IEA IMPLEMENTING AGREEMENT FOR A CO-OPERATIVE PROGRAMME ON SMART GRIDS (ISGAN)

Smart Grid Cyber Security

ISGAN white paper
Annex 4, Subtask 3.4

Mackay MILLER, National Renewable Energy Laboratory (USA)
Daniel HAGLUND, Swedish Civil Contingencies Agency (MSB) (Sweden)
Gunhee LEE, Attached Institute of Electronics and Telecommunications Research Institute (ETRI) (Korea)

25 April 2012

Verification: ____X_____ Korea Smart Grid Institute (Operating Agent)
Approval: _____X_____ ISGAN Executive Committee Chair or Vice Chair

From the ISGAN Annex 4 Programme of Work, adopted October 2011:
"This white paper will survey the critical issues in smart grid cyber security, discuss the state of the art, and describe the range of efforts underway to ensure secure, reliable grids."

Abstract:
Maximizing electric sector innovation while minimizing cyber security risk is a key goal of smart grid policy development. Significant policy gaps exist in the field of grid cyber security, and ISGAN is well-positioned to convene stakeholders and foster discussion to advance best practices that support innovation while protecting critical infrastructure and consumer data privacy. This report identifies key issues in cyber security policy design, and suggests potential collaborations for the ISGAN membership.

Partial reproduction of this document is permitted only with written permission from ISGAN, to be obtained from the Operating Agent, the Korea Smart Grid Institute (isgan@smartgrid.or.kr).

Acknowledgements
The authors would like to thank our colleagues for their helpful additions, comments, and technical assistance in reviewing this document, especially Giovanna Dondossola, Axel Strang, Luz Aurora Ortiz Salgado, and David Williamson.

Disclaimer
ISGAN, also known as the IEA Implementing Agreement for a Co-operative Programme on Smart Grids (ISGAN), functions within a framework created by the International Energy Agency (IEA). The views, findings and publications of ISGAN do not necessarily represent the views or policies of the IEA Secretariat, all of its individual member countries or all of ISGAN's Participants.

The ISGAN white papers are meant as inputs into the broader ISGAN dialogue. The findings, analysis, and opinions expressed therein are those of the listed authors only.

Contents

1. Introduction

Awareness of critical infrastructure cyber security issues reached new heights in 2011. New cyber threats emerged, targeted primarily at sensitive industrial control systems. Additionally, consumer data privacy issues took on new importance as millions of new smart meters were deployed. And while the importance of cyber security issues has become increasingly apparent, implementation of comprehensive cyber security remains challenging for two distinct reasons. First, making the business case for significant expenditures on grid cyber security is a complex task: uncertainties around type and level of potential threats, who should bear responsibility for investment, and the actual costs of appropriate preparation all complicate decision making in this vital public policy and corporate governance area. Second, the institutional and cultural barriers to comprehensive cyber security – in other words, the organizational dimension of cyber security -- are substantial. While significant progress has been made on these issues in the more mature field of commercial information technology security, the unique threats, vulnerabilities, and responses in grid control systems merit distinct technical and policy approaches.

In 2012 and beyond, it is possible that public awareness of these issues may be accelerated by events beyond the control of grid operators. Preferably, a culture of smart policy, consumer education, and proactive investment will take root. In this context, this white paper outlines critical issues that should inform ISGAN cyber security efforts.

The report is organized as follows. Section 2 provides a brief overview of smart grid cyber security concepts. Section 3 outlines two key problems in cyber security policy development: *security economics* and *the organizational dimension of security*. Section 4 focuses on the unique issues of consumer data privacy, and potential frameworks for policy development in that domain. Section 5 concludes with a range of possibilities for continued ISGAN research and collaboration.

2. Context – the Cyber Security Landscape

Cyber security, for the purposes of this paper and most ISGAN work, is broadly defined to include the protection of critical infrastructure involved in the generation and delivery of electricity, as well as the protection of data produced by consumer “smart” meters. Across these two domains, five specific security properties are pertinent: [1]

- Confidentiality –information is protected from unauthorized disclosure
- Availability – systems remain operational when needed
- Integrity – systems and information are protected from unauthorized modification
- Authentication – system access is limited exclusively to authorized individuals
- Non-Repudiation – the ability of users or systems to deny responsibility for actions is prevented.

Together, these five properties of cyber security are applicable across the vast majority of cyber-physical systems. Importantly, different applications of smart grids require different security properties, and thus technical preparation (and policy making) is distinct for different parts of the grid. The relevant security properties of five common smart grid systems are shown in Table 1:[1]

Table 1: Smart Grid Cyber Security Requirements

	Smart Grid System / Application	System / Application Definition	Information and Infrastructure Security Requirements	Application Security Requirements
Critical Infrastructure Domain	**Power Markets**	Commodity-based energy markets necessary to balance supply and demand for energy	*Integrity; Availability; Authentication; Confidentiality*	*Integrity; Non-Repudiation*
	Wide Area Measurement, Protection, and Control (WAMPAC)	The set of applications and systems that collectively provide Phasor-Measurement-Unit-based wide-area monitoring (state estimation), protection, and control	*Integrity; Availability; Authentication; Confidentiality*	*Integrity; Availability*
	Energy Management Systems (EMS)	The set of applications and systems used to control bulk power system generation and transmission	*Integrity; Availability; Authentication*	*Integrity*
	Distribution Management Systems (DMS)	Utility IT information systems capable of integrating and analyzing real-time electric distribution data to manage voltage and power at the distribution level	*Integrity; Availability; Authentication*	*Integrity; Availability*
Consumer Data Domain	**Advanced Metering Infrastructures (AMI)**	Systems deployed to provide two-way communication to customer power meters, enabling more granular management of energy pricing, usage, and renewable energy generation	*Integrity; Authentication; Confidentiality*	*Integrity; Non-Repudiation*

Source: Adapted from Govidarasu, Hann, and Sauer (2012)

Preparation in the domain of consumer data protection requires a particular focus on integrity, authentication, and confidentiality, and applications involved in the handling of consumer data should ensure integrity and non-repudiation. In other words, malicious intrusion into AMI applications should be extremely difficult *and* extremely difficult to cover up after the fact. The same principles pertain to applications in the critical infrastructure domain, with the addition of a higher premium placed on *availability*, given the importance of continuous operation of the grid.

It should be noted that risks to the integrity of electrical grids are not isolated to malicious attack. Incidental risks, including operator error, natural disasters, consumer errors, can also contribute to cyber security vulnerability. While this report focuses on malicious attack vulnerabilities, the other types of risk should be kept in mind.

The risks and challenges in the domains of critical infrastructure and consumer data are unique but equally worthy of international discussion and policy coordination.[1] Significant and ongoing coordination is underway in both domains. International coordination in critical infrastructure cyber security is undertaken through a range of multilateral collaborations, including:

[1] While these domains present unique operational and policy challenges, the interplay between them is important. Data security issues have heightened the utility focus on, and expertise in, security issues which can also be applied to their overall control system security environment.

- European Network and Information Security Agency (ENISA) – a multilateral organization dedicated to improving network and information security across the EU.
- Coordination between the US and Korea, including research collaboration between the Attached Institute of the Electronics and Telecommunications Research Institute (the primary smart grid security research institute in Korea) and the University of Illinois at Urbana-Champaign in the US.
- The EU-US Working Group on Cyber-Security and Cyber-Crime, established at a EU-US Summit in November 2010, is tasked with developing collaborative approaches to a wide range of cyber-security and cyber-crime issues.
- European Smart Grid Coordination Group (SG-CG) – set up to implement the Smart Grid Standardisation Mandate M/490 EN[2] to European Standardisation Organisations (CEN/CENELEC/ETSI). The ongoing work, focusing on the gap analysis of existing standards, establishes liaisons with international IEC and NIST technical committees related to the smart grid developments.

At the same time that international collaboration is increasing, as a general trend investment in utility cyber security is also growing. Pike Research, a US-based consultancy, estimates that smart grid cyber security spending will total $14 billion across the 2011-2018 timeframe.[3] Whether this amount is adequate remains to be seen, and ultimately, the impact of investment depends critically on changes to business and security processes within energy companies. But progress is being made in this area too. Multiple conferences on national and international best practices in security have been held in recent years.

But while investment is growing and collaboration is increasing, the 'adversarial community' is also gaining greater awareness of control system vulnerability.[4] At the same time, the range of potential vulnerabilities – the cyber 'vulnerability surface' -- is increasing due to the sheer number of intelligent devices being added to the grid.[2] Indeed, a survey of industry predictions in the US in 2009 reinforces that cyber security issues were perceived to be gaining in importance and potential impact (see Figure 1). In the face of this trend, industry-led efforts are absolutely critical. At the same time, the ability of the utility industry to keep up with the evolving threat landscape depends in no small part on smart policies that promote adequate investment and holistic organizational change.

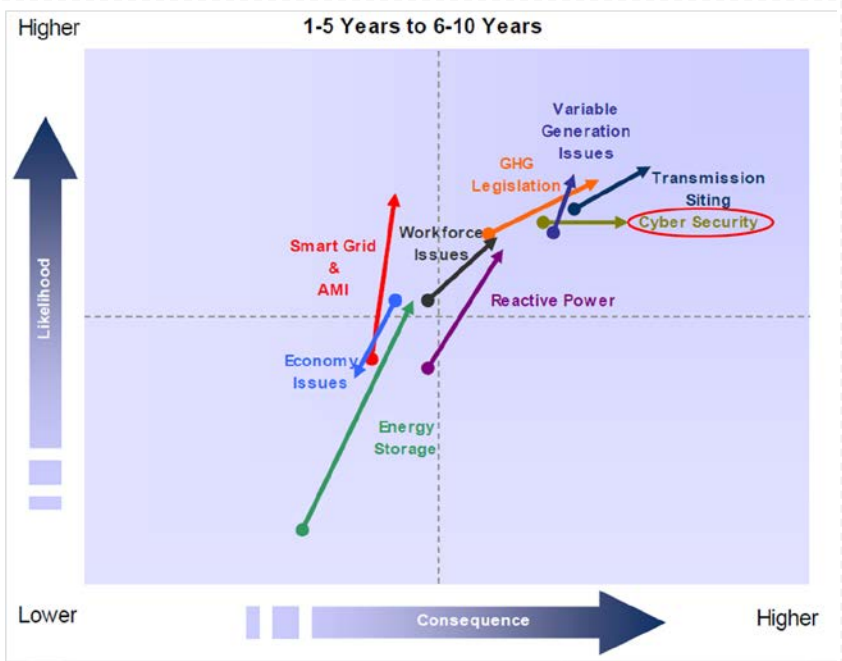

Figure 1: Emerging and Standing Issues identified by a survey of U.S. electric industry participants, Source: NERC Long Term Reliability Assessment, 2009

These complexities have been recognized for quite some time within policy circles. The range of financial, organizational, cultural, and technical challenges facing grid cyber security were clearly spelled out in a 2006 report by the US Department of Energy (DOE) and Department of Homeland Security (DHS), which identified 9 challenges to effective security in the energy sector:[5]

1. *"Limited resources are available within businesses to address security needs.*
2. *Cyber security is a difficult business case.*
3. *Limited knowledge, understanding and appreciation of control systems security risks inhibit sector.*
4. *Insufficient sharing of threat and incident information among government and industry entities.*
5. *Effective security-oriented partnerships between government and industry have been difficult to establish.*
6. *Poor coordination among government agencies creates confusion and inefficiencies.*
7. *New regulation may impose requirements beyond the technical capability of legacy systems.*
8. *Highly educated staff with broad skill sets is needed to manage future operations.*
9. *Increasing sophistication of tools used by hackers."*

There has been significant progress on these issues internationally, and while much work remains to be done, an examination of each is beyond the scope of this report. Instead, broad challenges that cut across several of these issues are identified as immediate priority areas for ISGAN collaboration. The next two sections describe these priority areas in more detail.

3. Key Challenges of Cyber Security Policy Development

In the face of an evolving threat landscape and persistent structural challenges, effective cyber security policy development is especially important. Two questions that are of particular importance to policy makers include:

- What are acceptable expenditures on cyber security? (In other words, when is the system "secure enough"?)
- Will policies have the intended effect, or are there real-world factors that might reduce their effectiveness?

The answers to these questions will be distinct in each grid and electrical market structure, and will evolve over time as underlying technologies, threats, and impacts change. The following sections attempt to provide frameworks to support productive policy dialogues around these two questions.

3.1. Cyber security as a 'security economics' problem

In the field of enterprise IT, the economics of cyber security investment has become a mature field of study in the past 10 years. The conversation is taking place more slowly and unevenly in utility cyber security, in large part due to the highly varied landscape of energy systems around the world. Given this variation, optimal investment in cyber security is a very unique calculation for each utility, and is highly sensitive to organizational profile and vulnerability landscape, which in turn are functions of grid topology, generation sources, market structure, end-user characteristics, and control systems internetworking, among other features.

Across this varied landscape, cyber security risk can be conceptualized as the product of *threats*, *vulnerabilities*, and *impacts*. While not intended to be a formal mathematical correspondence, this relationship is often written as an equation:

Risk = [Threat] * [Vulnerability] * [Attack] * [Impact] [6]

In this context, *threat* refers to the source of an attack or cyber security event, for example a motivated group of hackers, or a type of operator error. *Vulnerability* refers to the grid-specific landscape of systems, infrastructure, and protocols deployed in the field. *Attack* refers to the attack process through which a specific threat is realized upon a vulnerable control network topology. And *impact* refers to the effects that a given event has on the grid system, whether on safety, reliability, or grid integrity.

Increasingly, a range of networked components sit at the interface between cyber and physical systems, opening the grid to new vulnerabilities. Cyber intrusions can focus on a wide range of control systems, typically targeting network components such as programmable logic controllers (PLC), distributed control systems (DCS), supervisory control and data acquisition (SCADA) systems, and human machine interfaces (HMI). Notably, the technical solutions for increasing the security of these components are already in existence, but they are not uniformly implemented.

Internationally, a consensus is emerging that the protection of grid assets is less a matter of technical solutions than of business models and regulation; in other words, 'security economics.[7] In nearly all scenarios, making the business case for substantial cyber security investment is quite difficult, not least because the 'payoff' is typically in the form of avoided costs, which are difficult to incorporate into regulators' net benefits tests. Furthermore, each utility business case is highly sensitive to the regulatory, organizational, and security landscape, since regulatory compliance costs vary widely across technology systems, as do threat and vulnerability surfaces.

More broadly, the following factors may constrain preventative cyber security investment:

- **Estimating costs and benefits.** At the level of specific technology components, securing network devices typically carries a very low per-unit cost, but at large scales the investment can easily cost millions of dollars and require significant changes in business operations. In regulated electricity markets, these costs raise legitimate questions of cost recovery mechanisms for regulatory bodies. And estimating potential losses is difficult, since system impacts can vary dramatically depending on the vulnerability and the threat, and costs of interrupted service are difficult to figure precisely. Furthermore, while some cyber security intrusions can be corrected through straightforward software updates, many other threats require systemic hardware replacement and "always-on" security monitoring, at great cost.

- **Tensions with traditional business processes for least-cost electricity.** Legitimate attempts to minimize consumer costs, for example selecting vendors who offer the lowest bid rather than the most secure system, are often at odds with robust security investments. Replacing these time-tested methods of cost-control will be a difficult cultural shift.

- **Distributed responsibility.** Principal-agent problems abound in grid security economics. With an increasingly complex supply chain of grid controls, and increasing customer 'ownership' of electricity data and devices, responsibility for cyber security preparation is becoming more diffuse. At the same time, the negative impacts of cyber security incidents can be spread across many broad groups of stakeholders, complicating the markets for cyber investment and insurance. And grids are vulnerable to serious externalities of 'correlated failure,' for example when highly interconnected systems suffer cascade failures whose impacts exceed the sum of the individual parts. While a single power producer may protect their thermal generation plant against cyber intrusion to devices

under their control, no single entity ensures an entire region against a network-induced outage.

- **Lack of regulatory 'security economics' expertise.** While most public utility regulators have well-trained staff in place to evaluate utility spending requests on generation and transmission investments, few have similar expertise to evaluate utility investments on cyber security and protection of consumer data privacy. This knowledge gap is narrowing, but efforts to deepen expertise among regulatory staff in this area are critical.

Around the world, the obstacles to accurate cyber security cost assessment methodologies have been noted but not resolved. For example, the 2010 NISTIR 7628 guidelines, one of the leading smart grid security efforts in the world, observes that:

> "There is a need to balance the impact of a security breach and the resources required to implement mitigating security measures […] **the assessment of cost of implementing security is outside the scope of this report. However, this is a critical task for organizations as they develop their cyber security strategy, perform a risk assessment, select security requirements, and assess the effectiveness of those security requirements.**"[8] [emphasis added].

Given the complexity of estimating the true costs of effective security, as well as developing methodologies that allow policy makers to evaluate security plans for appropriateness, this issue deserves concerted international effort.

Case Study: Wide-Area Network Communications
Choosing the most suitable communication platform at both local and wide-area network levels has been a key decision for utilities, vendors and regulators since the development of automated meter reading (AMR) technology in the 1980's. Current options for smart grid communication platforms raise important questions of balancing performance, security and economics:

- One option is to retain currently widespread technologies (radio frequency, power-line communication, and broadband), which have moderate performance and security, and moderately improving bandwidth, latency and Internet Protocol capabilities.
- A second option is to maintain a similar system architecture, but adopt and invest in advanced communication technologies (3G and 4G, GPRS, or WiMax). While providing performance enhancements, the future capabilities and level of service of these platforms is a subject of debate.
- A third option is to provide service and consumer interaction through an existing internet connection. In this model, a meter is essentially replaced with a data server at home that acts as a "virtual meter." This meter may be linked up with a customer's computer as an interface and would provide HAN functionality while sending the metering data back to the utility that needs it.

The cost, security, and long-run viability of each of these platforms are the subject of significant analysis and debate within utility and vendor communities. Policy makers charged with evaluating the cost and security of these options face a difficult task, as do the utilities seeking to unify and integrate platforms and grid components to develop a coherent solution. The choice of a communication platform still remains an open question for all smart grid stakeholders.

Recommendation: *ISGAN should prioritize efforts to advance regulatory and industry best practices in cyber security economics in the smart grid context.*

3.2. Moving from "Compliance Minimum" to "Defense in Depth"

The availability of low-cost network technology has yielded tremendous cost savings to utilities in the process of adding intelligence to their grid operations. But these cost savings have come at a price. The systems and components borrowed from the IT and industrial control system (ICS) markets have increased the vulnerability surfaces of utilities. Specifically, the US Department of Energy notes that utilities are introducing "Transmission Control Protocol/Internet Protocol" (TCP/IP) networking technology in ICS devices, connection of operations systems to back-office and Internet-connected networks,

connection to third-party systems, and the development of home-level and distribution systems automation that crosses the line between traditional operations and "public" networks." Many of these devices were designed for non-critical security environments. While these internet-facing devices may dramatically reduce costs, they also expose control networks to new vectors of sophisticated attack.

Furthermore, some policies can have unintended interactions. For example, some analysts observe a pattern of 'compliance minimum' investment: energy companies only investing the minimum amount necessary to comply with cyber security regulations. Some compliance-based regulatory frameworks have even been observed to have counterproductive effects in the real world. One anecdotal example is the U.S. Critical Infrastructure Protection standards relating to "black start" generators[2]. When increased standards were promulgated for these generators, some utilities simply removed these generators from their portfolio of operating assets in order to avoid costs associated with protecting these assets from cyber attack.[9] This response degraded the dependability of the grid instead of achieving the intended goal of greater security. Policymakers face the difficult challenge of creating regulatory environments in which security takes hold at deeper levels of energy companies, as opposed to simple compliance-based investments. Somewhat instructively, the UK has taken a different approach to regulation, leaving industry to manage the proper path for cyber security assessment and protection. And in Europe, a range of regulatory approaches are being tested.[10]

Even when left to their own devices, energy companies will also face challenges in effecting the organizational changes necessary to achieve robust cyber security. Key issues in this area include:

- Managing the entire supply chain of networked components to ensure integrity, involving contractual obligations with third-party actors
- Designing grid control architectures that allow secure integration of new control components into existing SCADA systems
- Establishing formal Change Management protocols to consistently guide the integration of new components.[11]
- Minimizing the number of users with administrative privileges [12]
- Establishing business continuity management protocols to ensure maximum electricity availability during cyber security events.

Regardless of the regulatory posture toward strict compliance-based policies, moving away from minimum investments will be complicated by the structure of the electricity delivery business. In contestable markets, this business comprises a complex network of utilities, vendors, third-party generators, consumers, third-party energy management firms, and regulators. While innovation can proceed more rapidly in this environment, clear responsibility for overall cyber security situation can be fragmented. Under such constraints, it is often quite rational for individual firms to seek to minimize their own responsibility and investment.

Alternative frameworks have been articulated that envision more holistic approaches to grid security. For example, at the Cigrè Information Systems and Telecommunication Colloquium in 2009 a Risk Management Framework for Electric Power Utilities was proposed[13] particularly to facilitate the incorporation of well-established information/ICT security risk assessment for operational ICT systems into the electric power enterprise risk management process. Of critical importance in this framework is the recognition of both potential ICT

[2] Black start generators can initiate operation without relying on the external electric power transmission network, for example hydro power plants and thermal plants with auxiliary diesel generators.

consequences and power consequences of cyber security risks. The framework proposes a method for assessing these risks and reporting on them against Risk Acceptance Criteria set at appropriate levels within electric power utilities. This provides an approach which permits the appropriate integration of these risks into an enterprise wide Risk Management process. Additionally, the U.S. National Science Foundation has articulated a framework of "Defense in Depth" for the IT sector that includes "methods to increase attacker cost, enable tailored security environments, and incentivize security deployment, socially responsible behavior, and deterrence of cyber crimes."[14] In line with the Cigrè approach, the U.S. Department of Energy has articulated a framework[15] for deep cyber security that will enable energy firms to:

- "Effectively and efficiently implement a risk management process (RMP) across the whole organization;
- Establish the organizational tolerance for risk and communicate throughout the organization including guidance on how risk tolerance impacts ongoing decision making;
- Prioritize and allocate resources for managing cybersecurity risk;
- Create an organizational climate in which cybersecurity risk is considered within the context of the mission and business objectives of the organization; and
- Improve the understanding of cybersecurity risk and how these risks potentially impact the mission and business success of the organization."

The steps necessary to achieve these deep security environments should continue to be a topic of international collaboration.

> ***Recommendation:*** *ISGAN should establish a forum to share best practices in cultivating organizational change and cost-effective technical innovations in support of cyber security in the smart grid context.*

4. Frameworks for Protecting Consumer Data Privacy

These two challenges described above – the economics of grid cyber security and the organizational changes required to achieve robust security -- are also relevant to the protection of consumer data privacy. Analysts from the United Kingdom raise several distinct policy and security concerns with regards to metering: [16]

1) The sheer amount of data may raise privacy concerns, which have already been cited in a court decision in the Netherlands which overturned a smart meter law there on the grounds that it runs contrary to the principles of the European Convention on Human Rights.
2) The availability of fine-grained consumption data to utilities raises questions around selective or predatory pricing and the potential for increased lock-in of customers.
3) The existence of widely distributed remote disconnect switches for electricity and/or gas increases vulnerability to malicious blackouts, whether due to nation state attack, terrorist attack, or criminal groups.
4) The existence of widely distributed remote disconnect switches also raises concerns about governments using targeted power cuts as a coercive measure to meet energy savings targets or pursue other policy objectives, such as punishing dissent.
5) The selection of data and device protocols has strong but complex implications for cost and the intellectual property landscape. For example, mandating certain specific encryption protocols, such as elliptic curve cryptography, would incur royalty costs for every appliance capable of communicating with an electricity meter.

While the relative merits of each of these concerns is debatable, they nonetheless underscore the complex interactions of policies enacted in the realm of consumer data

privacy. This should reinforce the important steps that utilities and policymakers must take to craft careful policies that balance innovation and privacy, preserve data integrity, and resolve potential conflicts-of-interest in the preservation of consumer rights. While innovation in the electric sector is vital and proceeding faster now than in recent memory, frameworks should be established early in order to ensure trust in smart grid systems, allowing the full exploitation of demand flexibility, electric vehicle charging infrastructure, and other customer applications. Fortunately, progress is being made in these domains, and the next section describes two emerging frameworks for consumer data privacy protection.

4.1. Fair Information Practices

Globally, policymakers are beginning to build upon existing frameworks to articulate policy frameworks tailored for smart meter privacy issues. Policy coordination in this area seeks to balance the need to promote deployment and business-model innovation while mitigating threats to consumer privacy.

In one key example from July of 2011, after soliciting the input of dozens of industry and NGO stakeholders, the California Public Utilities Commission (CPUC) adopted "Fair Information Practice" (FIP) principles to guide implementation of smart meter data management. FIP principles "are a set of internationally recognized practices for addressing the privacy of information about individuals. Information privacy is a subset of privacy. Fair Information Practices are important because they provide the underlying policy for many national laws addressing privacy and data protection matters." [17]

The CPUC decision relies upon seven key concepts of the FIP framework, drawing heavily upon principles articulated by the OECD in 1980. [18][19][20][21]

1. **Transparency**

   There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

2. **Purpose Specification**

   The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

3. **Data Minimization**

   There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

4. **Use Limitation**

   Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law.

5. **Data Quality and Integrity**

   Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

6. **Security**

   Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

7. **Accountability and Auditing**

   A data controller should be accountable for complying with measures, which give effect to the principles stated above.

The guiding philosophy of these principles is fairly straightforward:

- "The customer gets his or her own data and can decide what he or she wants to do with it"; and,
- Others get access to "scrubbed" data (aka data that has no specific customer information) for their use in developing products to sell to the public."[22]

In the United States, a new initiative called "The Green Button" seeks to embody many of the FIP principles while still promoting innovation in energy data usage. [23] In other countries too, variations on this framework are emerging. For example, the Korean Ministry of Public Administration and Security directs policy development for smart grid data protection. One such policy from 2011 requires protection of personal information in commercial use, limiting the processing and usage of personal information to specific cases, and requiring companies to protect consumer data. This act only covers personally identifiable information, however, and does not restrict the use of other information that may be collected from a smart meter. In some countries, such as Mexico, only limited customer-related information currently travels through cyberspace, mainly because of the relatively limited deployment of smart meters to date. As the pace of smart meter deployment accelerates in these countries, data and device protocols will need to be introduced or strengthened to ensure the desired confidentiality of data.

4.2. Privacy as a Human Right

Prior to California's adoption of FIP principles to guide consumer data privacy protection, Dutch courts in April 2009 declined to approve a smart metering bill that would mandate all Dutch citizens to have smart meters installed in their home. Appealing to Section 8 of the European Convention on Human Rights, the court objected to the mandatory nature of smart metering as an unacceptable infringement of citizens' privacy and security, following opposition by the Dutch consumers' association to central collection of energy data. In November of 2010, the Netherlands enacted policies requiring that smart meters have an option for "administrative off" as well as a port for decentralized metering services (i.e. real-time feedback with data remaining in the house).[24]

The appeal to the EU Convention on Human Rights constitutes a strong policy preference in support of precaution when it involves customer energy data. Similar rulings in other jurisdictions could potentially limit the system-wide impacts of AMI deployments, given that it limits the business case for customization of electricity products and aggregation of consumer usage as a demand response resource.

Establishing an appropriate balance of consumer privacy and electric grid innovation remains a critical issue worthy of international policy consideration, and should be a focus of ISGAN collaboration.

> ***Recommendation:*** *ISGAN should establish a forum to share best practices in policy development in the area of customer data privacy in the smart grid context.*

5. Conclusion

While progress is underway, significant policy gaps remain in the field of grid cyber security, and ISGAN is well-positioned to convene stakeholders and foster discussion to advance best practices in this area. Balancing cost and security is a critical difficulty, and further research in this area should be considered essential to a sustainable development of smart grids. Balancing system innovation and consumer data privacy is also a key challenge worthy of targeted focus and dialogue.

The landscape of cyber security is changing rapidly: the deployment of millions of networked components is spurring potential for technological innovation, and at the same time is rapidly increasing the vulnerability landscape. Maximizing system evolution and innovation while minimizing risk should be the goal of policy makers, but this will entail costs and trade-offs. The range of policy solutions in development across the ISGAN membership is a rich resource that should be developed, organized, and shared for public benefit.

References

[1] Govindarasu, M., Hann, A., Sauer, P. (2012). "Cyber-Physical Systems Security for Smart Grid." Prepared with funding from the US Department of Energy. PSERC Publication 12-02. February 2012.

[2] EC (2011) Smart Grid Mandate M/490 EN.

[3] Lockhart, B., & Gohn, B. (2011a). Utility Cyber Security: Seven Key Smart Grid Security Trends to Watch in 2012 and Beyond. Boulder: Pike Research.

[4] Stanford, J. (2012). Cybersecurity: Time for utilities to step it up, Part 1. (A. Poszywak, Interviewer). January 3, 2012. http://www.snl.com/InteractiveX/article.aspx?ID=13906555 Accessed January 21, 2012.

[5] DOE (2006). "Roadmap to Secure Control Systems in the Energy Sector." http://www.cyber.st.dhs.gov/docs/DOE%20Roadmap%202006.pdf Accessed January 18, 2012.

[6] Dondossola, G., Garrone, F., Szanto, J. (2011). Cyber Risk Assessment of Power Control Systems - A Metrics weighted by Attack Experiments. IEEE Power & Energy Society General Meeting, Detroit, Michigan, USA, 24-29 July 2011.

[7] Anderson, R., & Fuloria, S. (2010a). Security Economics and Critical National Infrastructure. In T. M. (eds.), Economics of Information Security and Privacy (pp. 55-66). Springer Science + Business Media.

[8] NIST (2010). NISTIR 7628: Guidelines for Smart Grid Cyber Security, Vol. 1. Washington, DC: U.S. National Institute of Standards and Technology.

[9] Anderson, R., & Fuloria, S. (2010b). On the security economics of electricity metering. Workshop on the Economics of Information Security 2010. Cambridge, MA.

[10] Anderson, R., & Fuloria, S. (2010a).

[11] Lockhart, B. (2011b). "Defense Security and Utilities." August 11, 2011. Retrieved January 21, 2012, from www.pikeresearch.com: http://www.pikeresearch.com/blog/articles/defense-security-and-utilities

[12] Australia DoD Cyber Security Operations Centre. (2011). "Strategies to Mitigate Targeted Cyber Intrusions." Canberra: Australia.

[13] Tritschler, M., Dondossola, G. (2009). Information Security Risk Assessment of Operational IT Systems

at Electric Power Utilities, Paper D2-01 D03, Cigré D2 Colloquium, October 21-22, 2009, Fukuoka, Japan.

[14] Landwehr, C. (2011). NSF Trustworthy Computing Program and Economic Incentives. Tenth Workshop on Economics of Information Security (WEIS 2011). Fairfax, VA: WEIS.

[15] DOE (2011). "Electricity Sector Cybersecurity Risk Management Process Guideline." September 2011. Draft for Public Comment.

[16] Anderson, R., & Fuloria, S. (2010b).

[17] Gellman, R. (2011). Fair Information Practices: A Basic History. Robert Gellman, October 3, 2011. www.bobgellman.com/rg-docs/rg-FIPShistory.pdf Accessed January 29, 2012.

[18] Gellman, R. (2011).

[19] CPUC Privacy Decision, 11-07-056 (California Public Utilities Decision July 28, 2011).

[20] OECD (1980). "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html Accessed February 8, 2012.

[21] Future of Privacy Forum (2011). "Future of Privacy Summary of California Public Utilities Commission Proposed Decision on Smart Grid Privacy and Security." May 9, 2011. http://www.futureofprivacy.org/wp-content/uploads/2011/05/cpuc_summary.pdf Accessed February 8, 2012.

[22] Prabhakaran, V. (2011, May 17). CPUC Smart Grid Decision Aims to Protect Customer Privacy. Retrieved January 25, 2012, from California Energy Law Blog: http://www.caenergylaw.com/2011/05/cpuc-smart-grid-decision-aims-to-protect-customer-privacy/

[23] Whitehouse.gov (2012). "Green Button: Providing Consumers with Access to Their Energy Data." January 18, 2012. http://www.whitehouse.gov/blog/2012/01/18/green-button-providing-consumers-access-their-energy-data Accessed February 9, 2012.

[24] Renner, S., Albu, M., van Elburg, H., Heinemann, C., Lazicki, A., Pentinnen, L., et al. (2011). European Smart Metering Landscape Report. Vienna: Intelligent Energy Europe.