NIST SGAC Federal Advisory Committee Homework

Working Group 3 – Long-Range Evolution of the U.S. Smart Grid Effort

1 Introduction

The challenge for Working Group 3 is to define the governance structures and working relationship between 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 working group on their 10 December 2010 conference call include:

1. The long-term planning range for the purpose of this working group is 5-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?
    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 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?

Because the Energy Independence and Security Act of 2007 is public law (PL 110-140, commonly known as either EISA 2007 or simply EISA), the various federal agencies named in the Act necessarily retain their responsibilities for Smart Grid. A map of these responsibilities is included in Figure 1. Within the U.S. Department of Energy, 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.

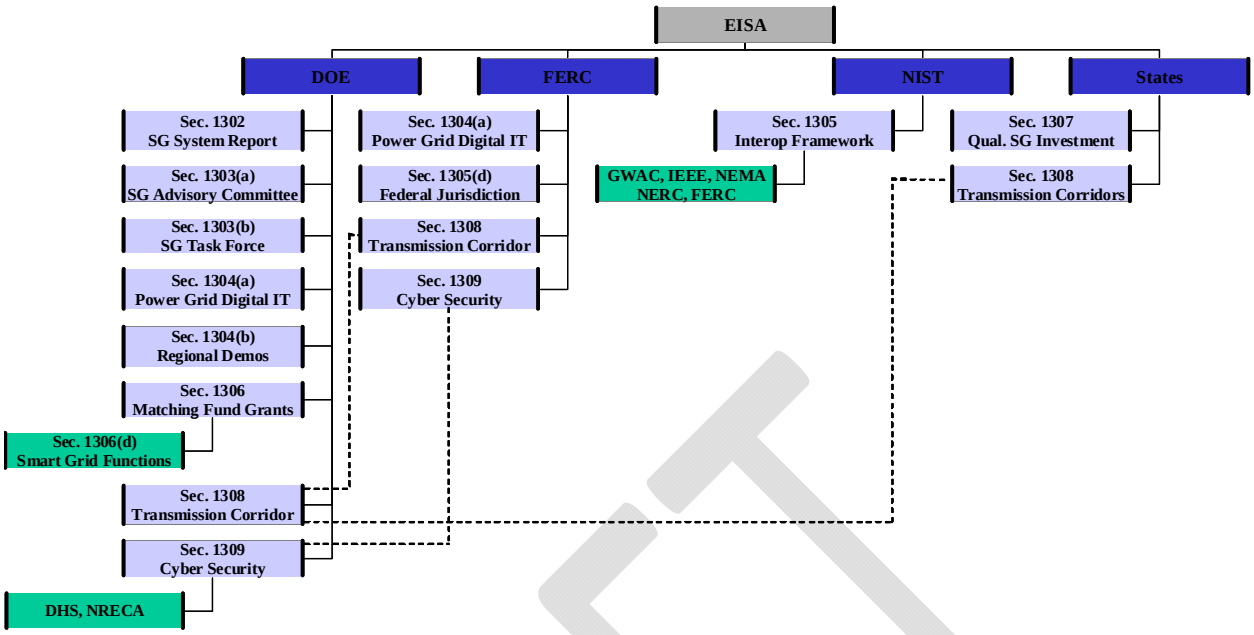

Figure 1. Map of Responsibilities under EISA

To support NIST's responsibilities, in 2009 they identified Dr. George Arnold to be the National Coordinator for Smart Grid. Under their 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%)
  - plus several part time 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%)
  - plus 4 additional part time
- Information Technologies
  - Several part time resources
- Engineering Laboratory
  - David Holmberg (100%)
  - Keith Stouffer (approx. 75%)

1.1 Smart Grid 2015 – A Baseline Narrative

By 2015, it's expected that the pilots and demonstrations that were initiated and funded as part of the American Recovery and Reinvestment Act of 2009 (ARRA, or The

Stimulus Bill) will be complete. As the fifth year of the national smart grid effort begins, a significant amount of deployment based on the results of those demonstrations will have taken place. As a result, electrical grid operators will have a substantial deployment of smart gear, largely centered on those applications that will most directly benefit the utility company. That is to say that items that don't necessarily have a consumer component, such as substation automation, outage management, and supervisory control systems will progress more rapidly and consistently than the technologies on the consumer side of the meter. .

Suburban areas will contain significantly more Smart Grid technology than either rural or urban areas because they will have been "built smart" as population growth causes the number of residents in the suburbs to continue to expand. Deployment of smart technologies was more necessary in suburbia to support the electrical vehicle market. In the period between 2010 and 2015, EVs tended to thrive in the suburbs because the residents not only have the disposable income to purchase the vehicles, but their lifestyle is also able to accommodate the vehicles' limitations in terms of range-between-charge requirements.

In 2015 deployment of Smart Grid technology lags in the urban areas because much of the existing legacy gear still has usable life and has not been fully depreciated. At the same time, rural areas and electric cooperatives offer a mixed bag of Smart Grid capabilities. Some of these utilities lag because there is little new construction and the revenue base simply isn't there to fund the wholesale replacement of their existing operational gear. Other co-ops have a much more advanced implementation because they realized early-on that Smart Grid was critical to their business case in terms of sustaining their operations.

In 2015 we expect the Smart Grid landscape to be fairly well developed in terms of standards, somewhere in the 80% complete range. It's impossible to know how many standards it will take, but by saying the task is 80% complete you would expect that the list will only grow by another 25%. By this time the conceptual architectures (and corresponding standards) for Smart Grid will be fairly well baked and accepted by a consensus of the electrical supply chain. The majority of the standards work beyond 2015 will center on the home market and corresponding grid-side ancillary services in order to support higher functionality inside the home. International standardization is also fairly stable as the important issues relative to Smart Grid operations are harmonized between the Americas, Europe, and Asia.

The legislative front is similarly quiet in 2015. As cited earlier, most of the major federal legislative initiatives for Smart Grid will have been completed, funded, etc. However, there may be some loose ends that need to be cleaned up as part of the ongoing energy policy process, but there are no major Smart Grid standalone initiatives (think EPA-2005, EISA, or ARRA) on the horizon. Of all of the issues being addressed, security and privacy continue to be relatively thorny, which is where the majority of the legislative effort will be focused.

In contrast, the regulatory environment of 2015 is likely to remain somewhat unsettled. Policy conflicts between federal and state authorities continue to bristle and be challenged in terms of the separation of authority. Lingering effects from regulatory activities related to energy efficiency, emission standards, renewable portfolio standards (RPS), and carbon production and offsets earlier in the decade will continue to produce concerns for the industry. A variety of lawsuits are initiated as state utility commissions try to wrest control from the fed.

1.2 Market Drivers

When you consider the adoption of Smart Grid, the overall assumption is that the United States and the other developed nations of the world are on the path to making it a reality. Therefore the role of the market drivers in this scenario will either be to accelerate or inhibit the arrival of individual components associated with Smart Grid. This paper makes no assumption about the status of these drivers, other than to comment on their possible impact for the deployment of smart technologies.

The impact of the global economy will continue to be a significant driver for Smart Grid deployment in 2015. Whereas the seeds for deployment of the technologies in the United States were sewn as a result of the $4.5 billion (US$) Smart Grid Investment Grant program in the American Reinvestment and Recovery Act, the speed of propagation in 2015 and beyond will benefit from a robust U.S. and global economy. Because every aspect of Smart Grid comes with a price tag, utilities will rely on PUC approval of rate cases in order to deploy smart equipment. Changes in utility rates are obviously more palatable under favorable economic conditions. Similarly, intelligent endpoint applications for Smart Grid (demand response, energy efficiency, renewables, storage, etc.) require an investment by the commercial, industrial, and residential consumer. These too are made more willingly during periods of prosperity.

Security and Privacy have the potential to become a major pacing item for Smart Grid, and the current state of these issues in 2015 will be a factor. As Smart Grid deployments progressed between 2010 and 2015, electric power providers across the globe will have established some history in the effectiveness of their cybersecurity measures. The key question will center on whether any aspects of the geopolitical climate have affected grid operations, and whether any nation launched a successful cyber attack on another country's electric grid. A close second to this is the hacker issue within the U.S. borders. As with the Internet and the financial services industries, hackers, some looking for financial gains and others seeking fame based on their computer skills, will continue to probe the vulnerabilities of digitally-controlled grid systems. Any headlines citing an interruption of services related to hacker activity will make regulators nervous and send legislators scrambling to the microphones, touting their latest plan to improve security of the grid. Such an event would have a detrimental affect on the rate of deployment.

The characteristics of the concerns over privacy will be somewhat different. There is no argument that the customer's identity must be protected. And, as expressed by the group "Privacy By Design," privacy must be the default – which is to say that if the customer takes no action, their data is protected. The real battle, however, is over the ownership of

that data. If it's determined that it is utility company data, they are already talking about ways to "monetize" its value. Possible applications of monetized data means that a utility company could possibly place targeted advertising inserts in the customer's bill, permit service providers to send advertisements to the customer's home energy management system, or the utility could let third-party providers market energy savings or specialized rate plans to those customers. In contrast, customer-owned data means that these kinds of programs would become the exception rather than the rule – their data could not be used for these purposes unless the customer signs up for some kind of marketing service.

Related to the state of the global and U.S. economies, the cost effectiveness of Smart Grid solutions will continue to have an impact on the rate of adoption. Quite frankly, if consumers don't see the value, either in terms of the solutions available for their home or in terms of the rates they are paying for electricity, they will resist the expansion of Smart Grid services. To date the state of California has been a case study in terms of the variety and depth of the opposition to Smart Grid, where accusations of faulty meters, environmental impact of transmission lines, and now health concerns over wireless technologies have all represented obstacles to the progress of Smart Grid deployments.

Adoption rates for electric vehicles, including the accommodations that retailers make for charging them will be an indicator of consumer acceptance. As will the variety of Smart Grid solutions that are available via retail outlets such as Lowes, Home Depot, Wal-Mart, Sears, and Dollar General. Other indicators include the variety of Smart Grid programs that are available from utility companies such as demand response, dynamic pricing, and energy efficiency, as is the willingness of the financial industry to provide capital for Smart Grid projects.

Whereas the progress on the utility side of the meter may be seen as a series of fairly steady gains in operational efficiency, there is bound to be a high level of variability on the customer side of the meter, particularly in the residential market. Homeowners that embrace technology, and are comfortable with it will represent an entirely different picture than those of the disadvantaged and elderly, meaning that the continuum of consumer acceptance will be somewhat broad. Just as the VHS versus Beta and HD DVD versus Blu-Ray market forces took two to three years to declare a winner, so too will the competing interests for the providers of home energy management systems or HEMS. By the year 2015, it's likely that the consumer technology preferences will finally be sorted out.

As stated earlier in the cybersecurity example, the regulatory environment will continue to have an impact on Smart Grid deployments. Beyond security, feed-in and net-metering tariffs will affect the rates of adoption for consumer-owned renewables and have a major impact on the classification of other distributed energy resources. Issues surrounding transmission corridors – siting, cost allocation, and the notions of federal pre-emption and/or backstop authority. Questions over the enforcement of cybersecurity requirements between federal and state authorities will be played out in the regulatory arena.

One of the lessons learned about the impact of the cost for a barrel of crude oil that played out between 2006 and 2010 is that the price for a gallon of gasoline has a major impact on the public's appetite for Smart Grid components such as electric vehicles. Similar instability in the cost of doing business for coal, natural gas, and nuclear generated power will also impact the desire for other Smart Grid features such as demand response, distributed generation, and renewables.

Also, changes in consumer economics could also fuel an appetite for Smart Grid services independent of what the utility companies are doing. Just as the utility companies will pursue the applications that are in their best interests, so too will the consumer. It's very likely that under this scenario, technology vendors will respond by delivering services whose benefits are not contingent on a corresponding change or deployment by the utility company.

Beyond the regulatory issues associated with the normal channels in the electrical supply chain, new complications brought about by regulations implemented by federal agencies such as the Environmental Protection Agency will have an impact on the popularity of Smart Grid. This not only includes the concerns over carbon emissions and air quality, but also the estimations about the amount of water necessary to sustain the growth in global energy requirements. Actions taken by the 112th, 113th, and 114th Congress in response to federal agency regulations leading into 2015 could either accelerate or decelerate the Smart Grid adoption process.

2 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.

2.1 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 Federal Smart Grid Advisory Committee (EISA §1303(a))
- Provide a staff representative to the Smart Grid Task Force (EISA §1303(b))
- Maintain the Interoperability Framework (EISA §1305)
- 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 3 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 compatability 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 January 31st 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.

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.

Add content on possible international activities.

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 encourages 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 there were standing up the SGIP. Eventually this group was reorganized as the Cybersecurity Working Group (CSWG) under the SGIP with the following goals and objectives:

> ***GOALS***
> *The primary goal is to develop an overall cyber security strategy for the Smart Grid that includes a risk mitigation strategy to ensure interoperability of solutions across different domains/components of the infrastructure. The cyber security strategy needs to address prevention, detection, response, and recovery. Implementation of a cyber security strategy requires the definition and implementation of an overall cyber security risk assessment process for the Smart Grid.*
>
> ***OBJECTIVES***
> *The following objectives address the CSWG's primary goal. These objectives may change as more Smart Grid implementations occur and Smart Grid technologies further develop. These objectives include:*
>
> 1. *Assessing Smart Grid Interoperability Panel (SGIP) identified standards within an overall risk assessment framework that focuses on cyber security within the Smart Grid.*
> 2. *Developing a set of recommended security requirements that may be used by strategists, designers, implementers, and operators of the Smart Grid, (e.g., utilities, equipment manufacturers, regulators) as input to their risk assessment process and other tasks in the security life cycle of a Smart Grid information system. These security requirements are intended as a starting point for organizations.*
> 3. *Identifying Smart Grid specific problems and issues that currently do not have solutions.*
> 4. *Creating a logical reference model of the Smart Grid, which will enable further work towards the creation of a logical architecture*

and a security architecture. This work is being performed in coordination with the SGIP Architecture Committee (SGAC).

5. *Identifying inherent privacy risk areas and feasible ways in which those risks may be mitigated while at the same time supporting and maintaining the value and benefits of the Smart Grid.*
6. *Developing a conformity assessment program for security requirements in coordination with activities of the SGIP Smart Grid Testing and Certification Committee (SGTCC).*

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 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 DHS) that is addressing the possible responses to a national cyber emergency. The expectation is that NIST should have a major role in helping to define those responses, and would provide the appropriate level of leadership to the industry to ensure that they were prepared to respond to a cyber emergency as well.

2.2 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
- 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 agencies 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.

3 SGIP-2015

The assumption driving the SGIP vision for 2015 and beyond is based on the implementation of Smart Grid being a 20 to 30 year effort. As such, there is a need for an industry body under which vendors of all kinds and electric power providers can organize to tackle important issues. Because of its origins, the SGIP is a possible candidate that could evolve into this role. However, because of its current legal standing (the SGIP is not a legal entity), beyond the Smart Grid technology framework and roadmap published by NIST, there needs to be an evolutionary path established for the SGIP. As with the organizational changes recommended for NIST, it is necessary to decompose the expected functionality of the SGIP in 2015 and beyond.

3.1 Functions & Activities

As with many technological endeavors in the latter years of the 20th Century (telecommunications, the Internet, etc.), industry will continue to push the performance frontier in terms of smart grid for decades to come. As such, it will be as important in 2015 as it is today that there remains a common, technology and vendor neutral forum for industry leaders to discuss their common challenges and potential solutions. Ideally this will also involve the features of the ANSI essential requirements such as Openness, Balance, Lack of Dominance, and Due Process.

If innovation for the grid will continue to be driven in industry, deep pockets of subject matter expertise in each of the functional domains (generation, transmission, distribution, and consumer) will continue to evolve. Having them organized under a continually functioning SGIP-like body will make this individual subject matter expertise readily accessible by both government and industry implementers of smart grid.

Another interesting feature of the government-industry dynamic in the United States is that unlike a lot of countries, we don't have a centralized, government effort to write standards. Although we have a "National Institute of Standards and Technologies," the process of standards writing in the U.S. rolls up under the American National Standards Institute, or ANSI – and industry body that doesn't actually write the standards, but accredits the processes for those who do. It should also be noted that the work of ANSI doesn't stop at the U.S. borders as they also administer the U.S. National Committee for the International Electrotechnical Commission (IEC).

However, while ANSI performs a vital administration function in the standards writing process, they have no responsibility to identify gaps or defects in the content of existing standards, or to suggest possible areas for new standardization, either in the U.S. or abroad. Again, this type of function would be best placed with a neutral, industry-based body such as the SGIP, who could very readily examine any combination of ANSI or non-ANSI standards and specifications within the U.S. as well as international candidates from a variety of sources including the IEC. This would create a global catalog of standards that any industry or government official, anywhere in the world could cite.

Combined with the pockets of subject matter expertise as described earlier, the SGIP can remain the coordination point between stakeholders in the standards, manufacturing, and utility industries. It can produce educational materials for federal and state government staffs, regulators, and legislators; provide a common forum for public-private workgroups and committees; and effectively manage the industry semantics so that the concepts behind the conversations are consistent. Further, it would provide input to the Dept. of Energy Clearinghouse and administer industry ballots to achieve consensus on a broad range of industry concerns.

3.2 Staffing & Structure

The structure of the SGIP in 2015 is a major question which centers around whether it becomes its own legal entity. Currently, the SGIP is merely a public-private partnership organized under NIST and is not a legal entity in the U.S. However, they do have a logo which includes a trademark symbol, which begs the question, who really "owns" this trademark?

It should be noted that the application of the trademark "™" symbol is somewhat inconsistent between the various SGIP newsletters, flyers, PowerPoint slides, etc.

The reason this is important is because in 2010, the SGIP was already producing documents with essentially no ownership, if in fact the SGIP has no legal standing as an organization. A select few of the SGIP work products may become government documents, such as the NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cybersecurity*. However, a vast majority of the documents produced by the membership of the SGIP will not be destined for U.S. Government Printing Office (USGPO) document number and will need to be owned, maintained, and maintained by some legal U.S. entity. Other concerns would be the fact that you cannot sign a memorandum of understanding or agreement (MOU or MOA) with the SGIP; and that they cannot provide any form of endorsement. For example, in January of 2011, the Testing and Certification Committee of the SGIP, the SGTCC, produced an *Interoperability Process Reference Manual (IPRM)* encouraging companies to become testing and certification authorities for various smart grid standards. In exchange for their diligence, any company that goes through the process of developing a testing and certification plan will be rewarded by being "listed" as an approved Interoperability Testing and Certification Authority, or ITCA by the SGTCC.

In light of these concerns, it seems obvious that in order to preserve the value of the work being done today by the SGIP members, and to maintain the integrity of the vendor and technology neutral forum for the industry that the SGIP should become its own legal entity. Possible models for this include the North American Electric Reliability Corporation (NERC), the American National Standards Institute (ANSI), or an "Industry Council" model, such as the Utilities Telecom Council (UTC), or the Sustainable Buildings Industry Council. This would permit the SGIP to charge a reasonable form of dues for its members, allow the federal government to cease funding the administration of the panel, and continue to maintain its own agenda, governing board, charter, and bylaws.

4 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 in Section 2.2 above.

Also, if they are going to be the lynchpin of Smart Grid NIST needs to develop a response capability in the event of an electric grid disaster – whether physical or cyber. This needs to be coordinated 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 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 C2 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.

Conduct a demonstration program, possibly aligned with the military Base Realignment and Closing (BRAC) strategy. The focus for this demonstration should be on reliability & 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 legal 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 SGAC Federal Advisory Committee 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.