2016

U.S. Energy Sector Cybersecurity: Hands-Off Approach or Effective Partnership?

T. M. Ballou
University of Nebraska at Omaha, tballou@unomaha.edu

Joseph A. Allen
University of Nebraska at Omaha, josephallen@unomaha.edu

Kyle Francis
University of Nebraska at Omaha, kylefrancis@unomaha.edu

U.S. Energy Sector Cybersecurity: Hands-off Approach or Effective Partnership?

TM Ballou, JA Allen, KK Francis

University of Nebraska, Omaha
Omaha, Nebraska
E-mail: tballou@unomaha.edu; josephallen@unomaha.edu; kylefrancis@unomaha.edu

Abstract: *Recent reporting has identified significant threats to the U.S. energy's critical infrastructure from nation states and other groups through cyberspace. Efforts to improve the security and resilience of U.S. energy infrastructure relies upon voluntary partnerships between the U.S. Government and public and private energy infrastructure owners. This paper examines ideal Public-Private Partnership (PPP) characteristics and compares them to an actual PPP in the U.S. The results identify strengths of and challenges to efforts to secure U.S. energy infrastructure. The research was conducted through a combination of literature reviews and interviews with a sample of U.S-government and private-energy infrastructure representatives.*

Keywords: *Cybersecurity, Public-Private Partnerships, Critical Infrastructure Protection, Energy Sector*

Introduction

Security of the United States' critical infrastructure (CI) is at risk from both physical and cyber threats. Cyber legislation, directing the protection of United States' CI, has been a subject of continuous scrutiny over the last few years. For example, due to Congress' inability to agree upon specific legislation, the President signed Executive Order 13636 (2013) and Presidential Policy Directive (PPD) 21 (2013). The intent was to enhance protection, security, and resiliency of our CI through collaborative efforts between federal agencies, public-private owners, and operators of critical infrastructure using existing federal authorities. The Department of Homeland Security (DHS) was designated the lead for coordinating security of the nation's CI. The means by which DHS intended to accomplish this responsibility was primarily through public-private partnerships (PPP) and voluntary programs.

There has been great effort between government, public, and private organizations to coordinate the way forward, while establishing programs to secure our CI. The fragmentation of CI due to privatization and, moreover, deregulation makes overall security that much more difficult and cumbersome (De Bruijne & Van Eeten 2007). De Bruijne and Van Eeten (2007) go on to state, "Instead of one or comparatively few public organizations cooperating under hierarchical command and control, large networks of organizations with competing interests became involved in the management of CIs and the reliable provision of services". Therefore, the government must rely upon complex and often fragmented PPPs to secure our CI.

Executive Order 13636 (2013) identified 16 critical infrastructure sectors spanning multiple U.S. areas from energy, financial services, and communications to transportations systems, dams, and the defense industrial base. Of particular concern is the energy infrastructure, the most critical CI, which is a fundamental component of the remaining fifteen critical infrastructure sectors. The DHS's Energy Sector Overview webpage states that the U.S. electricity sector "contains more than 6,413 power plants" with "more than 80 percent of the country's energy infrastructure owned by the private sector" (DHS 2014a). Not long ago, the energy grid was physically and virtually separated from the Internet. The 'smart grid' is "basically the system of control, computer, communication, and automation technologies that will allow a rapid response to rapidly changing grid conditions" (Kaster & Sen 2014). From a business perspective, it has become more effective and efficient to utilize capabilities that can monitor and transmit data regarding the status of energy production and distribution. The upside is that the electricity segment of the energy sector is one of the only CI sectors with mandatory cyber security standards (Zhang 2013). However, a 2013 report from the United States Congress found that 74 of 85 (87%) reporting utilities complied with a list of North American Electric Reliability Corporation (NERC) mandated security measures, but only 13 of 36 (36%) implemented voluntary measures against the same threat (Kaster & Sen 2014). From a security standpoint, a much greater risk exists because of the interdependencies within the grid and an increased risk from potential cascading effects (Massoud & Wollenberg 2005).

Regardless of the existing partnerships, there remains a philosophical difference between the government, which is focused on the security of CI, and private owners and operators, whose focus is on business continuity, efficiency, and profit (Dunn-Cavelty & Suter 2009). The purpose of this study is to synthesize the concepts of the ideal PPP to provide context and to allow a comparative analysis of how the government is executing the partnership to secure the energy grid in order to identify areas of success and areas of heightened risk. First, what makes successful PPPs are reviewed; this review is followed by a review and assessment of current PPPs used by the DHS and DOE to protect the U.S.'s energy infrastructure. Finally, impediments and opportunities to improve overall U.S. energy sector cybersecurity are identified.

Likelihood of a Cyberattack on U.S Power Infrastructure

In recent years, a significant increase in cyber exploitation and attacks directed against the United States and abroad has occurred. In July 2012, General Keith Alexander, then Director of the National Security Agency and Commander, U.S. Cyber Command, stated that there was a 17-fold increase in cyberattacks on American infrastructure from 2009 to 2011, which were initiated by criminal gangs, hackers, and other nation states (Sanger & Schmitt 2012). This concern was reinforced in November 2014 when the Director of the National Security Agency, Admiral Mike Rogers, testified to the House (Select) Intelligence Committee that

> there shouldn't be any doubt in our minds that there are nation-states and groups out there that have the capability to do that, to enter our systems, to enter those industrial control systems, and to shut down, forestall our ability to operate our basic infrastructure, whether it's generating power across this nation, whether it's moving water and fuel. (NSA 2014)

This vulnerability is illustrated in the following examples of the effect cyber tools can have on critical infrastructure. First, there is the STUXNET worm, which affected Iran's nuclear

development capabilities in 2010. STUXNET caused a malfunction that was invisible to human operators because the Supervisory Control and Data Acquisition (SCADA) screens in the control room suggested normal operation. In this case, the worm was aimed solely at industrial equipment made by Siemens that controls oil pipelines, electric utilities, nuclear facilities, and other large industrial sites (Sanger 2010). Second is the SHAMOON virus directed against Saudi Arabian Oil Company (ARAMCO) in 2012. SHAMOON spread throughout the company's network and affected as many as 30,000 computers. In addition to affecting ARAMCO, the virus spread and was found on the system of RasGas, a Qatari owned liquefied natural gas company (Nakashima 2013). Third, is the hack of a German steel mill as reported by the German Federal Office for Information Security in 2014 (BBC News 2014). Attackers targeted emails using a 'spear phishing' technique to obtain log-in information, which gave them access to critical production systems at the mill leading to massive damage.

The previous cases represent a small example of the potential damage a cyberattack can have on critical systems and networks. With the reliance the U.S. places on critical infrastructure, a deliberate cyberattack directed against the United States' energy infrastructure could have a devastating impact on the country and on the economy. Understanding this new reality, collective situational awareness must be insured, critical infrastructure must be protected, and efficient mitigation measures must be established to minimize effects generated by a cyberattack on the nation's CI. Given these examples and challenges, the authors next review the current literature on PPP for ways to improve the situation.

Ideal Public-Private Partnership (PPP) Characteristics

After reviewing the extant literature on PPPs (Mohr & Spekman 1994; DHS 2013a; Dunn-Cavelty & Suter 2009; Das & Bing-Sheng 1998; Bovaird 2004; Rufin & Rivera-Santos 2012; Ring & Van de Ven 1992) two models for successful partnerships that have support from multiple types of PPPs were identified. **Table 1**, below, depicts the two models and their associated characteristics identified for successful PPPs. It is clear that the models have both similarities and differences. After comparing the models it was determined that trust and information sharing are the two common characteristics. The existence of these attributes implies that both partners acknowledge their mutual dependence and their willingness to work for the survival of the relationship. Should one party act opportunistically, the relationship will suffer and both will feel the negative consequences (Mohr & Spekman 1994). Cheating, distorting information, and misleading partners are examples of opportunistic behaviour in alliances, which is a cause for the relatively high rate of failure of alliances (Das & Bing-Sheng 1998).

Mohr & Spekman (1994)	**Department of Homeland Security (2013a)**
Trust: The belief that a party's word is reliable and that a party will fulfil its obligation in an exchange.	**Trusted Environment:** Environment where partners can continue to collaborate despite any differences in organizational structure, culture, motivation, and other factors that could easily

	lead to conflict.
Commitment: Willingness of trading partners to exert effort on behalf of the relationship.	**Appropriate Membership:** Having the involvement of the major parties that shape the security and resilience environment of critical infrastructure.
Coordination: Related to boundary definition and reflective of the set of tasks each party expects the other to perform.	**Defined Purpose:** Partners must have a common interest to form an effective partnership.
Interdependence: Acknowledgement that each is dependent on the other.	**Articulated Goals:** Generally based on specific risk or risk-management considerations (or the need to build greater capability to fill a security gap) and should be developed jointly among partners.
Communication Behaviour: **- Quality:** Includes such aspects as the accuracy, timeliness, adequacy, and credibility of information exchanged. **- Information Sharing:** Extent to which critical, often propriety, information is communicated to one's partner. **- Participation:** Extent to which partners engage jointly in planning and goal setting.	**Robust Communication:** Refers to relationships, processes, and channels for sharing perspectives and information, and engendering open conversation.
Conflict Resolution Techniques: Given that a certain amount of conflict is expected, an understanding of how such conflict is resolved.	**Clear Governance:** Clearly defining and documenting expectations, as well as roles and responsibilities and related decision-making ground rules and protocols.
	Leadership Involvement: Successful public-private partnerships are guided by strong and consistent leadership from all participants.
	Measurable Outcomes: Well-designed outputs which can represent progress and provide results to management and external

	stakeholders that sustain the commitment of time and resources.

Table 1: Model comparison (shading depicts similarities)

Organizations and individuals enter into partnerships to establish strategic relationships with others who share similar goals, but rely upon each other to accomplish their objectives. Without these relationships the objectives could not accomplished (Mohr & Spekman 1994; Rufin & Rivera-Santos 2012). However, PPPs are not always the answer. Bovaird (2004) states,

> a major problem of partnership approach to public issues is that it brings fragmentation of structures and processes, which in turn leads to blurring of responsibilities and of accountability…yet there is no direct mechanism by which these partnerships can be held accountable in a proper fashion.

Based on the research, it appears that trust is the foundational building block that all successful PPPs are built upon. Because PPPs are generally less hierarchal and more consensus-focused, partners within a PPP rely heavily upon trust for execution of tasks, exchange of information, and limiting opportunistic behaviors. Ring and Van de Ven (1992) identify "two definitions [of trust] frequently used in literature: (1) confidence or predictability in one's expectations and (2) confidence in the other's goodwill". Rufin and Rivera-Santos (2012) assert "that interpartner trust in PPPs would greatly facilitate interactions. Yet our reasoning suggests that the difficulty to build trust in a PPP is such that partners are likely to rely on formal procedures rather than on trust". Generally, trust may be based on norms of equity which define the degree to which one party judges that another party will fulfil its commitments and that the relationship is equitable (Ring & Van de Ven 1992).

Often PPPs lack familiarity with their partners due to differing goals, organizational processes, and cultures, which can affect the trust factor. The degree to which trust may be created between the partners is thus extremely limited (Rufin & Rivera-Santos 2012). In addition, the potential exists that any or all partners may enter the PPP with pre-existing biases and mistrust due to previous interactions and partnership efforts. Trust affects how leaders view risk to their own companies and corporations. How much risk a company or corporation is willing to take depends upon whether the risks are within or outside their span of control. According to Dunn-Cavelty and Suter (2009), "The fundamental problem is that trust can only be developed through collaboration which in turn also depends on trust". Closer ties result in more frequent and more relevant information exchanges between high performing partners (Huber & Daft 1987).

Communication and sharing of information, the second common characteristic, is essential to ensuring that defense and protective measures are effective. The new-found reliance upon the Internet for connectivity to monitor and to track the status of the energy grid is paramount, yet the same reliance makes users more vulnerable to greater lasting effects if attacked. The assumption is that this interdependence generates a shared risk to the entire PPP. Therefore, partners must have confidence that the information shared is used for the intended purpose and is accurate, timely, and actionable. Mohr and Spekman (1994) make the case that information sharing is a component to overall communication behaviour. They contend that this behaviour consists of communication quality, information sharing, and participation. This suggests that quality and pertinent data are

more likely to improve open and honest lines of communication, to establish credibility, and to increase overall trust among the partners. From a business perspective, information may have direct consequences for profits and future ventures if compromised or handle inappropriately. For example, information exchange, if used improperly or shared with the wrong audience, can bring about lawsuits due to breaches of civil liberties or negligent release of personal information. However, when the government and public and private industry share information, it demonstrates their willingness to cooperate and coordinate to achieve common goals and purpose.

With greater interdependency comes increased reliance upon coordination and cooperation to protect and secure the energy sector. Das and Bing-Shen (1998) define partner cooperation as the willingness of a partner to pursue mutually compatible interests in the alliance rather than to act opportunistically. In other words, partners work towards a common goal and purpose. Coordination and cooperation will only be achieved if the PPP has common objectives and goals and if partners consider it beneficial to business continuity. However, commitment is required at all levels of the PPP. Because more committed partners will exert effort and will balance short-term problems with long-term goal achievement, higher levels of commitment are expected to be associated with partnership success (Mohr & Spekman 1994). Mohr and Spekman (1994) also suggest that trust, the willingness to coordinate activities, and the ability to convey a sense of commitment to the relationship are keys to success. At times, cooperation among partners may be in competition with business operations and profitability. When this occurs, the latter is most likely to take priority and result in a failed PPP.

The most research attention has been on PPP governance methods. First, the issue of governance and oversight required to support PPPs must be considered. There are many forms of governance; however, Dunn-Cavelty and Suter (2009) identify two primary forms of governance: the "network approach" and the "neoliberal approach". The latter refers to the assumption that the "state" precisely defines and contractually stipulates how the tasks delegated to the companies must be fulfilled, all while maintaining control and intervening if the private sector fails to meet its obligations. "Network approach" describes the middle ground between the neoliberal and a "hands off" approach. In this method, the government becomes a coordinator, and thereby ensures that tasks are met by the network providers while relegating control to the individual private owners. This is done by way of an established framework and by using different types of instruments at their disposal as an enforcement mechanism. Instruments are tools to compel compliance or completion of the required tasks and standards and can take the form of loans, subsidies, or tax relief, to name a few. Without a hierarchal command and control structure, governance and oversight must be considered as a part of the PPP (Dunn-Cavelty & Suter 2009).

In this section the major characteristics for a successful PPP have been identified. However, there are characteristics identified in **Table 1**, above, that were not essential for PPP success. For example, leader involvement, distribution of tasks, and measurable outcomes were deemed important by some, but they are merely sub-characteristics of the four primary characteristics (trust, information sharing, mutual goals and purpose, and coordination and cooperation) noted earlier. Regardless of whether the partnership demonstrates the above characteristics, the primary focus of private owners and operators is on business operations. If business operations are affected, profits due to the PPP will also be affected and then the partnership will likely fail. Therefore, the partners have to believe that the risk of not supporting the PPP outweighs the potential long-term effect on

the company's mission and profitability.

Actual Model in Practice

Based on the review of the processes and procedures established by the government and by the private sector, it is clear that there has been considerable effort towards establishing PPPs to secure the nation's critical infrastructure. In the U.S. Government Accountability Office (2010) (GAO), all of the organizations identified trust as the essential underlying element to successful relationships and said that trust could be built only over time and, primarily, through personal relationships. The government has established multiple mechanisms to coordinate, collaborate, and share information; however, there are few mechanisms deliberately targeting trust and relationship building within the partnership. In an effort to mitigate this concern, DHS has employed the Critical Infrastructure Partnership Advisory Council (CIPAC) legal protections and has established the Protected Critical Infrastructure Information (PCII) program to enhance that level of trust (DHS 2013a). However, building trust typically occurs over time, is often personality driven, and requires appropriate mechanisms to facilitate these types of relationships. Barring any radical changes to U.S. law granting DHS and DOE greater authority, the government's only option to establish a successful PPP is by establishing and building trust within and among the PPP. Based on the research, the most pointed measure to determine if trust exists within the PPP is the willingness to share sensitive information between the government and private sector.

To improve overall communication and coordination of the protection efforts, DHS established Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC) to address sector-specific protection and resilience (DHS 2014b). Additionally, specific to the energy sector are the ES-ISAC, Energy GCC, Energy Sub-Sector (Electricity and Oil and Natural Gas) SCCs, and others. **Figure 1**, below, depicts a combination of these entities, multiple sub-sector ISACs, and programs such as DHS's Homeland Security Information Network—Critical Infrastructure (HSIN-CI) and Protected Critical Infrastructure Information (PCII) Program—and demonstrates the government's commitment to protecting its CI. Effective coordination among the partners can mitigate duplicative efforts and can minimize the resources required to correct or to mitigate a problem that may arise. According to Frangopoulos, Eloff and Venter (2015), "economic considerations are being used in the process of risk assessment, usually to define an organization's 'risk appetite' and lead to informed decisions regarding the implementation of security measures". This is particularly important when issues such as research and development (R&D), building the necessary workforce, and establishing technical standards across a wide variety of networks are being considered.

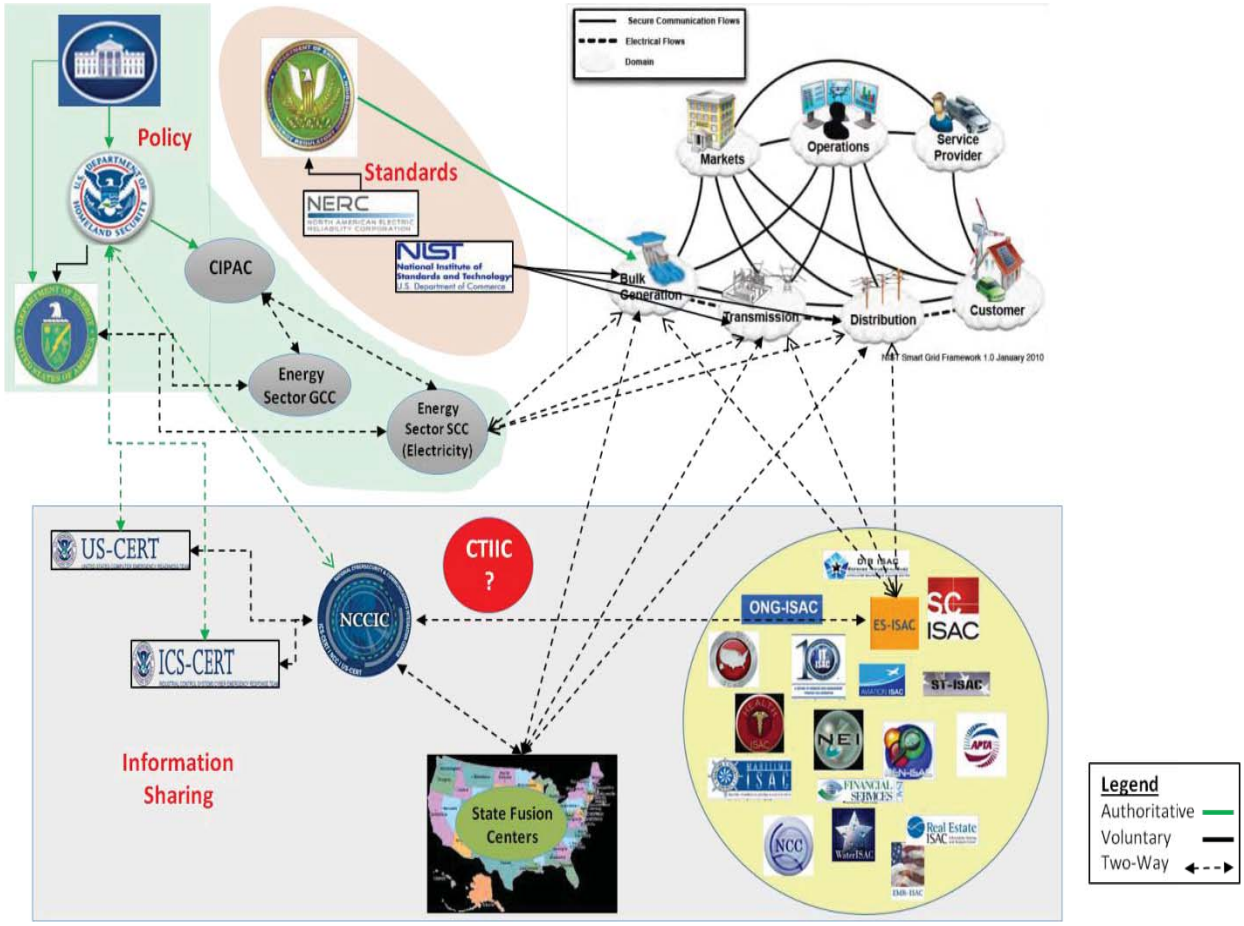

Figure 1: Energy sector overview (representative only)

With the establishment of these numerous entities, programs, and processes, findings from a 2013 GAO report were particularly troubling. In this report, the U.S. GAO (2013) found that the lack of a centralized information-sharing system continues to hinder progress. The National Cybersecurity and Communications Integration Center (NCCIC) and the ES-ISAC were designed to be those central clearing houses for sharing information for the overall U.S. CI sector and the energy sector, respectively. Private industry expects access to sensitive or classified information regarding cyber threats that is useable, timely, and accurate and must also have a means of sharing the information securely (GAO 2010). The process which the government uses to downgrade or to declassify information is time consuming and "unfortunately, too often the information that is shared is not considered to be of sufficient quality, nor is it sufficiently actionable" (DHS 2013b). Laws, regulations, and policy regarding the over classification, declassification, and sharing of information precludes timely dissemination of threat information from the government to the private sector. Incidents similar to Snowden's release of top-secret National Security Agency (NSA) surveillance practices and the discovery of NSA's PRISM program do not benefit the government's case with the protection of shared information; moreover, such discoveries justify the private owners' and operators' reasons for concern.

Information sharing is not solely for sharing threat information, but it also includes communicating goals, objectives, and future plans. Mutual goals provide partners a common understanding of expectations which should be accomplished along the way. In the NIPP, the DHS identifies its vision, mission, and objectives and describes its goals as a national unity of effort to secure the nation's CI. This vision and objectives document

> was developed through a collaborative process that included the active participation of the critical infrastructure community, including private industry; public and private sector owners and operators; state, local, tribal, and territorial government agencies; non-governmental organizations; sector-specific agencies; and other federal departments and agencies. (DHS 2013b)

However, specific goals for each sub-sector are established via the previously mentioned GCCs, and SCCs and are codified in Sector-Specific Plans (SSP)/Charters. The energy sector, in coordination with private owners and operators, developed its own goals in its 2010 SSP (DOE 2010). The goals are sector-specific and build upon the overall DHS goals. DHS noted in its assessment that "selecting and working toward clear, relevant, tangible and achievable goals create unity of effort and motivate partners" (2013a). The report added that "too often, though, there appears to be a difference between the sector partnerships' goals and objectives, and the actual risk management programs developed by stakeholders" (DHS 2013a).

Research suggests that a key consideration is that the private partner must believe that the risk of not supporting the PPP outweighs the potential long-term effect on the company's mission and profitability. This only occurs when the partnership's purpose and benefit are greater than the individual need. Through the PPP, the government and private sectors are to work in tandem to create the context, framework, and support for coordination and information-sharing activities required to implement and sustain a specific sector's critical infrastructure protection efforts (GAO 2013). The Critical Infrastructure Cyber Community C³ Voluntary Program is a great example. It provides the coordination point within the federal government for critical-infrastructure owners and operators interested in improving their cyber-risk-management processes. The C³ Voluntary Program aims to: 1) support industry in increasing its cyber resilience, 2) increase awareness and use of the Framework, and 3) encourage organizations to manage cybersecurity as part of an all-hazards approach to enterprise risk management (DHS 2015).

Although not identified as critical to the success of the PPP or to achieving the mission or end state of the partnership, some level of governance is required to protect the energy sector CI. Executive Order 13636 (2013) explicitly states that

> this order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

Essentially, all private owners' and operators' activities are voluntary, which makes enforcement nearly impossible. The U.S. government takes a *laissez-faire* approach to CI protection. However, because of current laws and regulations, DHS has few options to direct the protection of the nation's

CI. In the end, there are a number of federal, state, local, and private organizations involved in energy CI protection and regulation including the DHS, DOE, FERC, NERC, NIST, state, local, and private utility commissions and boards (Hébert 2013).

Telephone interviews with local and federal representatives associated with the protection of U.S. energy infrastructure were conducted. Interviews were conducted between 27 March and 6 April 2015 with local and federal energy representatives. All interviewees requested to remain anonymous due to the fact that they were not authorized to speak on behalf of their organizations. The information provided is considered personal opinion based on the observations during execution of daily duties. The interview questions (see **Appendix 1**, below) focused on the elements of the PPP that are being executed successfully and the areas in which the PPP needs to improve. During the interview with a federal government agency representative responsible for coordinating the protection of the nation's CI, it was stated that trust is critical to the success and is reliant upon personal relationships established at the lowest levels. According to the interviewee, trust at the local level took a long time to establish and is working quite well. However, trust does not automatically exist from the local level up to the government agencies. This affects all aspects of the partnership at the local, regional, and national levels. Much of the interaction between government and private sector is via the energy infrastructure of state and local associations because of the large number of ES CI owners and operators. It was said that not only do private owners and operators not trust the government, but also federal energy agencies are reluctant to share identified vulnerabilities with the ES community in fear that the information will become public knowledge. Similar issues arise when the private sector releases potentially damaging information to the government, which may have a damaging impact on company reputation, privacy, and civil liberties. Legal and corporate barriers discourage sharing of data that may impact the company's reputation. While the larger corporations are more likely to participate, the smaller companies are not incorporated into this information-sharing mechanism due to resource constraints and lack of awareness, thus resulting in increased risks to their networks.

This sentiment was reinforced during a discussion with a local power company representative. He praised the positive efforts DHS, DOE, and public and private owners and operators have made over recent years. However, the representative stated that the most problematic issues are poor relationships and lack of communication between the government agencies and private industries. At the local level, personal relationships exist, but this is not reflected at the upper level. He admitted that, although his company receives and acts upon warnings and reports from the ES-ISAC, NCCIC, and other organizations, these organizations deliberately do not reciprocate by sharing company information with the government. The concern is the same—they fear that the information will not be handled appropriately. He praised the government’s willingness to provide vulnerability assessments and added that it was beneficial to the company’s protection efforts. He also acknowledged his company's participation in the SCC and collaboration with the regulatory bodies to assist with standards development. He expressed doubt that smaller energy providers were aware of many of the government's efforts and that they lacked the resources to provide increased cybersecurity measures. Lastly, the opinion of the representative was that, to effectively protect the energy sector, the government will eventually have to make many of the voluntary programs mandatory with incentivized participation to ensure compliance with established cybersecurity standards.

Similarly, a representative from the ES-ISAC agreed that the lack of information sharing, due in large part to the lack of trust in the government agencies, is the primary obstacle to protecting the energy infrastructure. Public and private companies are concerned that information shared with the ES-ISAC, which is funded by the FERC and the regulatory body for the energy CI, will be used against the reporting company. It was further stated that the government, as a whole, must do a better job to teach and to educate the community of interest in order to improve the relationships and to ease the concerns of the public and private partners. The representative, however, did say that much progress has transpired over the years and that the current membership consists of over 1900 regulated energy companies and over 4000 non-regulated companies. The overall increase in membership suggests the possibility of improved relationships generally. This is great progress, but there is still a long way to go in improving the overall situational awareness and cybersecurity of our energy CI.

Conclusion/Implications

One conclusion that can be drawn from this research is that technology will only increase, and this includes the energy grid. Electric grid owners and operators will continue to rely on smart technology to provide power to the nation and to increase overall efficiency while simultaneously increasing our already prevalent vulnerabilities. Based on research and interviews, PPPs within the energy sector have begun to establish trusting relationships, but primarily in smaller groups (individual to individual) and not consistently across the entire energy sector. Academic, government, and industry reports agree that relationships must be improved. Given the ideal characteristics and what is actually occurring as introduced earlier, the following suggestions are made:

First and foremost there should be mechanisms for ensuring: 1) all partners are informed of the threats and recommended actions, and 2) standards are complied with in order to mitigate vulnerabilities and threats. The energy sector, as well as the broader U.S. CI, is only as strong as the weakest link. Markey and Waxman (2013) illustrate this concern:

> of those that responded to the question regarding compliance with mandatory STUXNET standards, 91% of investor-owned utilities (IOU), 83% of municipally- or cooperatively-owned utilities, and 80% of federal entities that own major pieces of the bulk power system reported compliance. By contrast, of those that responded to a separate question regarding compliance with voluntary STUXNET measures, only 21% of IOUs, 44% of municipally- or cooperatively-owned utilities, and 62.5% of federal entities reported compliance.

The key takeaway is that the mandatory standards, directed by the FERC, were inconsistently followed. If mandatory standards are not implemented across the sector, how can there be assurance that voluntary programs, actions, and activities will effectively protect energy CI?

Second, the DOE should reassess the best approach for coordinating the protection of energy CI. Building trust within the partnership is the single characteristic within the PPP, which everything else hinges upon. This requires a deliberate and concerted effort working closely with public and private owners and operators at all levels to improve overall awareness. This starts by increasing participation in voluntary programs by educating the public and private sector of programs, processes, and available support mechanisms. Also, incentivizing and rewarding participation is

essential as long as the legislation fails to provide additional authorities to the DHS. There have been discussions and research efforts to address increased participation for protection of energy CI, using incentives and rewards; however, implementation of such measures has failed to materialize.

Third, the government needs to provide the public-private sector with liability protection for voluntarily sharing critical information. This gets to the heart of the concern regarding sharing information from the private sector. The fear of sharing sensitive information opens the organization up to civil suits affecting reputations and profits. Public and private owners and operators need assurance that information shared between the private sector and government will be treated in accordance with established laws and regulations. For example, they must be confident that information shared by private owners with the ES-ISAC, which is funded by the FERC, will not result in fines or penalties by the FERC.

Fourth, the U.S. Government should establish a national cybersecurity strategy to protect critical infrastructure. The energy sector faces a wide variety of regulation, guidance, and policies from local, state, and federal agencies. This guidance sometimes clashes or is not in line with the company's business plans and operations, which may drive limited implementation of the cybersecurity guidance affecting overall cybersecurity risk. A national cybersecurity strategy would serve as the source guidance and would drive the development and content within all subordinate agency-level guidance documents. This would provide a mechanism to ensure all plans are nested and consistent to minimize confusion among the community of interest. Therefore, it is crucial for DHS, DOE, regulatory agencies, and for the private owners and operators to work together to clearly identify and to update all plans and policies to ensure consistency throughout the energy sector.

Lastly, authorities and oversight must be addressed in future legislation. DHS, DOE, and other agencies lack the authority to establish, to direct, and to enforce compliance with cybersecurity standards. Without requisite authority, the government's approach to protect the energy infrastructure is banking on public and private companies to do the right thing. Proper authority would allow the DHS or DOE to initiate deliberate steps to establish, to direct, and to compel compliance and to enforce cybersecurity standards across the energy critical infrastructure. The electric grid and associated infrastructure are too important to hope for cybersecurity.

Appendix 1 – Interview Questions

1. What traits do you believe are most critical for a successful PPP?
2. What traits do you believe are currently working well in the protection of our energy infrastructure? Please explain your response.
3. What traits do you believe are not being executed well in the protection of our energy infrastructure and why?
    i. In your opinion, how would you improve these traits?
4. In your opinion, how do organizations and government agencies establish mutual trust?
    i. Do you feel that there is trust between your organization and the private or government agencies responsible for coordinating the protection of energy critical infrastructure? Explain.
5. How would you rate the partnership and your organization's willingness to:
    i. Participate with the DHS/DOE or public/private sector (whatever is applicable) regarding energy infrastructure protection?
    ii. Coordinate with the DHS/DOE or public/private sector (whatever is applicable) regarding energy infrastructure protection?
    iii. Cooperate with the DHS/DOE or public/private sector (whatever is applicable) regarding energy infrastructure protection?
6. How often does your organization coordinate/collaborate with government agencies and other public/private energy infrastructure owners & operators regarding security and protection issues?
    i. How is it accomplished (e.g., venues, groups, etc.)?
7. How would you assess the partnership and your organization's willingness to share information regarding vulnerabilities, intrusions etc.?
8. How is information shared between your organization and the government or public/private sector (whatever is applicable)?
    i. What mechanisms are in place to share information regarding current, imminent, or potential threats?
    ii. Are the processes and mechanisms different based on imminence of the threat?
    iii. How is threat information received?
9. Describe to me the oversight and/or supervision of protection and security efforts?
    i. What is the leadership structure as it relates to protecting critical energy infrastructure?
10. The U.S. strategy for protecting our critical infrastructure relies primarily on public-private voluntary participation. What is your opinion on this approach and is it effective?

References

BBC News 2014, 'Hack attack causes 'massive damage' at steel works', *BBC News Technology,* viewed 7 January 2016, <http://www.bbc.com/news/technology-30575104>.

Bovaird, T 2004, 'Public–private partnerships: from contested concepts to prevalent practice', *International Review of Administrative Sciences*, vol. 70, no. 2, pp. 199-215.

Das, TK & Bing-Sheng, T 1998, 'Between trust and control: developing confidence in partner cooperation in alliances', *Academy of Management Review*, vol. 23, no. 3, pp. 491-512.

De Bruijne, M & Van Eeten, M 2007, 'Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment', *Journal of Contingencies and Crisis Management*, vol. 15, no. 1, pp. 18-29.

DHS 2013a, Evaluation of the Existing Public-Private Partnership Model., viewed 28 February 2015, <https://www.chicagofirst.org/resources/dhs_partnership_report.pdf>.

DHS 2013b, *National Infrastructure Protection Plan (NIPP) 2013: partnering for critical infrastructure security and resilience*, viewed 1 March 2015, <http://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf>.

DHS 2014a, *Energy sector: sector overview*, viewed 15 February 2015, <http://www.dhs.gov/energy-sector>.

DHS 2014b, *Critical Infrastructure: sector partnerships*, viewed 1 March 2015, <http://www.dhs.gov/critical-infrastructure-sector-partnerships>.

DHS 2015, 'About the critical infrastructure cyber community C^3 voluntary program', viewed 11 March 2015, <http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program>.

DOE 2010, 'Energy sector-specific plan: An annex to the national infrastructure protection plan', viewed 7 March 2015, <http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Energy_SSP_2010.pdf>.

Dunn-Cavelty, M & Suter, M 2009, 'Public–private partnerships are no silver bullet: an expanded governance model for critical infrastructure protection', *International Journal of Critical Infrastructure Protection*, vol. 2, no. 4, pp. 179-87.

Executive Order No. 13636 2013, 'Improving critical infrastructure cybersecurity', *Federal Register,* vol. 78, no. 33, p. 11739.

Frangopoulos, ED, Eloff, MM, & Venter, LM 2015, 'Cybersecurity economics: induced risks, latent costs, and possible controls', *Journal of Information Warfare,* vol. 13, no. 4.

Hébert, C 2013, 'The most critical of economic needs (risks): a quick look at cybersecurity and the electric grid', *The Electricity Journal*, vol. 26, no. 5, pp. 15-19.

Huber, GP & Daft, RL 1987, 'The information environments of organizations', *Handbook of Organizational Communications,* Sage Publications, Newbury Park, CA, U.S.A., pp. 130-64.

Kaster, P & Sen, PK 2014, 'Power grid cyber security: challenges and impacts', *North American Power Symposium* (NAPS), pp. 1-6.
Markey, EJ & Waxman, HA 2013, 'Electric grid vulnerability: industry responses reveal security gaps', U.S. House of Representatives, Washington, D.C., U.S.A.

Massoud, AS & Wollenberg, BF 2005, 'Toward a smart grid: power delivery for the 21st century', *Power and Energy Magazine, IEEE*, vol. 3, no. 5, pp. 34-41.

Mohr, J & Spekman, R 1994, 'Characteristics of partnership success: partnership attributes, communication behavior, and conflict resolution techniques', *Strategic Management Journal*, vol. 15, no. 2, pp. 135-52.

Nakashima, E 2013, 'U.S. warns industry of heightened risk of cyberattack', *Washington Post,* viewed 15 February 2015, <http://articles.washingtonpost.com/2013-05-09/world/39139314_1_senior-u-s-oil-and-gas-companies-iran>.

NSA 2014, Rogers Testimony, Hearing of the House (Select) Intelligence Committee Subject: 'Cybersecurity Threats: The Way Forward', National Security Agency/ Central Security Service, viewed 15 February 2015, <https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS. Hill.20.Nov.pdf>.

Presidential Policy Directive 21 2013, 'Critical infrastructure security and resilience', viewed 22 February 2015, <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

Ring, PS & Van de Ven, AH 1992, 'Structuring cooperative relationships between organizations', *Strategic Management Journal*, vol. 13, no. 7, pp. 483-98.

Rufín, C & Rivera-Santos, M 2012, 'Between commonweal and competition; understanding the governance of public-private partnerships', *Journal of Management*, vol. 38, no.5, pp. 1634-54.

Sanger, DE 2010, 'Iran fights malware attacking computers', *The New York Times*, viewed 15 February 2015, <http://www.nytimes.com/2010/09/26/world/middleeast/26iran.html?_r=2>.

Sanger, D & Schmitt, E 2012, 'Rise is seen in cyberattacks targeting U.S. infrastructure', *The New York Times*, viewed 15 February 2015, <http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html?_r=3&>.

U.S. GAO 2010, 'Critical infrastructure protection: key private and public cyber expectations need to be consistently addressed', viewed 15 February 2015, <http://www.gao.gov/products/GAO-10-628>.

U.S. GAO 2013, 'Cybersecurity national strategy, roles, and responsibilities need to be better defined and more effectively implemented', viewed 15 February 2015, <http://www.gao.gov/assets/660/652170.pdf>.

Zhang, Z 2013, 'Cybersecurity policy for the electricity sector: the first step to protecting our critical infrastructure from cyber threats', *Boston University Journal of Science and Technology Law,* vol. 319, pp. 319-20.