Section Two: Long-term Evolution of the U.S. Smart Grid Effort

Introduction

The challenge for the SGFAC Subcommittee Three, which focused its efforts on long-term gaps, was to define the governance structures and working relationship between the U.S. Department of Energy (DOE), the National Institute of Standards and Technology (NIST), and the Smart Grid Interoperability Panel (SGIP) relative to their roles in Smart Grid and the vision of the grid in 2015 and beyond. With this in mind, the critical concepts identified by the working group on their December 10, 2010 conference call included:

1. The long-term planning range for the purpose of this working group is five years and beyond.

2. It is necessary to consider how the current structures in both the government and industry will evolve.
    a. What is the NIST role in this structure and how might NIST need to organize for its evolving role by 2015 and beyond?
    b. What is the industry role in this structure?
    c. How do other government agencies fit?

3. How can the process of identifying standards and their supporting technologies transition from the current government-funded, industry-led NIST/SGIP initiative to being solely an industry function with government input?

4. What does a mature SGIP program look like as a component of the long-term vision?

In order to organize this discussion, the working group needed to create a common vision of the future of Smart Grid in the United States. For readers who are interested, these assumptions can be found in Appendices A and B of Section Three.

Because the Energy Independence and Security Act of 2007 is public law (PL 110-140, EISA 2007), the various federal agencies named in the Act necessarily retain their responsibilities for Smart Grid. A map of these responsibilities is included in Figure 2. Within DOE, the EISA designated the Office of Electricity (DOE-OE) as the lead agency. To support this role, in 2009 OE identified Eric Lightner and Chris Irwin as the leads for Smart Grid. In the absence of any specific lead designation at FERC, they've identified the Office of Energy Policy and Innovation under Deputy Director Jamie Simler as the lead agent for Smart Grid.

Note: The content of this report is premised on industry interviews that were conducted prior to September 2011 and do not reflect discussions, initiatives, activities, or developments that are subsequently taking place within the SGIP or other stakeholder forums.

To support NIST's responsibilities, in 2009 Dr. George Arnold was identified to be the National Coordinator for Smart Grid Interoperability. Under the current operating structure, Dr. Arnold leads a team of 20 to 30 individuals who support his office and the program:

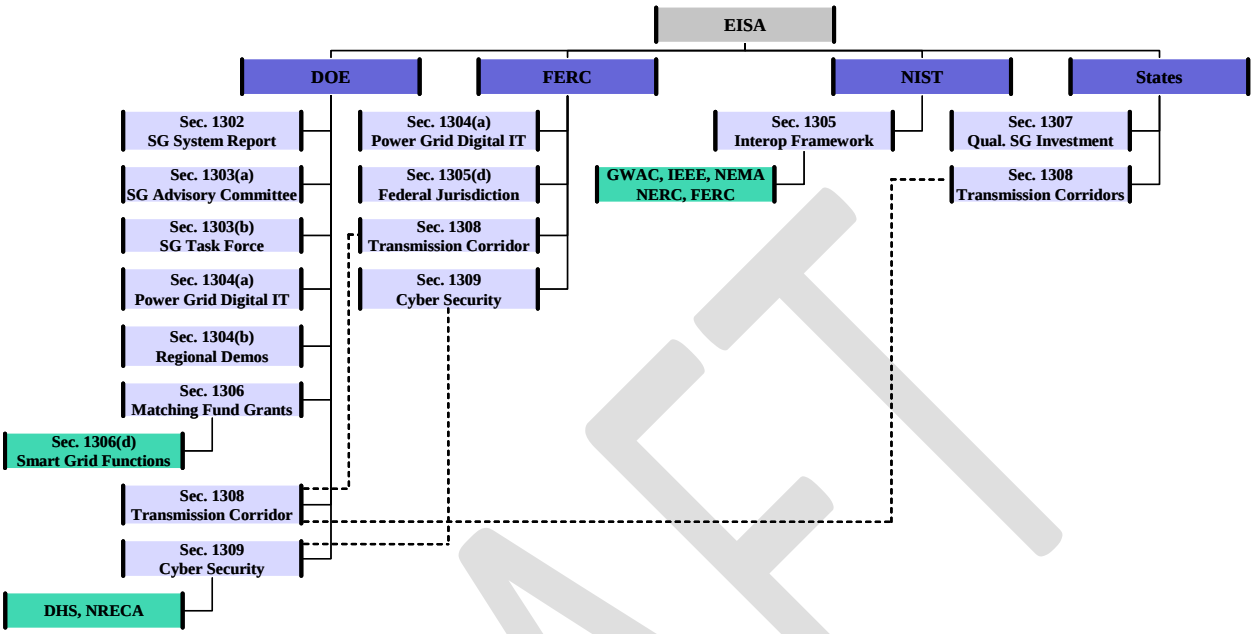
- *Office of the Director (NIST Headquarters)*
  - Dean Prochaska (100%)
  - Cuong Nguyen (100%)
  - International Coordinator (vacant)
  - Admin Assistant (100%)
  - Several part-time resources from NIST locations around the country
  - Additional Ad Hoc Support
    - Public and Business Affairs Office
    - Congressional & Legislative Affairs Office
    - Contracts Management

- *Physical Measurement Lab*
  - Jerry Fitzpatrick (100%)
  - Paul Boynton (100%)
  - David Wollman (approx. 80%)
  - Four additional part-time resources

- *Information Technologies*
  - Several part-time resources

- *Engineering Laboratory*
  - David Holmberg (100%)
  - Keith Stouffer (approx. 75%)

Figure 2. Map of Responsibilities under EISA



NIST-2015

It is widely agreed by the working group that in terms of an organizational structure, a "no change" scenario will not be sustainable by NIST in the years 2015 and beyond. To support an evolving mission as the NIST role in Smart Grid changes, the organization will need to develop some bench strength with greater detailed expertise in terms of both the technological and administrative functions necessary to support Smart Grid. It's therefore necessary to decompose the functions and activities that NIST will be expected to support in 2015 in order to identify the constituent elements that are required by its staff.

Functions & Activities

As stated above, NIST has responsibilities under EISA that it must support Smart Grid. A few of the specific mentions of NIST in EISA include:

- Contribute to the Dept. of Energy Smart Grid Systems Report (EISA §1302)
- Possibly support the Smart Grid Federal Advisory Committee (EISA §1303(a))
- Provide a staff representative to the Smart Grid Task Force (EISA §1303(b))
- Maintain the Interoperability Framework (EISA §1305)

Note: The content of this report is premised on industry interviews that were conducted prior to September 2011 and do not reflect discussions, initiatives, activities, or developments that are subsequently taking place within the SGIP or other stakeholder forums.

- Support/advise/counsel FERC on rulemaking for Smart Grid Standards for Interoperability in Federal Jurisdiction (EISA §1305(d))

Additional functions as envisioned by Working Group Three that are either implied by EISA or the NIST mission statement include:

- Provide advice and counsel on Smart Grid to:
  - U.S. Congress
  - Other Federal Agencies
  - State Energy Authorities and Utility Commissions

- Provide input to other Federal Agencies on cybersecurity issues
  - Develop a cybersecurity response plan

- Interface with state utility and public service commissions

- Analyze international Smart Grid policies, activities, and technical efforts

- Opine on standards relative to National Technology Transfer and Advancement Act (NTTAA), and the Office of Management and Budget (OMB) Circular A-119

- Development of test methodologies to measure smart grid performance
  - Ensure consistency across the applications of the SGIP Testing and Certification Committee's Interoperability Process Reference Manual (IPRM)
  - Provide guidance and review of certification bodies in accordance with the National Voluntary Laboratory Accreditation Program (NAVLAP)

- Coordinate with other Federal Agencies on Cybersecurity

- Provide laboratory service and guidance on electromagnetic compatibility and interference issues

- Provide Input to DOE Smart Grid Clearinghouse

A major discussion item that was part of the FERC Technical Conference on January 31, 2011 was over the nature of what it means for a Smart Grid standard to be "adopted" by FERC. However, the disconnect between NIST, FERC, and the Conference panelists highlights an operational need relative to NIST's role in the regulatory process. The form of the NIST suggestion for the five families of standards that were discussed at the conference was merely a letter naming the standards with a brief description of their purpose in the Smart Grid. It seems obvious in the aftermath that some additional context needs to be supplied with any future recommendation.

Note: The content of this report is premised on industry interviews that were conducted prior to September 2011 and do not reflect discussions, initiatives, activities, or developments that are subsequently taking place within the SGIP or other stakeholder forums.

The regulatory process is not binary, which is to say that it's not about the mere presence of a standard (as suggested by the form of the NIST letter to FERC) in a regulation, but much more about the appropriate time, place, and method of employment for that standard. There is no doubt that in the future, these notions need to be part of any recommendation to FERC. To manage this responsibility, the NIST organizational structure needs to be prepared to support the process of developing more detailed descriptions.

Regarding the National Technology Transfer and Advancement Act (NTTAA) as encoded by the Office of Management and Budget (OMB Circular A-119), Federal Agencies are directed to use consensus standards, developed by consensus standards bodies, and to encourage participation in voluntary consensus standards bodies when compatible with agency missions, authorities, etc. The Act further directs NIST to coordinate Federal standards and conformity assessment activities with those of the private sector.

On a related note, FERC citations following the release of their Smart Grid Policy Statement in June of 2009 note the responsibility they have relative to advancing regulations that are compatible with the NTTAA. Therefore, it appears that by extension, NIST will be obligated to support the FERC (and also likely the Dept. of Energy and Nuclear Regulatory Commission) if they desire to implement any Smart Grid standards in regulation. This is not only important to note in terms of NIST staffing, but there are also a variety of legal implications that will come into play.

In a similar vein, the implications associated with Section 1309 of EISA, *Cybersecurity*, fall jointly on the Dept. of Energy and FERC. In response to the cybersecurity challenge that Smart Grid faces, NIST formed the Cybersecurity Coordinating Task Group, or CSCTG, at about the same time they were establishing the SGIP. Eventually this group was reorganized as the Cybersecurity Working Group (CSWG) under the SGIP with the following goals:

> *The primary goal is to develop an overall cybersecurity strategy for the Smart Grid that includes a risk mitigation strategy to ensure interoperability of solutions across different domains/components of the infrastructure. The cybersecurity strategy needs to address prevention, detection, response, and recovery. Implementation of a cybersecurity strategy requires the definition and implementation of an overall cybersecurity risk assessment process for the Smart Grid.*

The unique thing about the CSWG, and the CSCTG before it under the SGIP, is that it is headed by a full-time member of the NIST staff. With the lofty expectations for the smart grid and the volumes of communications protocols and technologies that are going to be required to achieve them, it is likely that cybersecurity will play a major role in NIST for years to come.
A complaint about the CSWG that has been highlighted by a number of sources including the panelists at the FERC January 31, 2011 Technical Conference, is that NIST Special Publication

Note: The content of this report is premised on industry interviews that were conducted prior to September 2011 and do not reflect discussions, initiatives, activities, or developments that are subsequently taking place within the SGIP or other stakeholder forums.

7628, *Guidelines for Smart Grid Cyber Security*, is much more of a philosophical document than a handbook for achieving a secure operating environment. The challenge is to parse each of the three volumes in SP 7628 in order to create a set of actionable recommendations to implement cybersecurity on a consistent basis. This needs to apply for like-products from different vendors as well as across the various utility company operations. As one FERC panelist stated, the security problem is not intractable, and we must strive to develop "an overriding security addendum that must be adopted along with the standards."

However, it's one thing to go through the rigor of identifying the piece-parts that formulate a cybersecurity strategy for the grid, but something altogether different to establish the appropriate response protocol in the event of a cyber emergency. To date, this working group is unaware of any agency within the Federal government (with the possible exception of some compartmentalized functions within the Department of Homeland Security) that is addressing the possible responses to a national cyber emergency. The expectation is that NIST should collaborate with DHS to define the Federal response to national cyber emergencies.

Conclusion and Recommendations

The challenges as the Smart Grid evolves over the next five-to-ten years mandate a change in both the form and structure of the NIST Smart Grid business unit and the SGIP. A lot of human capital will need to exist if NIST is to adequately support the regulatory process in light of both the kinds and volume of information necessary for the seamless adoption of a technical standard in regulation. This includes specific use cases that describe the time, place, and method of employment for the standard in regulation, the implications based on the NTTAA, and any associated cybersecurity concerns. NIST must also be prepared to support state and federal regulators after adoption as challenges are issued through both the legal or regulatory processes. NIST must also consider a staffing plan to support the responsibilities as described under "Staffing" below.

Also, if NIST is going to be one of the key players in Smart Grid, it needs to develop a response capability in the event of an electric grid disaster—whether physical or cyber. This needs to be done in collaboration with other federal agencies, and should follow the model of the *National Diversity Assurance Initiative (NDAI)* as developed by the Federal Reserve Board. According to their website, the NDAI:

> *"...resulted from concerns that a widespread disruption of the telecommunications infrastructure that was not quickly recovered would bring the nation's wholesale financial system to a halt. The susceptibility of the telecommunications infrastructure to disruption was underscored by the September 11 attacks. The Federal Reserve, in conjunction with other federal and private sector entities, has worked to identify business continuity*

Note: The content of this report is premised on industry interviews that were conducted prior to September 2011 and do not reflect discussions, initiatives, activities, or developments that are subsequently taking place within the SGIP or other stakeholder forums.

objectives and sound practices aimed at strengthening the resilience of the U.S. financial system."

This plan should form a template for emergency response for both the physical/electrical and command and control functions: how to find, isolate, and remediate the breech; how to manage command and control between utility providers; how to coordinate with other federal agencies including DHS, FEMA, FCC, DOD, and DOE; how to collaborate with state, local, and municipal authorities during the remediation process; and how to marshal industry resources to supply patches for the vulnerabilities and prevent similar occurrences in the future.

This plan should include conducting a demonstration program, possibly aligned with the military Base Realignment and Closing (BRAC) strategy. The focus for this demonstration should be on reliability and stability, not the consumer, and it should include features like microgrid(s), renewables, storage, and distributed generation.

A similar evolution needs to take place in the SGIP. To begin, in order to sustain its existence, the SGIP will need to become a registered entity, separate and distinct from NIST. This would require the development of some form of business plan. It is understood by this working group that the contract for the current SGIP administrator required some form of recommendation to perpetuate the SGIP in the absence of government funding. It will be very worthwhile for the NIST SGFAC to review this report.

Also, to relieve the tensions that currently exist, the SGIP needs to get greater involvement from utility companies and revamp its voting procedures to ensure consensus. While unanimity is not currently required, some shared form of consensus should exist across the stakeholder categories. As it currently exists, 100% of the utility companies could vote against some issue in the SGIP, but it could still carry the day because of the current majority voting procedures. Unanimous consent against an issue in a designated voting bloc, should serve as a trigger and cause the SGIP Leadership to re-evaluate its merit and/or modify the approach.

The SGIP should push to ensure that regulations are in place so that costs incurred by utility companies to support the SGIP are recoverable at both the federal and state levels.

Staffing

Given the functions and responsibilities as described above for NIST, the following staff functions would seem to be necessary in 2015 and beyond:

- National Coordinator for Smart Grid
    - Also staffs the SG Task Force in EISA §1303(b)

- Coordinator(s) for Regulatory Affairs
    - Federal
    - State

Note: The content of this report is premised on industry interviews that were conducted prior to September 2011 and do not reflect discussions, initiatives, activities, or developments that are subsequently taking place within the SGIP or other stakeholder forums.

- Required Technical Expertise
    - Generation
    - T&D
    - Consumer Technologies (Commercial, Industrial, Residential)
    - Cybersecurity
    - Privacy
    - Metering
    - Communications

- Legal Counsel
- Interagency liaisons with DHS, DOE, FCC, DOD, FEMA, etc.
- International
    - Collaboration with peer organizations in foreign counties, both public and private

Again, this would seem to meet the agency's needs in terms of the three primary functions they will continue to face: identification and implementation of appropriate technical standards; support for federal and state policymakers; and support for federal and state regulators.

Note: The content of this report is premised on industry interviews that were conducted prior to September 2011 and do not reflect discussions, initiatives, activities, or developments that are subsequently taking place within the SGIP or other stakeholder forums.