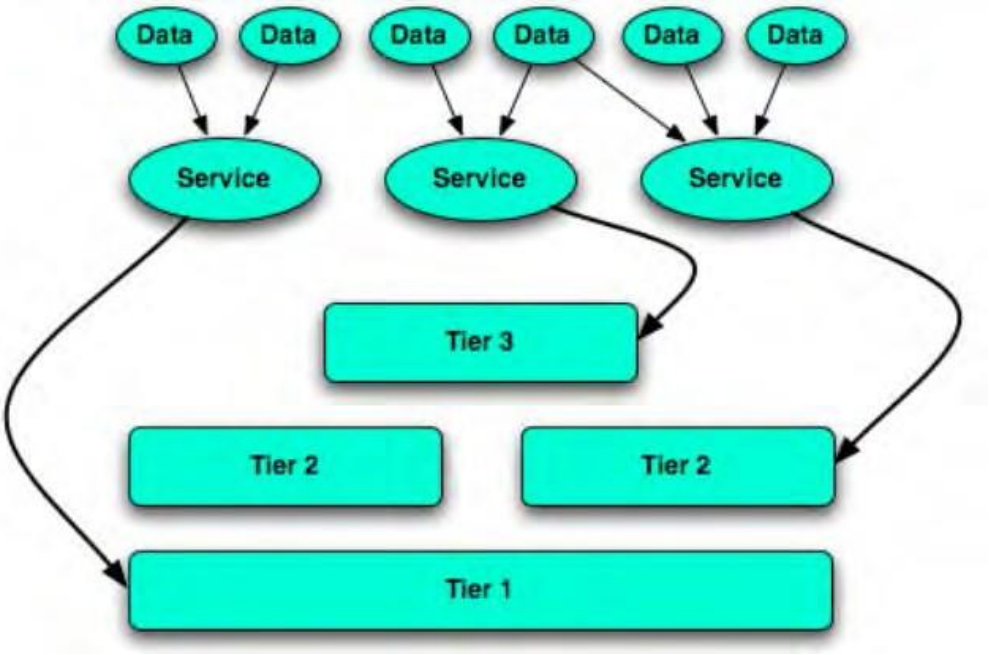

Figure 22. Data Classification Tier Organization [48]

Other information that must be considered when classifying data includes association of operations requirements to the data classification, key performance constraints for each data type, and association of the data to the service it provides in the control system. [48]

The third step in the data classification process is to assign the data to an appropriate protection profile. To assign a data protection profile to a data class, the protection level for that class needs to be determined. The security requirements for addressing threats against the operating environment must be included in the profile. In addition, when assigning a profile, the process must take into account the overall importance of the data to the operations, the physical location of the data in the control system architecture, and the crossing points of the data at interface boundaries within the architecture. To characterize each profile, information assurance elements are used. The elements of information assurance used to protect data include availability, confidentiality, integrity, reliability, authenticity, non-repudiation, and restoration of information systems that include protection, detection, and response capabilities. [48]

The fourth and final step in the data classification process is to produce an implementation guide that details the practical implementation of the protection profile. The implementation guide tells implementers how to realize a physical implementation based on the logical description. Identification of device requirements (described at a top level) is part of the implementation process and is a way to recognize security attributes. All devices are associated with their appropriate subsystems, which can be reviewed independently, but if isolation points exist between subsystems, the final level of security must fit into the overall integrated system. [48]

Sandia recommends this process to utility administers, control engineers, and IT personnel as an approach to understanding the necessary protection, prospect, and limitations of implementing security methods based on data classification in the process control environments. The use of this process provides better protection of data of importance.

8.6 International Energy Agency Recommendation on Smart Grids and General Cybersecurity Policy Considerations

Enhancing cybersecurity is essential and companies that are making smart grid technology offering such services include technology and communication firms.[10] In particular, the deeply integrated use of digital technology with power grids means that data is flowing and information management is central to the smart grid. Integration of the new grid information flows into utility processes and systems is one of the key issues in the design of smart grids. The key challenges therefore are: a) how to secure the data that is flowing; b) how to ensure that the energy infrastructure remains unharmed, especially the communications technology at the heart of the smart grid; and c) how to address data privacy concerns.

[10] Office of Electricity Delivery and Energy Reliability, "Smart Grid", http://energy.gov/oe/services/technology-development/smart-grid, energy.gov.

Malicious actors are increasingly attempting to sabotage power grids, financial institutions, and air traffic control systems.[11] Threat actors in this space can include criminals, possible terrorist actors, politically motivated "hacktivists", recreational hackers, disgruntled employees/insiders, and malicious states. For instance, one of the key capabilities of this connectivity is the ability to remotely switch off power supplies. Cybercriminals have apparently infiltrated the U.S. electric grid on previous occasions. There are also concerns that computer malware like Stuxnet, which targeted SCADA systems that are widely used in industry, could be used to attack a smart grid network.[12] Electricity theft is another concern given that, for instance, devices can be created to change the actual usage reported. Moreover, industrial control systems (in other words, computer systems that are used to monitor and control a range of physical processes within critical infrastructures) and the critical infrastructures within which they operate are increasingly vulnerable to malicious cyber intrusions.[13]

It is clear therefore that while smart grids can improve electricity system reliability and efficiency, their use of new ICTs can also introduce vulnerabilities that jeopardise this reliability, including the potential for cyber-attacks.[14] In addition, the IEA highlights that aspects of the regulatory environment for electricity systems may also make it difficult to ensure the cybersecurity of smart grid systems, and it seems that utilities have been focusing more on regulatory compliance instead of "comprehensive security".[15] According to an IEA study, insufficient security features are being built into some smart grid systems, the electricity industry does not have an effective mechanism for sharing information on cybersecurity and it does not have metrics for evaluating cybersecurity. It finds that cybersecurity must be considered as part of a larger smart grid deployment strategy. It also recommends that lessons can be learned from other industries like the financial sector. Equally, lessons can be learned from the experiences of other regions or countries such as the Joint Research Council of the European Commission, which has initiated the European Network for the Security of Control and Real-Time Systems (ESCoRTS). This is a joint project among industries, utilities, equipment manufacturers and research institutes to foster progress and solutions for cybersecurity of control and communication equipment and the use of data for acceptable purposes, which is required for the successful deployment of smart grid technologies.

---

[11] Ryan Ellis, **"Protecting US Critical Infrastructure: One Step Forward for Cybersecurity, One Back?",** http://belfercenter.ksg.harvard.edu/publication/23271/protecting_us_critical_infrastructure.html?breadcrumb=%2Fproject%2F69%2Fcyber_project%3Fpage_id%3D367%26page%3D4, 24 July 2013.

[12] Wikipedia, "Smart Grid", http://en.wikipedia.org/wiki/Smart_grid.

[13] Ryan Ellis, **"Protecting US Critical Infrastructure: One Step Forward for Cybersecurity, One Back?",** http://belfercenter.ksg.harvard.edu/publication/23271/protecting_us_critical_infrastructure.html?breadcrumb=%2Fproject%2F69%2Fcyber_project%3Fpage_id%3D367%26page%3D4, 24 July 2013.

[14] International Energy Agency, "Technology Roadmap: Smart Grids", https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf, 2011.

[15] International Energy Agency, "Technology Roadmap: Smart Grids", https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf, 2011.

According to the IEA, several concepts are emerging that extend the reach of the smart grids from electricity systems to broader energy and societal contexts such as the "smart community" or "smart city". A smart community is understood to integrate several energy supply and use systems within a given regional in order to optimize operation and allow for the maximum integration of renewable energy resources – from large scale wind farm deployments to residential energy managements systems. This concept includes existing infrastructure systems, such as electricity, water, transportation, gas, waste and heat, as well as future systems like hydrogen and electric vehicle charging. Smart communities are regarded as a logical extension of smart grids from electricity systems to other types of infrastructure systems, which are ultimately expected to evolve in this direction. The study notes that regions might follow different pathways as they develop smart grid technologies.

Economies with older systems must manage deployment within an older infrastructure base.

Another issue is the relationship between various stakeholders in this space. According to the IEA, smart grid equipment and systems are provided by many industry sectors that have not traditionally worked together. For example, equipment manufacturers, ICT providers, the building industry, and consumer products and service suppliers. In addition, control systems operated by utilities whose networks interconnect must be able to exchange information. Therefore, standards, definitions and protocols for the transport of data are needed to allow seamless and secure operation. One of the highest priority areas therefore identified are cybersecurity and data communication in the smart grid. However, countries differ in their infrastructure requirements. The IEA study identifies the collaborating on a policy and regulatory environment that supports smart grid investment as perhaps the single most important task for all stakeholders in the electricity sector. It finds that a lack of collaboration had led to problems in demonstration and deployment projects.

It recommended in 2011 that cybersecurity issues should be addressed proactively through both regulation and the application of best practices. In other words, there should be proactive actions across all sectors of the electricity system rather than solely meeting regulatory requirements.

Consumers should also be informed about the risks associated with smart grid systems. The IEA previously recommended developing new policies and mechanisms for the control and regulation of privacy, ownership and security issues associated with detailed customer usage behavior information. The main cybersecurity issues that arise include privacy, ownership and security issues because of the availability of detailed customer energy consumption data. These should be addressed during the stages of smart grid design and deployment planning. The policy questions relevant to this report that are identified by the IEA include: 1) Who owns the customer's data and how is access to and use of this data regulated?; and 2) Who guarantees privacy and security of customer data (for example, against surveillance or criminal activity?

The report does highlight however that best practices are being developed in certain regions like the EU Task Force on Smart Grids and countries like the UK through its Office of Gas and Electricity Markets (OFGEM), for instance, which had proposed an independent organization to access and store data, and to only disseminate the basic required data to parties for billing or usage purposes. Such best practices are still under development and are evolving.

9 Other Resources

9.1 Sandia National Laboratories Documents

The following is a link to additional documents, published by Sandia National Laboratories related to cybersecurity in the energy sector:

http://energy.sandia.gov/infrastructure-security/cyber/scada-systems/scada-documents-2/

9.2 Cyber-Energy Nexus Documents

The following are links to documents and resources related to cybersecurity:

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) US Department of Energy, Office of Electricity Delivery and Energy Reliability

http://www.nist.gov/itl/cyberframework.cfm. NIST Cybersecurity Framework Draft

Roadmap to Achieve Energy Delivery Systems Cybersecurity (2011) US Department of Energy, Office of Electricity Delivery and Energy Reliability

Advanced Metering Infrastructure (AMI) System Security Requirements AMI-SEC Task Force - December 2008

Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology (2007) ANSI/ISA-99

Manufacturing and Control Systems Security, Part 2: Establishing a Manufacturing and Control Systems Security Program (2009) ANSI/ISA-99

InfraGard FBI Cybersecurity Collaboration Federal Bureau of Investigation, InfraGard Program

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

Standards for Security Categorization of Federal Information and Information Systems (February 2004) FIPS 199

Cyber Assessment Methods for SCADA Security (2005) Idaho National Laboratory

Guidelines for Smart Grid Cybersecurity, Introduction and Volumes 1-3, The Cybersecurity Coordination Task Group, Advanced Security Acceleration Project Smart Grid (August 2010) National Institute of Standards and Technology (NIST), NISTIR 7628

DRAFT Managing Risk from Information Systems: An Organizational Perspective (April 2008) National Institute of Standards and Technology (NIST) Special Publication (SP), 800-39

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

Smart Grid Cybersecurity Blog Spot

IT, Telecommunications, and Energy Sectors: Sector Specific Plans (SSPs) (updated tri-annually) US Department of Homeland Security

Roadmap to Achieve Energy Delivery Systems Cybersecurity (September 2011) US Department of Energy, Office of Electricity Delivery and Energy Reliability (OE) and the Energy Sector Control Systems Working Group

U. S. Computer Emergency Readiness Team (US-CERT) US Department of Homeland Security

9.3 Other References and Resources

Security Guidelines for the Petroleum Industry (April 2005) American Petroleum Institute

A Comparison of Oil and Gas Segment Cybersecurity Standards (November 2004) Idaho National Engineering and Environmental Laboratory

9.3.1 Articles

http://www.foreignpolicyjournal.com/2009/09/14/a-new-security-paradigm-is-needed-to-protect-critical-us-energy-infrastructure-from-cyberwarfare/

http://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/

9.3.2 Cybersecurity Policy Planning and Preparation

TR99.00.02: Integrating Electronic Security into the Manufacturing and Control Systems Environment, ISA, 2004.

NIST SP 800-82 Rev 1, Guide to Industrial Control Systems (ICS) Security, May 13, 2013.

NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

Additional Information

21 Steps to Improve Cybersecurity of SCADA Networks," Office of Energy Assurance, Office of Independent Oversight And Performance Assurance, US Department of Energy.

Kilman, D. and Stamp, J. "Framework for SCADA Security Policy," Sandia Corporation. 2005.

Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, US Department of Homeland Security National Cybersecurity and Communications Integration Center, ICS-CERT.

NIST SP 800-64 Rev 2, Security Considerations in the System Development Life Cycle, October 2008.

9.3.3 Establishing Network Segmentation, Firewalls, and DMZs

Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, Centre for the Protection of National Infrastructure (CPNI), London, 2005.

NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook.

Mix, S., Supervisory Control and Data Acquisition (SCADA) Systems Security Guide, EPRI, 2003.

NIST SP 800-82 Rev 1, Guide to Industrial Control Systems (ICS) Security, May 13, 2013.

Additional Information

Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, US Department of Homeland Security National Cybersecurity and Communications Integration Center, ICS-CERT.

Control Systems Cybersecurity: Defense in Depth Strategies, October 2009, US Department of Homeland Security National Cybersecurity Division, Control Systems Security Program.

9.3.4 Patch, Password, and Configuration Management

NIST SP: 800-118, Guide to Enterprise Password Management (Draft)

NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook.

NIST SP: 800-40, Creating a Patch and Vulnerability Management Program, 2005.

Mix, S., Supervisory Control and Data Acquisition (SCADA) Systems Security Guide, EPRI, 2003.

Dzung, D., Naedele, M., Von Hoff, T., and Crevatin, M. "Security for Industrial Communication Systems," Proceedings of the IEEE. Institute of Electrical and Electronics Engineers Inc. 2005.

NIST SP 800-82 Rev 1, Guide to Industrial Control Systems (ICS) Security, May 13, 2013.

NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

Additional Information

Ashier, J. and Weiss, J. "Securing your Control System,"2004.

Wooldridge, S. "SCADA/Business Network Separation: Securing an Integrated System," 2005.

"21 Steps to Improve Cybersecurity of SCADA Networks," Office of Energy Assurance, Office of Independent Oversight And Performance Assurance, US Department of Energy.

Good Practice Guide on Patch Management, Centre for the Protection of National Infrastructure (CPNI), London, October 24, 2006.

Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, US Department of Homeland Security National Cybersecurity and Communications Integration Center, ICS-CERT.

9.3.5 Control System Cybersecurity Training for Engineers, Technicians, Administrators, and Operators

Wilson, Mark, Hash, Joan, NIST SP: 800-50, Building an Information Technology Security Awareness and Training Program, 2003.

NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook.

Mix, S., Supervisory Control and Data Acquisition (SCADA) Systems Security Guide, EPRI, 2003.

NIST SP 800-82 Rev 1, Guide to Industrial Control Systems (ICS) Security, May 13, 2013.

NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

Additional Information

Boyes, W. "Security is More than Hating Microsoft," May 31, 2005.

Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, US Department of Homeland Security National Cybersecurity Division, Control Systems Security Program,

Using Operational Security (OPSEC) to Support a Cybersecurity Culture in Control Systems Environments (draft), February 2007, US Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT.

9.3.6 Establishing and Conducting Asset, Vulnerability, and risk Assessments

Rinaldi, et al, Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, 2001.

GAO-04-354, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, US GAO, 2004.

Stamp, Jason, et al., Common Vulnerabilities in Critical Infrastructure Control Systems, Sandia National Laboratories, 2003.

Duggan, David, et al, Penetration Testing of Industrial Control Systems, Sandia National Laboratories, Report No SAND2005-2846P, 2005.

NIST SP: 800-40, Creating a Patch and Vulnerability Management Program, 2005.

NIST SP: 800-34 Rev. 1, Contingency Planning Guide for Information Technology Systems, 2010.

NIST SP: 800-61 Rev. 2, Computer Security Incident Handling Guide, March 2012.

Mix, S., Supervisory Control and Data Acquisition (SCADA) Systems Security Guide, EPRI, 2003.

NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

NIST SP 800-53A Rev 1, Guide for Assessing the Security Controls in Federal Information Systems, June 2010.

NIST SP: 800-115, Technical Guide to Information Security Testing and Assessment, September 2008.

Additional Information

Hart, D. "An Approach to Vulnerability Assessment for Navy Supervisory Control and Data Acquisition (SCADA) Systems," Naval Postgraduate School, Monterey, California, September 2004.

"Supervisory Control and Data Acquisition (SCADA)," Data Comm. for Business, Inc., Oct 1999.

Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, US Department of Homeland Security National Cybersecurity and Communications Integration Center, ICS-CERT.

Byres, E., and Creery, A. "Industrial Cybersecurity for Power System and SCADA Networks," September 2005.

9.3.7 Control System Security Procurement Requirements Specification

TR99.00.01: Security Technologies for Manufacturing and Control Systems, ISA, 2004.

TR99.00.02: Integrating Electronic Security into the Manufacturing and Control Systems Environment, ISA, 2004.

NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

Additional Information

Merritt, R. "What Vendors Say About Control System Security," January 31, 2005.

SCADA and Control Systems Procurement Language Project, September 2009, US Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT.

Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, US Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT.

9.3.8 Placement and Use of IDSs and IPDSs

NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook.

NIST SP: 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)

Mix, S., Supervisory Control and Data Acquisition (SCADA) Systems Security Guide, EPRI, 2003.

Additional Information

Wooldridge, S. "SCADA/Business Network Separation: Securing an Integrated System," 2005.

Ashier, J. and Weiss, J. "Securing your Control System," 2004.

Network Monitoring System Designed to Detect Unwanted Wireless Networks, September 14, 2005.

Rakaczky, E. "Intrusion Insights Best Practices for Control System Security," July 2005.

Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, US Department of Homeland Security National Cybersecurity and Communications Integration Center, ICS-CERT.

Control Systems Cybersecurity: Defense in Depth Strategies, October 2009, US Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT.

Mitigations for Security Vulnerabilities Found in Control System Networks, June 2006, US Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT. .

9.3.9 Authentication, Authorization, and Access Control For Direct and Remote Connectivity

NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook.

NIST SP: 800-73-2, Interfaces for Personal Identity Verification (4 parts), September 2008.

NIST SP 800-76-1, Biometric Data Specification for Personal Identity Verification, 2007.

Mix, S., Supervisory Control and Data Acquisition (SCADA) Systems Security Guide, EPRI, 2003.

Baker, Elaine, et al, NIST SP: 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007.

NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

NIST SP: 800-57 Recommendation for Key Management, March 2007

Part 1, General (Revised)

Part 2, Best Practices

Part 3, Application Specific Key Management Guidance (Draft), October 2008

NIST SP 800-82 Rev 1, Guide to Industrial Control Systems (ICS) Security, May 13, 2013.

Additional Information

Wooldridge, S. "SCADA/Business Network Separation: Securing an Integrated System," 2005.

Ashier, J. and Weiss, J. "Securing your Control System," 2004.

"Thales e-Security." 2005.

Schwaiger, C. and Treytl, A. "Smart Card Based Security for Fieldbus Systems," 2003, Austria Card, Vienna, Austria.

Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, US Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT. .

9.3.10 Securing Wireless Connections

NIST SP: 800-48 Revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks, July 2008.

NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook.

Additional Information

Pescatore, J. "Keep your Wireless Business Secure," August 21, 2005.

Network Monitoring System Designed to Detect Unwanted Wireless Networks, September 14, 2005.

Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, US Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT.

Securing ZigBee Wireless Networks in Process Control System Environment (draft), April 2007, US Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT.

9.3.11 Use of VPNs and Encryption in Securing Communications

NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook.

NIST SP: 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007.

SP 800-56 B, Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography, August 2009

NIST SP: 800-57 Recommendation for Key Management, March 2007

Part 1, General (Revised)

Part 2, Best Practices

Part 3, Application Specific Key Management Guidance (Draft), October 2008

Additional Information

AGA Report No. 12: Cryptographic Protection of SCADA Communications Part 1 Background Policies and Test Plan, American Gas Association, 2006.

Peterson, D. "Protocol for SCADA Field Communications," July 12, 2005.

Cohen, B. "VPN Gateway Appliances-Access Remote Data like the Big Guys," April 28, 2005.

Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, US Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT.

9.3.12 Establishing a Secure Topology and Architecture

NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook.

Mix, S., Supervisory Control and Data Acquisition (SCADA) Systems Security Guide, EPRI, 2003.

NIST SP 800-82 Rev 1, Guide to Industrial Control Systems (ICS) Security, May 13, 2013.

Additional Information

"Study Suggest Increased Concerns with Cybersecurity and SCADA System Reliability," June 14, 2005.

Berg, M. and Stamp, J. "A Reference Model for Control and Automation Systems in Electric Power," Sandia Corporation. 2005.

Control Systems Cybersecurity: Defense in Depth Strategies, October 2009, US Department of Homeland Security National Cybersecurity Division, Control Systems Security Program.

Curtis, Ian, ABB. "Security against cyber-attack," July 19, 2010.

Invensys Operations Management (Australia) Pty Ltd. "Integrating control and safety -- where to draw the line," Jan 20, 2009.

9.3.13 Applying and Complying with Security Standards

TSA Pipeline Security Guidelines, Transportation Security Administration, April 2011.

INGAA Control Systems Cybersecurity Guidelines for the Natural Gas Pipeline Industry, Interstate Natural Gas Association of America (INGAA), April 2011.

TR99.00.01: Security Technologies for Manufacturing and Control Systems, ISA, 2004.

TR99.00.02: Integrating Electronic Security into the Manufacturing and Control Systems Environment, ISA, 2004.

Additional Information

Peterson, D. and Howard, D. "Cybersecurity for the Electric Sector," September 12, 2005.

Berg, M. and Stamp, J. "A Reference Model for Control and Automation Systems in Electric Power," Sandia Corporation. 2005.

9.3.14 Ensuring Security when Modernizing and Upgrading

TR99.00.01: Security Technologies for Manufacturing and Control Systems, ISA, 2004.

Cybersecurity Procurement Language for Control Systems, US Department of Homeland Security National CyberSecurity Division, September 2009.

Additional Information

Ladd, E. "Dispelling the myths of HART-enabled devices," April 18, 2005.

Verhappen, I. "What makes a fieldbus go?" April 27, 2005.

Verhappen, I., "On the bus: Design hurdles to fieldbus technology," Control Global, 2005.

NIST SP 800-64 Revision 2, Security Considerations in the System Development Life Cycle, October 2008

"Supervisory Control and Data Acquisition (SCADA)," Data Comm. for Business, Inc., Oct 1999.

Digital Bond, British Columbia Institute of Technology, and Byres Research. "OPC Security White Paper #1: Understanding OPC and How it is Deployed," July 27, 2007.

Digital Bond, British Columbia Institute of Technology, and Byres Research. "OPC Security White Paper #2: OPC Exposed," November 13, 2007.

Digital Bond, British Columbia Institute of Technology, and Byres Research. "OPC Security White Paper #3: Hardening Guidelines for OPC Hosts," November 13, 2007.

References

1. ICS-CERT (United States Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team), 2014: http://ics-cert/us-cert.gov

2. IEC (International Electrotechnical Commission). *TC 57 Power systems management and Associated Information Exchange*, IEC, 2014: http://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID,FSP_LANG_ID:1273,25

3. Cleveland, Frances. *IEC TC57 WG 15: IEC 62351 Security Standards for the Power System Information Infrastructure*. Geneva, Switzerland: IEC (International Electrotechnical Commission), 2012.

4. Heinl, Caitríona H. *Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime*. Asian Policy, Number 18 (pg. 131-59), 2014. http://asianpolicy.nbr.org Seattle, WA: The National Bureau of Asian Research.

5. NIST (National Institute of Standards and Technology) United States Department of Commerce, 2014: http://www.nist.gov

6. NIST (National Institute of Standards and Technology). *NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security*. United States Department of Commerce, Recommendations of the National Institute of Standards and Technology, NIST, June 2011

7. NERC (North American Electric Reliability Corporation), 2013: http://www.nerc.com

8. NERC (North American Electric Reliability Corporation). Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets. NERC Critical Infrastructure Protection Committee, June 2010.

9. NERC (North American Electric Reliability Corporation) CIP (Critical Infrastructure Protection), 2013: http://www.nerc.com/pa/CI/Comp/Pages/default.aspx

10. NIST (National Institute of Standards and Technology). *NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems*. United States Department of Commerce, Recommendations of the Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology, NIST, February 2005.

11. NIST (National Institute of Standards and Technology). *NISTIR 7628 Guidelines for Smart Grid Cybersecurity*. United States Department of Commerce, The Smart Grid Interoperability Panel – Cybersecurity Working Group, NIST, August 2010.

12. ISO (International Organization for Standardization), 2014: http://www.iso.org

13. Wikipedia. *International Organization for Standardization*, Wikimedia Foundation Inc. September 2014: http://en.wikipedia.org/wiki/International_Organization_for_Standardization

14. ISO (International Organization for Standardization). *ISO/IEC 27000:2014 (E) – Information Technology, Security Techniques, Information Security Management Systems, Overview and Vocabulary*. Third Edition, ISO/IEC, 2014.

15. Wikipedia – *ISO/IEC 27000-Series*, Wikimedia Foundation Inc. September 2014: http://en.wikipedia.org/wiki/ISO/IEC_27000-series

16. ISO (International Organization for Standardization). *ISO/IEC 27002:2013 (E) – Information Technology, Security Techniques, Code of Practice for Information Security Controls*. Second Edition, ISO/IEC, 2013.

17. ISO (International Organization for Standardization). *ISO/IEC 27005:2011 (E) – Information Technology, Security Techniques, Information Security Risk Management*. Second Edition, ISO/IEC, 2011.

18. ISO (International Organization for Standardization). *ISO 31000:2009 (E) – Risk Management, Principles and Guidelines*. First Edition, ISO/IEC, 2009.

19. OSCE (Organization for Security and Co-operation in Europe). *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*. OSCE, 2013.

20. NIST (National Institute of Standards and Technology), Information Technology Laboratory. *Federal Information Processing Standards Publication (FIPS PUB 104-2) – Security Requirements For Cryptographic Modules*. United States Department of Commerce, Recommendations of the National Institute of Standards and Technology, NIST, May 2001

21. Wikipedia. *Institute of Electrical and Electronic Engineers*, Wikimedia Foundation Inc., October 2014: http://en.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers

22. IEEE (Institute of Electrical and Electronic Engineers), 2014: http://www.ieee.org

23. IEEE (Institute of Electrical and Electronic Engineers). *IEEE Guide for Electric Power Substation Physical and Electronic Security*. Substations Committee of the IEEE power Engineering Society, IEEE, 2000; reaffirmed 2008.

24. Heinl, Caitrionia H. *Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime*. Asia Policy, Number 18, page 131-159. The National Bureau Of Asian Research, July 2014.

25. ASEAN (Association of Southeast Asian Nations). ASEAN Community in Figures (ACIF) 2013, ASEAN, February 2014.

26. Wikipedia. *Smart Grid Interoperability Panel*, Wikimedia Foundation Inc. September 2014: http://en.wikipedia.org/wiki/Smart_Grid_Interoperability_Panel

27. NIST (National Institute of Standards and Technology) Smart Grid Interoperability Panel (SGIP) United States Department of Commerce, 2013: http://www.nist.gov/smartgrid/sgipbuffer.cfm

28. Smart Grid Interoperability Panel, SGIP 2.0 Inc., 2014: http://www.sgip.org

29. US Department of Energy Office of Electricity Delivery & Energy Reliability – *RoadMap To Achieve Energy Delivery Systems Cybersecurity 2011*, United States Department of Energy, 2014: http://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011

30. ESCSWG (Energy Sector Control Systems Working Group). *2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity*. United States Department of Energy, ESCSWG, September 2011.

31. OSCE (Organization for Security and Co-operation in Europe). *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace.* Organization for Security and Co-operations in Europe, 2013.

32. ES-C2M2 (Electricity Subsector Cybersecurity Capability Maturity Model). *Electricity Subsector Cybersecurity Capability Maturity Model.* United States Department of Energy and United States Department of Homeland Security. Version 1.1, February 2014.

33. SGIP (Smart Grid Interoperability Panel), 2015: http://www.sgip.org/index.php?bid=77

34. US Department of Energy Office of Electricity Delivery & Energy Reliability. *Energy Sector Cybersecurity Framework Implementation Guidance*. United States Department of Energy, January 2015.

35. ESCC (Electricity Subsector Coordinating Council). *Protecting the Electric Grid from Threats that Could Impact National Security is a Responsibility Shared By Both the Government and the Electric Power Sector.* Electricity Subsector Coordinating Council, March 2015.

36. Berkely III, Alfred R. and Mike Wallace. *A Framework for Establishing Critical Infrastructure Resilience Goals, Final Report and Recommendations by the Council.* Arlington, VA: NIAC (National Infrastructure Advisory Council), October 2010.

37. EEI (Edison Electric Institute). *Electric Power Industry Initiative to Protect the Nation's Grid from Cyber Threats*. Edison Electric Institute, October 2014.

38. ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) Monitor. *Brute Force Attacks on Internet-Facing Control Systems*. April/May/June 2013. US Department of Homeland Security, June 2013.

39. West, Candid, *Security Response: Targeted Attacks Against the Energy Sector*. Version 1.0. Symantec, January 13, 2014.

40. Symantec Security Response. *Dragonfly: Cyberespionage Attacks Against Energy Suppliers*. Version 1.2. Symantec, July 2, 2014.

41. Ashford, Warwick. *Symantec Exposes Hackers Targeting Power Grids*. Newton, MA. ComputerWeekly.com, July 2015: http://www.computerweekly.com/news/2240223795/Symantec-exposes-hackers-targeting-power-grids

42. Baldwin, Caroline. *South Korean Nuclear Power Plant Attacked by Hacker*. Newton, MA. ComputerWeekly.com, December 2014: http://www.computerweekly.com/news/2240237130/South-Korean-nuclear-power-plant-attacked-by-hacker

43. CBC News Canada. *Canadian Companies Open to Cyber-attacks, Says Federal Agency / Cybersecurity Lacking in Business*. July 14, 2013: http://www.cbc.ca/news/canada/canadian-companies-open-to-cyber-attacks-says-federal-agency-1.1325194

44. PwC (PricewaterhouseCoopers). *Embedding Cybersecurity into the Energy Ecosystem / An Integrated Approach to Assessing Cyber Threats and Protecting Your Assets*. PricewaterhouseCoopers LLP, February 2013.

45. Clemente, Dave. *Security Think Tank: Three Steps to Effective Incident Response*. Newton, MA. ComputerWeekly.com, July 2014: http://www.computerweekly.com/opinion/Security-Think-Tank-Three-steps-to-effective-incident-response

46. Chavez, Adrian R. *Position Paper: Protecting Process Control Systems Against Lifecycle Attacks Using Trust Anchors*. Sandia National Laboratories, July 2009.

47. Duggan, David P. and John T. Michalski. *Threat Analysis Framework*, Sandia Technical Report SAND2007-5792, Sandia National Laboratories, September 2007.

48. Richardson, Bryan T. and John Michalski. *Security Framework for Control System Data Classification and Protection*, Sandia Technical Report SAND2007-3888P, Sandia National Laboratories, July 2007.

49. Finkle, Jim. *U.S. Utility's Control System was Hacked, Says Homeland Security*. Boston, MA. Reuters, May 2014: http://www.reuters.com/article/2014/05/21/us-usa-cybercrime-infrastructure-idUSBREA4J10D20140521

50. Pagliery, Jose. *Hackers Attacked the U.S. Energy grid 79 Times This Year*. New York, NY. CNN, December 2014: http://money.cnn.com/2014/11/18/technology/security/energy-grid-hack/

51. Rashid, Fahmida Y. *DOE Lab Shuts Down Email, Web Access After Sophisticated Cyber-Attack*. Woburn, MA. eWEEK, July 2011: http://www.eweek.com/c/a/Security/DOE-Lab-Shuts-Down-EMail-Web-Access-After-Sophisticated-CyberAttack-161664

52. Cloherty, Jack and Pierre Thomas. *'Trojan Horse' Bug Lurking in Vital US Computers Since 2011*. New York, NY. ABC News, November 2014: http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476

53. Asia Pacific Energy Research Centre (APERC), "APEC Energy Overview 2013", http://aperc.ieej.or.jp/file/2014/3/18/APEC_Energy_Overview_2013.pdf, for the APEC Secretariat, March 2014.

54. International Energy Agency, "Technology Roadmap: Smart Grids", https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf, 2011.

55. International Energy Agency (2012). Energy Policies of IEA Countries-Australia. www.iea.org/

56. ITU, "Cyberwellness Profile Australia", http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Australia.pdf, last updated 15 January 2015.

57. Australian Government, "Critical Infrastructure Resilience Strategy", http://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf, Commonwealth of Australia, 2010.

58. Paul Budde, "Australia - Smart Grid - Major Players and Projects", http://www.budde.com.au/Research/Australia-Smart-Grid-Major-Players-and-Projects.html, last updated July 2014.

59. SmartGridAustralia, "SmartGrid Australia Intelligent Intelligent Networking Working Group Networking Working Group Study - Topic 2: Securing the Topic 2: Securing the SmartGrid", http://smartgridaustralia.com.au/SGA/Documents/IN_Work_Group_Securing_The_Smart_Grid.pdf, 2009.

60. Global Smart Grid Federation, http://www.globalsmartgridfederation.org/?s=australia+smart+grid.

61. SAIC, "Smart Grid Around the World Selected Country Overviews", http://www.eia.gov/analysis/studies/electricity/pdf/intl_sg.pdf, Prepared for the Energy Information Administration, 3 October 2011.

62. Northeast Group LLC, "Oceania Smart Grid: Market Forecast (2015 – 2025)", http://www.northeast-group.com/reports/Brochure-Oceania%20Smart%20Grid-Market%20Forecast%202015-2025-Northeast%20Group.pdf, May 2015.

63. ESCI, "Smart Grid, Smart City: a new Direction for a new Energy Era", http://esci-ksp.org/project/smart-grid-smart-city-a-new-direction-for-a-new-energy-era-2/?task_id=915, last modified 5 September 2014.

64. Logica, "2010 Australian Smart Grid Study", http://esci-ksp.org/wp/wp-content/uploads/2012/03/Australian-Smart-Grid-Study.pdf, 2010.

65. ESCI, "Solar Cities Program", http://esci-ksp.org/project/solar-cities-program/?task_id=645, last modified 3 November 2014.

66. Global Smart Grid Federation, "Global Smart Grid Federation Report", https://www.smartgrid.gov/sites/default/files/doc/files/Global_Smart_Grid_Federation_Report.pdf, 2012.

67. New America, "Compilation of Existing Cybersecurity and Information Security Related Definitions", Tim Maurer & Robert Morgus, http://www.newamerica.org/downloads/OTI_Compilation_of_Existing_Cybersecurity_and_Information_Security_Related_Definitions.pdf, October 2014.

68. Critical 5, "Forging a Common Understanding for Critical Infrastructure", http://www.infrastructure.govt.nz/publications/critical5/crit5-narrative-v2.pdf, March 2014.

69. Australian Government, "Cyber Security Strategy", https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/AGCyberSecurityStrategyforwebsite.pdf, 2009.

70. UNIDIR, "The Cyber Index: International Security Trends and Realities", http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf, 2013.

71. CFR Energy Brief, "Addressing Cyber Threats to Oil and Gas Suppliers", http://www.cfr.org/cybersecurity/addressing-cyber-threats-oil-gas-suppliers/p30977, June 2013.

72. ASPI International Cyber Centre, "Cyber Maturity in the Asia Pacific Region 2014", https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2014/ASPI_cyber_maturity_2014.pdf, 2014.

73. ASPI, The Strategist, "Cyber Wrap", http://www.aspistrategist.org.au/cyber-wrap-70/, 13 May 2015.

74. Energy Department, Prime Minister's Office, www.energy.gov.bn.

75. Engerati, "Southeast Asia's Smart Grid Market is Growing", http://www.engerati.com/article/southeast-asia%E2%80%99s-smart-grid-market-growing, 14 May 2014.

76. PR Newswire, "Southeast Asian Countries To Invest $13.6bn In Smart Grid Infrastructure', http://www.prnewswire.com/news-releases/southeast-asian-countries-to-invest-136bn-in-smart-grid-infrastructure-279107171.html, 14 October 2014.

77. Brunei Darussalam, Submission to the United Nations General Assembly Resolution A/62/98, 2008, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/62/98 .

78. ITU, "Cyberwellness Profile Brunei", http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Brunei.pdf, last updated 21 August 2014.

79. Brunei Times, "Strategic plan to achieve e-governance", http://www.bt.com.bn/home_news/2009/05/31/strategic_plan_to_achieve_e_governance, 31 May 2009.

80. APEC ESCI, Smart Grid Canada", http://esci-ksp.org/project/smart-grid-canada/?task_id=645.

81. Smart Grid Canada, http://sgcanada.org/.

82. Public Safety Canada, National Strategy for Critical Infrastructure, (Public Safety Canada, 2009), p.2.

83. Emergency Management Policy Directorate, An Emergency Management Framework for Canada (2nd ed.), (Emergency Management Policy Directorate, 2011), p.8.

84. ITU, "Cyber Wellness Profile Canada", http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Canada.pdf, last updated January 2015.

85. Government of Canada, Canada's Cyber Security Strategy For a stronger and more prosperous Canada", http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf, 2010.

86. Government of Canada, "Action Plan 2010-2015 for Canada's Cyber Security Strategy", http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf, 2010.

87. The Canadian Institute, "Cyber Security for Energy: Protecting the Critical Infrastructure of the Oil, Gas and Utility Sectors", http://www.canadianinstitute.com/2015/270/cyber-security-for-energy, 2015.

88. Stephen Starr, "Cyberattack threat in Canada's oil patch raises risk of disruptions, stolen data", http://business.financialpost.com/news/energy/cyberattack-threat-in-canadas-oil-patch-raises-risk-of-disruptions-stolen-data?__lsa=58a4-a33c, 3 January 2013.

89. Information & Privacy Commissioner, Ontario, Canada, "Operationalizing Privacy by Design: The Ontario Smart Grid Case Study", https://www.ipc.on.ca/images/Resources/pbd-ont-smartgrid-casestudy.pdf, 2011.

90. ENEL Foundation, "Energy Transitions in Cities. Lifestyle, experimentation and change: Fourth Case Study – Santiago de Chile", http://www.enel.com/it-IT/doc/enel_foundation/library/papers/ef_wp4.2014_euricur_santiago.pdf, Working Paper 4/2014.

91. International Trade Administration, "Opportunities for U.S. Renewable Energy and Smart Grid Exporters in Peru's Electricity Market", Industry & Analysis (I&A) Market Intelligence Brief, August 2014.

92. NRECA, "Chile **SOCOEPA AMI Project Profile",** http://www.nreca.coop/what-we-do/international-programs/smart-grid-initiative/smart-grid-alliance/pilot-projects/chile/.

93. United Nations ECLAC & Cooperazione Italiano, "Smart grids in Latin America and the Caribbean", http://repositorio.cepal.org/bitstream/handle/11362/3987/S2012019_es.pdf?sequence=1, Project Document, July 2012.

94. Electric Light & Power, "Chile, U.S. to work together on smart grid, renewable energy", http://www.elp.com/articles/2014/07/chile-u-s-to-work-together-on-smart-grid-renewable-energy.html, 7 February 2014.

95. Kamstrup, "Smart Grid Prepared", https://www.kamstrup.com/en-uk/case-stories/electricity-casestories/case-tecnet-smart-metering-chile.

96. Transmission and Distribution World, "AMI Pilot for Starters", http://tdworld.com/ami/ami-pilot-starters, Eduardo Mora TECNET, August 2013.

97. SmartGridNews.com, "South American smart grid market at the starting line", http://www.smartgridnews.com/story/south-american-smart-grid-market-starting-line/2013-06-19, 19 June 2013.

98. PennEnergy, “Leading energy provider in Chile ramping up for the Smart Grid”, http://www.pennenergy.com/articles/pennenergy/2012/04/leading-energy-provider.html, 19 April 2012.

99. Energy News, “Chile aims to include smart grids to its national energy strategy”, http://www.energynews.es/english/chile-aims-to-include-smart-grids-to-its-national-energy-strategy/, 25 October 2013.

100. Trend Micro/OAS, “Report on Cybersecurity and Critical Infrastructure in the Americas”,http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf?mkt_tok=3RkMMJWWfF9wsRoluK3MZKXonjHpfsX74uwlXaKylMI/0ER3fOvrPUfGjI4DTMZiI+SLDwEYGJlv6SgFQ7TAMaN43rgNXRM=, 2015.

101. Trend Micro/OAS, “Latin American and Caribbean Cybersecurity Trends and Government Responses”, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf, 2013.

102. U.S. Department of State, “Strengthening Cyber Security in the Americas”, http://www.state.gov/s/cyberissues/releasesandremarks/185700.htm, Remarks by Christopher Painter, Coordinator for Cyber Issues Inter-American Committee Against Terrorism, 7 March 2012.

103. CICTE, “Declaration Strengthening Cyber-Security in the Americas”, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/OAS%20-%20STRENGTHENING%20CYBER-SECURITY%20IN%20THE%20AMERICAS.pdf, 7 March 2012.

104. OAS & Symantec, “Latin American and Caribbean Cyber Security Trends”, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/OAS-Symantec_Cyber_Security_Report_2014.pdf, June 2014.

105. ITU, “Cyberwellness Profile Chile”, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Chile.pdf, last updated 11 February 2015.

106. Global Gas Transport, “Critical Infrastructure Protection: Strategies for securing gas pipeline infrastructure”, http://www.globalgastransport.info/archive.php?id=12663, 1 June 2013.

107. IEEE Spectrum, “China Pushes Past U.S. in Smart Grid Spending”, http://spectrum.ieee.org/energywise/energy/the-smarter-grid/china-pushes-past-us-in-smart-grid-spending, 21 February 2014.

108. IEEE Smart Grid, “China’s Smart Grid Program: One Goal, Two Main Lines, Three Stages and More”, http://smartgrid.ieee.org/october-2012/684-china-s-smart-grid-program-one-goal-two-main-lines-three-stages-and-more, October 2012.

109. greentechgrid, “Some Snapshots of China’s Smart Grid”, http://www.greentechmedia.com/articles/read/a-snapshot-of-chinas-smart-grid, 25 June 2013.

110. Worldwatch Institute, “Smart Grid Investment Grows with Widespread Smart Meter Installations”,http://vitalsigns.worldwatch.org/sites/default/files/vital_signs_smart_grid_final_pdf.pdf, 22 May 2014.

111. Policy Innovation EastWest Institute, “China’s Critical Cyber Infrastructure Protection”, http://ewipolicy.tumblr.com/post/64666359685/chinas-critical-cyber-infrastructure-protection, 21 October 2013.

112. McAfee, In the Dark: Crucial Industries Confront Cyberattacks”, http://www.mcafee.com/sg/resources/reports/rp-critical-infrastructure-protection.pdf.

113. ITU, “Cyber Wellness Profile China”, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/China.pdf, last updated January 2015.

114. Michael D. Swaine, “Chinese Views on Cybersecurity in Foreign Relations”, http://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf, 2013.

115. Georgetown Journal of International Affairs, “U.S.-CHINA CYBERSECURITY RELATIONS: UNDERSTANDING CHINA’S CURRENT ENVIRONMENT, http://journal.georgetown.edu/u-s-china-cybersecurity-relations-understanding-chinas-current-environment/, 15 September 2014.

116. PCWORLD, “China develops its first homegrown server amid cybersecurity concerns”, HTTP://WWW.PCWORLD.COM/ARTICLE/2838692/CHINA-DEVELOPS-ITS-FIRST-HOMEGROWN-SERVER-AMID-CYBERSECURITY-CONCERNS.HTML, 24 OCTOBER 2014.

117. CLP, “Smart Grid”, https://www.clp.com.hk/ourcompany/electricityjourney/powergrid/smartgrid/Pages/smartgrid.aspx.

118. The University of Hong Kong, “Smart Grid, Smart Planet”, http://www.hku.hk/research/video/7820/.

119. Digital 21 Strategy Advisory Committee, “Cyber Security”, http://www.digital21.gov.hk/eng/D21SAC/attachments/D21SAC_paper_9-2011.pdf, Paper No. 9/2011, 3 November 2011.

120. Cyber Security Symposium 2014, “Keynote Speech by Mr Victor Lam, JP, Deputy Government Chief Information Officer”, http://www.ogcio.gov.hk/en/news_and_publications/speeches/2014/01/sp_20140116.htm, 16 January 2014.

121. ITU, “Cyberwellness Profile Hong Kong”, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Hongkong.pdf, last updated 12 August 2014.

122. APEC, “Counter-Terrorism Action Plan – Hong Kong, China”, http://mddb.apec.org/Documents/2014/CTWG/CTWG1/14_ctwg1_008.pdf, 2014/SOM1/CTWG/008, 1st Counter-Terrorism Working Group Meeting, China, 22-23 February 2014.

123. Between the Poles, “Electric power, renewables and smart grid in Indonesia”, http://geospatial.blogs.com/geospatial/2011/10/electric-power-renewables-and-smart-grid-in-indonesia.html, October 2011.

124. Engerati, “Southeast Asia’s Smart Grid Market is Growing”, http://www.engerati.com/article/southeast-asia%E2%80%99s-smart-grid-market-growing, 14 May 2014.

125. PR Newswire, “Southeast Asian Countries To Invest $13.6bn In Smart Grid Infrastructure’, http://www.prnewswire.com/news-releases/southeast-asian-countries-to-invest-136bn-in-smart-grid-infrastructure-279107171.html, 14 October 2014.

126. Coordinating Ministry of Economic Affairs, “Smart Grid Development Policy in Indonesia”, http://www.egnret.ewg.apec.org/meetings/egnret40/[E4]%20Indonesia.pdf, Republic of Indonesia, 2 April 2013.

127. The World Bank, “Indonesia - Capacity Building for Smart Grid Investment for Transmission and Distribution Project : resettlement plan : Land acquisition and resettlement policy framework”, http://documents.worldbank.org/curated/en/2014/01/18805987/indonesia-capacity-building-smart-grid-investment-transmission-distribution-project-resettlement-plan-land-acquisition-resettlement-policy-framework, 15 January 2014.

128. McAfee/CSIS, “In the Dark - Crucial Industries Confront Cyberattacks”, http://www.mcafee.com/sg/resources/reports/rp-critical-infrastructure-protection.pdf, 2012.

129. ITU, “Cyberwellness Profile Indonesia”, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Indonesia.pdf, last updated 5 October 2014.

130. http://www.futuregov.asia/articles/5924-indonesia-plans-to-set-up-national-cyber-security-agency, December 2014.

131. DAKA Advisory, “Meeting the cyber security challenge in Indonesia: AN Analysis of threats and responses”, http://dakaadvisory.com/wp-content/uploads/DAKA-Indonesia-cyber-security-2013-web-version.pdf, Commissioned by the British Embassy Jakarta, 2013.

132. ITU, “Cyber Wellness Profile Japan”, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Japan.pdf, last updated January 2015.

133. The Japan Times, “Smart grid systems key area of focus”, http://www.japantimes.co.jp/news/2014/11/04/business/smart-grid-systems-key-area-focus/#.VV1GzWkjFVA, 4 November 2014.

134. Metering & Smart Energy International, “Smart grid trends in Japan: 7 things to know”, http://www.metering.com/smart-grid-trends-in-japan-7-things-to-know/, 4 March 2015.

135. ets insights, “Japan’s Smart City Initiatives: Four Model Areas the World Can Watch”, http://etsinsights.com/news/japans-smart-city-initiatives-four-model-areas-the-world-can-watch/, 2012.

136. Information Security Policy Council, “Cybersecurity Strategy – Towards a world leading, resilient and vigorous cyberspace”, http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf, 10 June 2013.

137. National Security Strategy. http://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf, 17 December 2013.

138. Dave Clement, Chatham House, “Cyber Security and Global Interdependence: What is critical?”, http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr_cyber.pdf, February 2013.

139. Information Security Policy Council, “International Strategy on Cybersecurity Cooperation-j-initiative for Cybersecurity Japan”, http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf, 2 October 2013.

140. Information Security Policy Council, “The Basic Policy of Critical Information Infrastructure Protection (3rd Edition)”, http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf, 19 May 2014.

141. ITU, “Cyber Wellness Profile Korea”, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Korea.pdf, last updated December 2014.

142. Korea Smart Grid Institute, http://www.smartgrid.or.kr/eng.htm.

143. Korea Smart Grid Insitute, “Smart Grid in Korea”,http://www.iea.org/media/training/bangkoknov13/session_7c_ksgi_korea_smart_grids.pdf, 2013

144. National Security Research Institute, “Protection of Critical Information Infrastructure in Korea”, http://aseanregionalforum.asean.org/files/Archive/13th/2nd%20ARF%20Seminar%20on%20Cyber%20Terrorism%20Cebu%20City,%20Philippines,%203-5%20October%202005/Annex%20H-Republic%20of%20Korea%20Country%20Report.pdf, 2005.

145. Ministry of National Defense, Republic of Korea, "2012 Defense White Paper", http://www.mnd.go.kr/user/mnd_eng/upload/pblictn/PBLICTNEBOOK_201308130553561260.pdf, 2012.

146. "National Cyber Security Masterplan", http://www.sicurezzacibernetica.it/en/[South%20Korea]%20National%20Cyber%20Security%20Strategy%20-%202011%20-%20EN.pdf, 2 August 2011.

147. "Seoul Framework for and Commitment to Open and Secure Cyberspace", https://www.gccs2015.com/sites/default/files/Seoul%20Framework.pdf, 2013.

148. Centre for Security Studies ETHZurich, "INTERNATIONAL CIIP HANDBOOK 2008/ 2009", http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf, 2009.

149. Engerati, "Southeast Asia's Smart Grid Market is Growing", http://www.engerati.com/article/southeast-asia%E2%80%99s-smart-grid-market-growing, 14 May 2014.

150. PR Newswire, "Southeast Asian Countries To Invest $13.6bn In Smart Grid Infrastructure', http://www.prnewswire.com/news-releases/southeast-asian-countries-to-invest-136bn-in-smart-grid-infrastructure-279107171.html, 14 October 2014.

151. FMT News, " TNB's smart grid to cut electricity bills", http://www.freemalaysiatoday.com/category/nation/2015/02/16/tnbs-smart-grid-to-cut-electricity-bills/, 16 February 2015.

152. CIRED Malaysia, "Smart Grid Implementation: Opportunities & Challenges for Malaysia", http://www.ieee-isgt-asia.org/files/2013/04/SMART-GRID-CHALLENGES-OPPORTUNITIES-FOR-MALAYSIA.pdf, May 2014.

153. SilverSpring, "Masers Energy and Silver Spring Networks Team on Smart Infrastructure for Malaysia - Silver Spring to Lead Smart Infrastructure Coordination Across Masers' Smart Grid City and Green Special Economic Zone in Melaka", http://www.silverspringnet.com/article/masers-energy-and-silver-spring-networks-team-on-smart-infrastructure-for-malaysia/#.VVGYv2kjFVA, 22 April 2013.

154. Electric Light & Power, "Trilliant, Malaysia's TNB agree to smart grid tech exchange", http://www.elp.com/articles/2014/04/trilliant-malaysia-s-tnb-agree-to-smart-grid-tech-exchange.html, 24 April 2014.

155. Metering & Smart Energy, "Smart grid: Malaysia prepares for pilot in June 2014", http://www.metering.com/smart-grid-malaysia-prepares-for-pilot-in-june-2014/, 24 April 2014.

156. CNII Portal, http://cnii.cybersecurity.org.my/main/about.html, CyberSecurity Malaysia, last accessed 12 May 2015.

157. Ministry of Science, Technology And Innovation, “National Cyber Security”, http://cnii.cybersecurity.org.my/main/ncsp/NCSP-Policy2.pdf.

158. ITU, “Cyberwellness Profile Malaysia”, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Malaysia.pdf, last updated 22 January 2015.

159. DAKA Advisory, “Digital Development in Malaysia: An analysis of cyber threats and responses”, http://dakaadvisory.com/wp-content/uploads/DAKA-Malaysia-cyber-security-2014-web-version.pdf, Commissioned by the British High Commission in Kuala Lumpur, 2014.

160. IEEE SmartGrid, “Impact of Reforms on the Smart Grid Model of Mexico”, http://smartgrid.ieee.org/october-2014/1162-impact-of-reforms-on-the-smart-grid-model-of-mexico, October 2014.

161. Smart Grid Mexico, “Why Smart Grid”, http://www.smartgridmexico.org/es/.

162. SmartGrid CI, “Mexico is jumping into smart meters, the smart grid and energy market liberalization all at once”, http://smartgrid-ci.com/mexico-jumping-a-new-energy-world/, 21 October 2014.

163. Elster, “Comision Federal de Electricidad (CFE) Selects Elster for Mexico City's First AMI Smart Grid Project”, http://www.elster.com/en/press-releases/2011/1551785, 19 April 2011.

164. PennEnergy, “Report: Mexico's smart grid market to reach $7.42 billion by 2020”, http://www.pennenergy.com/articles/pennenergy/2013/07/mexicos-smart-grid-market-to-reach-over-7b-by-2020.html, 26 June 2013.

165. SilverSpring Networks, “Silver Spring Networks Selected for Comisión Federal de Electricidad (CFE) Smart Grid Program in Mexico City”, http://www.silverspringnet.com/article/silver-spring-networks-selected-for-comision-federal-de-electricidad-cfe-smart-grid-program-in-mexico-city/#.VVA842kjFVA .

166. ets insights, “Mexico Smart Grid Outlook, 2012 – 2020”, http://etsinsights.com/reports/mexico-smart-grid-outlook-2012-2020/, 23 July 2013.

167. Northeast Group LLC, “Mexico SmartGrid: Market Forecast (2013 – 2023)”, http://www.northeast-group.com/reports/Brochure-Mexico%20Smart%20Grid%20Market%20Forecast%20(2013-2023)-Northeast%20Group.pdf, November 2013.

168. Electric Light & Power, “Mexico smart grid market to grow to $2.1 billion per year”, http://www.elp.com/articles/2013/11/mexico-smart-grid-market-to-grow-to-2-1-billion-per-year.html, 11 June 2013.

169. United Nations ECLAC & Cooperazione Italiano, “Smart grids in Latin America and the Caribbean”, http://repositorio.cepal.org/bitstream/handle/11362/3987/S2012019_es.pdf?sequence=1, Project Document, July 2012.

170. The.Report Company, "Defending Mexico's critical infrastructure against threats", http://www.the-report.net/mexico-prw/600-defending-mexico-s-critical-infrastructure-against-threats, 22 July 2013.

171. McAfee/CSIS, "In the Dark - Crucial Industries Confront Cyberattacks", http://www.mcafee.com/sg/resources/reports/rp-critical-infrastructure-protection.pdf, 2012.

172. FTI Journal, "Mexico's Energy Reform: How to Meet the Risks and Seize the Opportunities", http://www.ftijournal.com/article/mexicos-energy-reform-how-to-meet-the-risks-and-seize-the-opportunities, January 2015.

173. ITU, "Cyberwellness Profile Mexico", https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Mexico.pdf, last updated 19 February 2015.

174. Northeast Group LLC, "Oceania Smart Grid: Market Forecast (2015 – 2025)", http://www.northeast-group.com/reports/Brochure-Oceania%20Smart%20Grid-Market%20Forecast%202015-2025-Northeast%20Group.pdf, May 2015.

175. ITU, "Cyberwellness Profile New Zealand", https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/New_Zealand.pdf.

176. Ministry of Business, Innovation, and Employment, "New Zealand Smart Grid Forum", http://www.med.govt.nz/sectors-industries/energy/electricity/new-zealand-smart-grid-forum.

177. New Zealand Smart Grid Forum, "NZ Smart Grid Forum: first six month report to the Minister of Energy ", http://www.med.govt.nz/sectors-industries/energy/electricity/new-zealand-smart-grid-forum/meeting-4/six-monthly-report-to%20minister.pdf, October 2014.

178. New Zealand Smart Grid Forum, "A catalogue of smart grid standards, publications, trials, case studies and activities in New Zealand", http://www.med.govt.nz/sectors-industries/energy/electricity/new-zealand-smart-grid-forum/meeting-4/workstream-a.pdf, November 2014.

179. National Infrastructure Unit, New Zealand National Infrastructure Plan, (New Zealand Government, 2011).

180. New Zealand Cyber Security Centre, http://www.ncsc.govt.nz/about-us/.

181. New Zealand Government, "NEW ZEALAND'S CYBER SECURITY STRATEGY", http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf, 2011.

182. National Cyber Security Centre, "Voluntary Cyber Security Standards for Industrial Control Systems

v.1.0", http://www.ncsc.govt.nz/assets/NCSC20voluntary20cyber20security20standards20for20ICD20v.1.0.pdf, March 2014.

183. Asian Development Bank, *Engagement in Fragile and Conflict-Affected Situations - Understanding and Responding to a Fragile Situation: A Pilot Assessment in Papua New Guinea*, http://www.adb.org/sites/default/files/publication/82574/understanding-responding-fragile-situation-png.pdf, September 2014.

184. World Bank Group, "Papua New Guinea Energy Sector Development Project", http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2015/01/06/000469252_20150106165401/Rendered/PDF/934900BRI00P100f0APPROVED000P101578.pdf, last accessed 1 May 2015.

185. Papua New Guinea Department of National Planning and Monitoring, "Papua New Guinea Medium Term Development Plan 2011-2015", http://planipolis.iiep.unesco.org/upload/Papua%20New%20Guinea/Papua_New_Guinea_MTDP_2011-2015.pdf, October 2010.

186. ITU, "Cyberwellness Profile Papua New Guinea", http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Papua_New_Guinea.pdf, last updated 12 August 2014.

187. APEC Submission by Papua New Guinea, "2009 Counter Terrorism Action Plan-Papua New Guinea", 2009.

188. International Trade Administration, "Opportunities for U.S. Renewable Energy and Smart Grid Exporters in Peru's Electricity Market", Industry & Analysis (I&A) Market Intelligence Brief, August 2014.

189. Metering and Smart Energy International, " Smart grid under study in Peru", http://www.metering.com/smart-grid-under-study-in-peru/, August 2012.

190. ITU, "Cyberwellness Profile Peru", http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Peru.pdf, last updated 19 February 2015.

191. OAS, "Peru Hosts OAS Cyber Crisis Simulation", http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-354/13, 23 September 2013.

192. Electric Power Industry Management Bureau, Department of Energy, "Philippines Smart Grid Vision", http://gsi.nist.gov/global/docs/apec2012/6-2-Capongcol.pdf, April 2012.

193. greentechgrid, "Philippines to Get Smart Metered With GE, Trilliant", http://www.greentechmedia.com/articles/read/philippines-to-get-smart-metered-with-ge-trilliant, 5 November 2013.

194. GMA News Online, "DoE committee to develop Smart Grid plan for power sector", http://www.gmanetwork.com/news/story/299865/economy/business/doe-committee-to-develop-smart-grid-plan-for-power-sector, March 2013.

195. ets insights, "Philippines Department of Energy creates smart grid committee for power industry".

196. http://etsinsights.com/news/philippines-department-of-energy-creates-smart-grid-committee-for-power-industry/, March 2013.

197. USTDA, "USTDA PROMOTES SMART GRID IMPLEMENTATION IN MANILA: *Clean Energy Pilot Project Builds on USACEP Cooperation*", http://www.ustda.gov/news/pressreleases/2014/southasia/philippines/philippinessmartgrid_012214.asp, Press Release, 22 January 2014.

198. SMARTGRID, "Directive from the Philippines' DOE Divulges Plans for Smart Grid", http://smart-grid.tmcnet.com/topics/smart-grid/articles/2013/03/18/330854-directive-from-philippines-doe-divulges-plans-smart-grid.htm, 18 March 2013.

199. Republic of the Philippines Department of Energy, "Department Circular No DC 2013-03-0003", http://www2.doe.gov.ph/popup/DC2013-03-0003.pdf, 2013.

200. Criminal Investigation and Detection Group, "G-CSIRT: Cyber Watchdog Launched", http://www.4law.co.il/ph1.htm.

201. ITU, "Cyberwellness Profile Philippines", http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Philippines.pdf, last updated 23 October 2014.

202. APEC Expert Group on Energy Efficiency and Conservation (EGEE&C), "Draft Meeting Summary", 43rd Meeting APEC EGEE&C 43, April 2014.

203. Philippine Daily Inquirer, "Microsoft, PNP to strengthen Philippine cybersecurity", http://newsinfo.inquirer.net/671724/microsoft-pnp-to-strengthen-philippine-cybersecurity, February 2015.

204. Office of the President, "NATIONAL CYBER SECURITY PLAN", http://icto.dost.gov.ph/wp-content/uploads/2014/07/Cyber-Plan-Pre-Final-Copy_.pdf, Task Force for the Security of Critical Infrastructure (TFSCI), 8 August 2004.

205. ph_cybersecurity, "Philippine National Cyber Security Plan 2005", http://phcybersecurity.blogspot.sg/2011/09/philippine-national-cyber-security-plan.html.

206. The Philippine Digital Strategy, "TRANFORMATION 2.0: DIGITALLY EMPOWERED NATION", http://www.ncc.gov.ph/files/PDS.pdf, 2011

207. thinkRussia, "RUSSIA TO INVEST IN SMART GRID ELECTRICAL INFRASTRUCTURE", http://www.thinkrussia.com/business-economy/russia-invest-smart-grid-electrical-infrastructure, 22 December 2014.

208. ets insights, "RUSSIA SMART GRID MARKET ANALYSIS", HTTP://ETSINSIGHTS.COM/REPORTS/RUSSIA-SMART-GRID-MARKET-ANALYSIS/, MARCH 2013.

209. USAID & USEA, "JOINT RUSSIAN/AMERICAN STUDY ON LEGAL/REGULATORY, MARKET, CONSUMER AND TECHNICAL IMPEDIMENTS TO SMART GRID TECHNOLOGY DEPLOYMENT", http://www.usea.org/sites/default/files/US-Russia%20Smart%20Grid%20Impediments%20Study%20-%20Final.pdf, September 2012.

210. United States Energy Association (USEA), "Russian-American Smart Grid Partnership:, http://www.usea.org/program/russian-american-smart-grid-partnership.

211. DNV KEMA Energy & Sustainability, "Market scan smart meters and smart grids in Russia",http://www.rvo.nl/sites/default/files/Final%20report%20DNV%20KEMA%20Market%20scan%20smart%20grids%20and%20smart%20meters%20in%20Russia.pdf, 15 March 2013. Katri Pynnöniemi, Researcher, The Finnish Institute of International Affairs, "Critical infrastructure protection: an evolution of Russian policy", http://www.fiia.fi/assets/events/Presentation_KP_18_12_poist.pdf.

212. ITU, "Cyberwellness Profile Russian Federation", http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Russia.pdf, last updated 22 January 2015.

213. "INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION",http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument, Approved by President of the Russian Federation Vladimir Putin, 9 September 2000 (29 December 2008).

214. APEC Expert Group on Energy Efficiency & Conservation (EGEE&C 43), "43rd Meeting: Draft meeting summary", https://www.google.com.sg/search?sugexp=chrome,mod=11&sourceid=chrome&ie=UTF8&q=APEC+Expert+Group+on+Energy+Efficiency+and+Conservation+(EGEE%26C)%2C+%E2%80%9CDraft+Meeting+Summary%E2%80%9D%2C+43rd+Meeting+APEC+EGEE%26C+43%2C+April+2014, 11 April 2014.

215. Energy Market Authority, "Smart Grid Initiative in Singapore", http://www.kpmg.com/Global/en/industry/Energy-Natural-Resources/global-energy-conference/aspac/Documents/Singapore-Smart-Grid-Initiative.PDF.

216. National climate change Secretariat and national research Foundation, "Smart grid Technology primer: a Summary", https://www.nccs.gov.sg/sites/nccs/files/Smart%20Grid%20Primer.pdf, 2011.

217. SilverSpring, "Singapore Power Wins Smart Grid Project of the Year with Silver Spring Networks", http://www.silverspringnet.com/article/singapore-power-wins-smart-grid-project-of-the-year-with-silver-spring-networks/#.VVMcIGkjFVB, September 2014.

218. Eco Business, "Future cities: the rise and rise of smart grids", http://www.eco-business.com/news/future-cities-rise-rise-smart-grids/, December 2013.

219. National Security Coordination Centre, "The Fight Against Terror: Singapore's National Security Strategy", http://www.nscs.gov.sg/public/download.ashx?id=48, 2004.

220. Defence Science & Technology Agency (DSTA), "Realising Critical Infrastructure Capability", https://www.dsta.gov.sg/programmes/dsta-masterplanning-and-systems-architecting/realising-critical-infrastructure-capability.

221. CSA Singapore, https://www.csa.gov.sg/.

222. IDA, "National Cyber Security Masterplan 2018", http://www.ida.gov.sg/~/media/Files/Programmes%20and%20Partnership/Initiatives/2014/ncsm2018/NationalCyberSecurityMasterplan%202018.pdf.

223. Energy Studies Institute, "ROUNDTABLE H: CYBER SECURITY IN THE ENERGY SECTOR", http://www.siew.sg/about-siew/past-events/siew-2014/roundtables/roundtable-h-cyber-security-in-the-energy-sector, 31 October 2014.

224. A*Star, "A*STAR rolls out new initiative to power Singapore's Smart Nation vision", http://www.a-star.edu.sg/Media/News/Press-Releases/ID/3664/ASTAR-rolls-out-new-initiative-to-power-Singapores-Smart-Nation-vision.aspx, 23 October 2014.

225. ITU, "Cyberwellness Profile Singapore", http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Singapore.pdf, last updated 12 August 2014.

226. IDA Singapore, "Annex A: Factsheet on National Cyber Security Masterplan 2018", https://www.ida.gov.sg/~/media/Files/About%20Us/Newsroom/Media%20Releases/2013/0724_ncsm/AnnexA.pdf.

227. http://www.siew.sg/about-siew/past-events/siew-2014/roundtables/roundtable-h-cyber-security-in-the-energy-sector

228. Centre for Security Studies ETHZurich, "INTERNATIONAL CIIP HANDBOOK 2008/ 2009", http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf, 2009.

229. APEC CTWG Workshop on CISR, "Singapore's Approach: Critical Infrastructure Protection", http://www.apec-epwg.org/public/uploadfile/act/98c54734e9ad749df3f5c174a50491c2.pdf, 16-17 October 2014.

230. IDA, "National Cyber Security Masterplan 2018", http://www.ida.gov.sg/~/media/Files/Programmes%20and%20Partnership/Initiatives/2014/ncsm2018/NationalCyberSecurityMasterplan%202018.pdf.

231. Slideshare, "Chinese Taipei's Regulatory Update", http://www.slideshare.net/bdyakin1/chinese-taipei-ct001-1366598053, APEC Telecommunications and Information Working Group, 47th Meeting 22-27 April 2013, Indonesia. [This document is not an official APEC document until

approved by the Telecommunications and Information Working Group. This version is a draft provided for discussion purposes only.]

232. APEC, "Development of Smart Grid in Chinese Taipei", http://mddb.apec.org/Documents/2011/EWG/WKSP4/11_ewg_wksp4_012.pdf, 2011/EWG42/WKSP1/012, Submitted by Chinese Taipei, Knowledge Sharing Platform Workshop for the Energy Smart Communities Initiative, Chinese Taipei, 17-18 October 2011.

233. APEC Energy Working Group, ESCI Knowledge Sharing Platform, http://esci-ksp.org/economy/chinese_taipei/.

234. Jesse Berst, "Chinese Taipei steps up smart grid investments, cites benefits from earlier AMI", http://www.smartgridnews.com/story/Chinese Taipei-steps-smart-grid-investments-cites-benefits-earlier-ami/2011-12-19, 19 December 2011.

235. Ministry of Economic Affairs, "2011 APEC Workshop on Addressing Challenges in AMI Deployment and Smart Grids in APEC", http://www.communications.org.tw/page.php?pg=detail&lang=eng&unit=1663&cone=4&ctwo=27, 2011.

236. (ROC) Chinese Taipei Executive Yuan, "APEC critical infrastructure workshop kicks off in Taipei", http://www.ey.gov.tw/en/News_Content.aspx?n=1C6028CA080A27B3&s=E02A946CFF927200, Department of Information Services Executive Yuan, 16 October 2014.

237. Office of Homeland Security Chinese Taipei, "The Developments and Trends of Critical Infrastructure Protection in Chinese Taipei", http://www.apec-epwg.org/public/uploadfile/act/4734ae56233c37cfa4656022c6aac21a.pdf, 16 October 2014.

238. APEC Submission by Chinese Taipei, "Counter-Terrorism Action Plan – Chinese Taipei", http://www.apec.org/~/media/Files/Groups/CTAPs/2013/2013_cttf1_016_ChineseTaipei.pdf, 2013/SOM1/CTTF/016, 28th Counter Terrorism Task Force Meeting Indonesia, January 2013.

239. Russell Hsiao, "Critical Node: Chinese Taipei's Cyber Defense and Chinese Cyber-Espionage",http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=41721&cHash=3505e552d9d50d88cfc539af1319e699#.VUHXKGkjFVB, The Jamestown Foundation, 5 December 2013.

240. William Lowther, "US has concerns over Chinese Taipei's defense: report", http://www.taipeitimes.com/News/Chinese Taipei/archives/2014/06/22/2003593394, Taipei Times, 22 June 2014.

241. Michael Gold, "Chinese Taipei seeks stronger cyber security ties with U.S. to counter China threat", http://www.businessinsider.com/r-Chinese_Taipei-seeks-stronger-cyber-security-ties-with-us-to-counter-china-threat-2015-3?IR=T&, Business Insider, 30 March 2015.

242. Annex Power, "MARKET POTENTIAL FOR SMART GRID TECHNOLOGY IN THAILAND AND VIET NAM", http://www.thai-german-cooperation.info/download/20131009_market_potential_th_vn.pdf, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH (on behalf of theGerman Federal Ministry of Economics and Technology (BMWi)), January 2013.

243. ZVEI, "Smart Grid in Thailand and Viet Nam", http://www.zvei.org/en/markets-and-law/foreign-trade/Pages/Smart-Grid-in-Thailand-and-Viet Nam.aspx, 2014.

244. PEA, "Smart Grid Initiative and Roadmap In Thailand", http://www.gmsarn.com/conference2011/document/presentations/Mr.Weerachai-SmartGridInitiative&RoadmapInThailand.pdf, 2012.

245. Critical Infrastructure Protection & Resilience Asia, "Securing critical infrastructure across ASEAN", http://cip-asia.com/, June 2015.

246. Deputy Executive Director, Electronic Transactions Development Agency (Public Organization) Ministry of Information and Communication Technology, Thailand, "Protecting Critical Information Infrastructure in Thailand", http://www.nisc.go.jp/security-site/campaign/ajsympo/pdf/paneldiscussion2(Thailand).pdf.

247. ITU, "Cyberwellness Profile Thailand", http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Thailand.pdf, last updated 17 December 2014.

248. Bangkok Post, "IT law update (PART 1): The Cybersecurity Bill", http://www.bangkokpost.com/business/news/459490/it-law-update-part-1-the-cybersecurity-bill, 23 January 2015.

249. U.S. Department of Energy, "2014 Smart Grid System Report: Report to Congress August 2014", http://energy.gov/sites/prod/files/2014/08/f18/SmartGrid-SystemReport2014.pdf, August 2014.

250. The White House, Office of the Press Secretary, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience: PRESIDENTIAL POLICY DIRECTIVE/PPD-21", https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, 12 February 2013.

251. The White House, Office of the Press Secretary, "EXECUTIVE ORDER: IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY", https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, 12 February 2013.

252. ITU, "Cyber Wellness Profile United States" http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/United_States.pdf, last updated January 2015.

253. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity Version

1.0", http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf 12 February 2014.

254. The Department of Defense, "The DoD Cyber Strategy", http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, April 2015.

255. Norton Rose Fulbright, "Energy cybersecurity – a critical concern for the nation", http://www.dataprotectionreport.com/2015/04/energy-cybersecurity-a-critical-concern-for-the-nation/, 9 April 2015.

256. Annex Power, "Market Potential for Smart Grid Technology in Thailand and Viet Nam", http://www.thai-german-cooperation.info/download/20131009_market_potential_th_vn.pdf, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH (on behalf of the German Federal Ministry of Economics and Technology), January 2013.

257. ITU, "Cyberwellness Profile Viet Nam", http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Viet Nam.pdf, last updated 19 February 2015.

258. Information Technology Industry Council, "Comments on Viet Nam's Draft Law on Information Security, version 2.22", http://www.itic.org/dotAsset/83fe0977-25ae-4382-ae0a-60226856f182.pdf, Addressed to the Ministry of Information and Communications, 10 July 2013.

259. James, Lewis, "Asia: The Cybersecurity Battleground", http://csis.org/files/attachments/130723_jimlewis_testimony_v2.pdf, Statement before the House Foreign Affairs Committee, Subcommittee on Asia and the Pacific, 23 July 2013.

260. United Nations General Assembly A/68/98*, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf, 24 June 2013.

This page intentionally left blank.

Appendix A:
Example of Cyber-Energy Nexus Survey Questions

Facility Infrastructure

1 – What forms of energy transmission are critical to your economy and population (e.g. electric power, oil, natural gas)?

2 – Where are energy generation (e.g. electric power plant, refinery) plants located? 2a – Where are energy control (e.g. substations, distribution centers) locations?

3 – Are Industrial Control Systems (ICS), Plant Logic Controllers (PLC), Supervisory Control And Data Acquisition (SCADA) and digital sensors/meters protected?

4 – What types of equipment or systems are used in energy systems that do not require an operator for day-to-day operations? (**We may want to reconsider this question or ask a different way since this answer may be too large a list to expect from the respondent**)

5 – Are there equipment or machines that do not require the human-machine interface of Industrial Control Systems (ICS), Plant Logic Controllers (PLC), or Supervisory Control And Data Acquisition (SCADA) systems or digital sensors meters? (i.e., automated and programmed systems that can be hacked remotely)

Network Infrastructure

6 – What energy system components are integrated into information technology networks?

7 – Do any Industrial Control Systems (ICS), Plant Logic Controllers (PLC), or Supervisory Control And Data Acquisition (SCADA) systems connect to the Internet?
7a – Are energy system(s) connected to Internet?

8 – Are adaptors used to bridge older technologies into a network?

9 –Is IPv4 or IPv6 used at the energy facility?

10 – Are any servers present or identified as development networks that are connected or isolated from the rest of the main network or system?

11 – Are firewalls used in the network to isolate and protect the facility network from the external Internet networks?

12 – Are there corporate spam filters used?

Technology Capabilities

13 – Are Wi-Fi or other wireless networking capabilities utilized in energy generation or control systems?
13a – Are other forms of remote controlled equipment used?

14 – Is there any malware or intrusion detection in place?

15 – Are there systems connected in a Read-Only mode? (for monitoring)

16 – Are redundant safety features implemented (failsafe switches in software)?

17 – Are smart meters and sensors used (i.e., meters and sensors with microcontrollers and or network capabilities built in)?

Policy and Procedures

18 – Does the energy entity/sector currently have or use a cybersecurity plan?

19 – What are the browsing practices policies for employees?

20 – Are audits performed to ensure compliance with a cybersecurity plan?

21 – Are audits random and no-notice?

22 – Are personal portable media drives allow in the facilities?

23 – Is there a personnel reliability and/or clearance program procedure in place?

24 – Is there a supply chain assurance program present and used?

Facility/Industry History

25 – Have any cyber threats been previously identified, if so what are they?

Offsite/Remote Locations

26 – Are there any remote offsite extensions or locations from major energy facilities?

27 – Is there an open energy market present or are there smaller contributors involved with the related energy sector (i.e., private water power plants, wind turbines, solar collectors)?

Example of Cyber-Energy Nexus Member Survey

Date:

Economy:

Representative's Name: Position:

1 – How does your economy define a critical cyber energy asset?

2 – What forms of energy are critical to your country/economy (e.g. electric power, oil, natural gas)? What parts of your energy infrastructure are "smart" or networked systems that connect to the Internet?

3 – What cybersecurity policies, protocols and/or standards govern your energy infrastructure?

4 – Are audits performed by external authorizing agencies to ensure compliance to the cybersecurity policies, protocols and/or standards used for your energy-infrastructure? If 'Yes', how often are they performed?

5 – What challenges have you encountered in networking energy-infrastructure?

6 – What opportunities have been or can be applied to the networking energy-infrastructure to improve cyber-energy security (i.e., demand response, increased efficiencies, interoperability, updated methodologies)?

This page intentionally left blank.