Response of RCC Consultants, Inc., to the Request for Information Entitled *Developing a Framework To Improve Critical Infrastructure Cybersecurity* and Issued by the National Institute of Standards and Technology

I. Introduction

RCC Consultants, Inc. ("RCC"), appreciates the opportunity to respond to the request for information issued on February 26, 2013, by the National Institute of Standards and Technology (that request for information, the "RFI"; and that institute, "NIST").[1]

The RFI, which is entitled, *Developing a Framework To Improve Critical Infrastructure Cybersecurity***,** was issued by NIST in connection with NIST's conducting a comprehensive review to develop a framework to reduce cyber risks to critical infrastructure[2] (the "Cybersecurity Framework" or the "Framework"). NIST has indicated that the Framework will consist of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

The purpose of the RFI is to obtain "information to help identify, refine, and guide the many interrelated considerations, challenges, and efforts needed to develop the Framework." The RFI indicates that "[i]n developing the Cybersecurity Framework, NIST will consult with the Secretary of Homeland Security, the National Security Agency, Sector-Specific Agencies and other interested agencies including the Office of Management and Budget, owners and operators of critical infrastructure, and other stakeholders including other relevant agencies, independent regulatory agencies, State, local, territorial and tribal governments."

The RFI poses a number of specific questions, but indicates that "[t]he questions are not intended to limit the topics that may be addressed. Responses may include any topic believed to have implications for the development of the Framework regardless of whether the topic is included in this document."

RCC appreciates the freedom afforded by the RFI, and, by this **Response of RCC Consultants, Inc., to the Request for Information Entitled *Developing a Framework To Improve Critical Infrastructure Cybersecurity* and Issued by the National Institute of Standards and Technology** (the "RCC Response"), RCC seeks both (i) to raise certain concerns respecting the cyber-security aspects of one particular network of special concern as an element of critical infrastructure and (ii) to contribute to the development of the Framework.

---

[1] The RFI may be found at 78 FR 13024 and https://federalregister.gov/a/2013-04413 and bears the following Docket Number 130208119-3119-01.

[2] The RFI defines "critical infrastructure" as having has the meaning given the term in 42 U.S.C. 5195c(e), "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

In the RCC Response, the following topics are examined:

- First:
    - The relationship between the Framework and national interoperable public safety broadband network envisioned by Title VI of the Middle Class Tax Relief and Job Creation Act of 2012 (that network, the "PSBN"; and that legislation, "Title VI");
    - The relationship between NIST and the development of proper cyber-security protection for the PSBN; and
    - The risks of failing to apply the Framework (and, perhaps, more specific mandatory standards in relation to cyber-security protection) to the PSBN; and
- Second: A proposed possible structure for the Cybersecurity Framework.

RCC's interest in the first topic derives from its more than thirty-year history of providing engineering consulting services in relation to public safety communications networks and systems and from RCC's particular interest and involvement in aspects of the development of the PSBN. On the first topic, it is the gravamen of the RCC Response that:

- The National Telecommunications and Information Administration ("NTIA") and the First Responder Network Authority ("FirstNet") should be included in the consultation process to be undertaken by NIST;
- Those agencies have responsibilities (as does NIST) in relation to the development of the PSBN;
- The PSBN clearly constitutes or, more accurately, will constitute critical infrastructure as defined in the RFI because the "the incapacity or destruction of [the PSBN] … would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters";
- The existing and yet-to-be developed public safety networks, data centers, databases, information systems, and applications to which the PSBN may ultimately connect directly constitute additional critical infrastructure with vulnerabilities to cyber-attacks if the PSBN is not secure;
- The PSBN will be substantially unique among elements of critical infrastructure because it will be both national critical infrastructure in its own right, and the PSBN will be

national critical infrastructure that should provide a central core of communications support for first responders addressing attacks upon other elements of critical infrastructure and their consequences, whether those attacks are of a cyber-warfare nature or a "kinetic" or physical nature;

- In the context of protection against cyber-attacks, the PSBN requires a very high level of attention that FirstNet has not to date provided;

- FirstNet appears to be proceeding with a much-criticized conceptual network architecture, which has its critics[3] and which does not sufficiently, if at all, reflect a concern for cyber-security despite the fact that it is generally recognized that cyber-security protections must be built into networks from their inception for functional and cost effectiveness[4];

- FirstNet appears to be principally concerned with rapidly rolling out the PSBN, and, while that view certainly has some merit, it is not at all consistent with a need to build cyber-security protective mechanisms into the network from the outset, particularly when some of those mechanisms may not currently exist because of the uniqueness of the PSBN in both its architecture and its user base;

- The conceptual architecture of FirstNet implies not only commercial user wireless access to mission critical networks and critical infrastructure but also potential physical access and vulnerabilities to infrastructure through shared facilities and backhaul;

- FirstNet has to date indicated a certain apparent indifference to the vulnerability of the PSBN to cyber-attacks despite the obligation of FirstNet under Title VI to "ensure the

[3] In this connection, see the responses to the NTIA NOI relating to that conceptual architecture, http://www.ntia.doc.gov/federal-register-notice/2012/comments-nationwide-interoperable-public-safety-broadband-network-noi, including, but not limited to, RCC Consultants, Inc., ***Notice of Inquiry National Telecommunications and Information Administration Docket No:*** *120928505-2505-01,* ***RIN:*** *0660-XC002* ***Development of the Nationwide Interoperable Public Safety Broadband Network, Response of RCC Consultants, Inc.*** (October 22, 2013), http://www.ntia.doc.gov/files/ntia/rcc_response_to_firstnet_noi_10142012.pdf.

[4] In this connection, consider the following: "Ensuring that the network architecture provides continuous systems security, including the ability to carry classified information, is essential, but could prove costly if added after network design is done. Security design and its continuously changing nature must be considered up front as a primary design element to control cost." (Emphasis supplied.) Textron Systems, Inc., *In Response to U.S. Department of Commerce, National Telecommunications and Information Administration, On Behalf of First Responder Network Agency, Notice of Inquiry* (November 8, 2013) (the "Textron Response"), http://www.ntia.doc.gov/files/ntia/textron_systems_firstnet_psbn_noi_final.pdf, p. 13; and "Security and prioritization requirements are vital to the success of the FNN and must be addressed from day one of the implementation of the FNN. In addition, resiliency against disasters and cyber attacks must be built into the system to preserve continuity of operation in extreme conditions." (Emphasis supplied.) Northrup Grumman Information Systems, Inc., *FirstNet Notice of Inquiry Response* (November 1, 2012) ("NG Response"), http://www.ntia.doc.gov/files/ntia/northrop_grumman_fnn-noi.pdf, p. 4, Table 1, #1

safety, security, and resiliency of the [PSBN], including requirements for protecting and monitoring the network to protect against cyberattack"[5];

- The criticality of the PSBN to the effective protection of critical infrastructure combined with the federal governmental nature of the PSBN (and the consequential absence of concerns regarding the imposition of federal standards upon the private sector[6]) suggest a more active federal role in cyber security standards-setting for the PSBN than would be applicable to private industry and further suggest that NIST develop cyber security standards for consideration for the PSBN that represent the minimum requirements applicable for that purpose;

- NIST has ample authority to undertake the role suggested by RCC both under generally applicable executive policy[7] and Title VI,[8] and there is recent precedent for an activist

[5] Section 6206(b)(2)(A)

[6] In this connection, see: *Principles for Federal Engagement in Standards Activities to Address National Priorities* (Executive Office of the President, Office of Management and Budget, United States Trade Representative, and Office of Science and Technology Policy, January 17, 2012).

[7] The more active federal governmental role is fully supported by the above-cited memorandum (*Principles for Federal Engagement in Standards Activities to Address National Priorities*), which states that "[i]n limited policy areas … where a national priority has been identified in stature, regulation, or Administration policy, active engagement or a convening role by the Federal Government to accelerate standards development and implementation …" The PSBN is a statutorily recognized national priority under Title VI and, subject only to the right of states and territories to "opt out" of the local radio access network ("RAN") proposed to be provided by FirstNet within their borders and build their own RANs within those borders, the PSBN is a federal undertaking by a federal agency.

[8] Section 6303, **Public safety wireless communications research and development**, of Title VI provides:

> (a) NIST directed research and development program.—From amounts made available from the Public Safety Trust Fund, the Director of NIST, in consultation with the Commission, the Secretary of Homeland Security, and the National Institute of Justice of the Department of Justice, as appropriate, shall conduct research and assist with the development of standards, technologies, and applications to advance wireless public safety communications.
>
> (b) Required activities.—In carrying out the requirement under subsection (a), the Director of NIST, in consultation with the First Responder Network Authority and the public safety advisory committee established under section 6205(a), shall—
>
> (1) document public safety wireless communications technical requirements;
>
> (2) accelerate the development of the capability for communications between currently deployed public safety narrowband systems and the nationwide public safety broadband network;
>
> (3) establish a research plan, and direct research, that addresses the wireless communications needs of public safety entities beyond what can be provided by the current generation of broadband technology;
>
> (4) accelerate the development of mission critical voice, including device-to-device "talkaround" capability over broadband networks, public safety prioritization, authentication capabilities, and

federal approach to matters affecting the surety and reliability of the facilities that support first responders[9];

> standard application programing interfaces for the nationwide public safety broadband network, if necessary and practical;
>
> (5) accelerate the development of communications technology and equipment that can facilitate the eventual migration of public safety narrowband communications to the nationwide public safety broadband network; and
>
> (6) convene working groups of relevant government and commercial parties to achieve the requirements in paragraphs (1) through (5). (Emphasis added.)

Section 6303(b)(6) is particularly relevant because of the obligation of FirstNet to consult regarding, among many other matters, with regional, State, tribal, and local jurisdictions regarding the distribution and expenditure of any amounts required to carry out the policies established under paragraph (1), including with regard to the … adequacy of hardening, security, reliability, and resiliency requirements; Section 6206 (c)(2)(A)(iv) of Title VI. NIST can, RCC believes, play an important role not only in the development of minimum cyber-security standards for the PSBN, but also in assuring that input is properly obtained from regional, State, tribal, and local jurisdictions regarding security requirements. That role could be particularly important because FirstNet has shown little enthusiasm for engaging in the required, broad consultation process and has demonstrated more interest in marketing its views to users and others (activities referred to by FirstNet as "outreach," which are fundamentally different from the consultation activities required by Title VI) than in obtaining the required input from users for the design of the PSBN.

[9] On March 20, 2013, the Federal Communications Commission (the "Commission") issued a release and a notice of proposed rule-making. The release, **FCC TAKES ACTION TO ENSURE RELIABILITY OF CALLS TO 9-1-1 DURING TIMES OF EMERGENCY; ADOPTS KEY RECOMMENDATIONS FROM INQUIRY INTO WIDESPREAD 9-1-1 FAILURES DURING 2012 DERECHO STORM**, states, in pertinent part:

> WASHINGTON, D.C. – The Federal Communications Commission today proposed action to improve the reliability and resiliency of America's 9-1-1 communications networks, especially during disasters, by ensuring that service providers implement vital best practices in network design, maintenance, and operation. The Commission also proposed amending its rules to clarify how service providers can more effectively and uniformly notify 9-1-1 call centers of communications outages and cooperate to restore service as quickly as possible.
>
> In a Notice of Proposed Rulemaking adopted today, the Commission moved forward to implement four key recommendations for strengthening 9-1-1 service made by the FCC's Public Safety and Homeland Security Bureau. The Bureau's recommendations, contained in a January 2013 report, resulted from an in-depth inquiry into the widespread 9-1-1service failures that occurred after a derecho storm hit portions of the Midwest and Mid-Atlantic in June 2012.
>
> A significant number of 9-1-1 systems and services were partially or completely down for several days after the derecho – from isolated breakdowns in Ohio, New Jersey, Maryland, and Indiana to systemic failures in northern Virginia and West Virginia. In all, 77 9-1-1 call centers serving more than 3.6 million people in these six states lost some degree of connectivity, including vital information on the location of 9-1-1 calls. Seventeen 9-1-1 call centers, mostly in northern Virginia and West Virginia, lost service completely, leaving more than 2 million residents unable to reach emergency services for varying periods of time.

Unlike hurricanes and superstorms, which are generally well-forecast, derechos are more like earthquakes, tornados, and man-made events for which there is little-to-no advance notice and opportunity to prepare. As a result, the derecho put a portion of the Nation's communications infrastructure to an unexpected test, revealing significant vulnerabilities in the design and maintenance of 9-1-1 networks. The Bureau found that most of the failures would have been avoided if the network providers that route calls to 9-1-1 call centers had fully implemented industry best practices and available industry guidance. …

The Commission put forth a range of possible approaches for implementing these recommendations, including:

- **Reporting** – where the Commission would require service providers to periodically report on the extent to which they are voluntarily implementing critical best practices or complying with standards established by advisory bodies or requirements established by the Commission;

- C**ertification** – where the Commission would require providers to certify periodically that their 9-1-1 network service and facilities meet specified criteria;

- **Reliability requirements** – where the Commission would specify minimum requirements for 9-1-1 communications reliability; and

- **Compliance reviews and inspections** conducted by the Commission to verify that 9-1-1 service providers are following certain practices or adhering to certain requirements.

The Commission also posed a range of questions regarding the extent to which 9-1-1 service providers implement existing best practices, the incentives most likely to ensure that they do so in the future, and the costs and benefits of ensuring that best practices are implemented in each area. Whatever approach is ultimately adopted must account for differences in service providers' networks and support the ongoing transition from today's legacy 9-1-1 system to a Next Generation 9-1-1 (NG9-1-1) system, the Commission said.

In addition, the Commission is considering clarifying its current rule that requires service providers to notify 9-1-1 call centers of significant communications outages. To provide service providers with greater specificity about their obligation, the proposed rule would require them to notify 9-1-1 call centers of outages immediately, by telephone and in writing via electronic means, with critical information.

Today's action builds on prior Commission efforts to ensure that the public has access to a reliable, state-of-the-art 9-1-1 communications system. Most notably, the Commission is working to promote the deployment of NG9-1-1, which offers greater resiliency during disasters and enables public safety responders to receive more information – text, photos, video, and data – to help them assess and respond to emergencies. The Commission has also taken action to spur the uniform availability of text-to-9-1-1, a major milestone in the transition to NG9-1-1. (Emphasis supplied.)

The willingness of the Commission to consider the imposition of "**Reliability requirements** – where the Commission would specify minimum requirements for 9-1-1 communications reliability"; and "**Compliance reviews and inspections** conducted by the Commission to verify that 9-1-1 service providers are following certain practices or adhering to certain requirements" surely reflects the need for an activist federal role in matters affecting communications bearing upon public safety, and the Cybersecurity of the PSBN is surely a matter that bears directly upon the effectiveness of public safety communications.

In this connection, see also: Federal Communications Commission, Notice of Proposed Rulemaking, *In the Matter of Improving 9-1-1 Reliability, PS Docket No. 13-75 and Reliability and Continuity of Communications Networks,*

- While RCC supports active NIST involvement in assuring the cyber-security of the PSBN, RCC is not unaware of the criticisms that have been expressed in relation to certain aspects of NIST's or the federal government's approach to cyber-security,[10] but still believes that NIST is the agency best positioned to work toward providing the basis for the protection of the PSBN from a cyber-security standpoint;

- In accordance with the provisions of the Federal Information Security Management Act ("FISMA"),[11] the Secretary of Commerce shall, on the basis of standards and guidelines developed by NIST, prescribe standards and guidelines pertaining to federal information systems and shall make standards compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of federal information systems;

- The exercise of the powers of the Secretary of Commerce under FISMA to make cyber-security standards developed for the PSBN by NIST would be entirely appropriate

---

Including Broadband Technologies, PS Docket No. 11-60 (March 20, 2013) and the Report of the Public Safety and Homeland Security Bureau, Federal Communications Commission, *Impact of the June 2012 Derecho on Communications Networks and Services, Report and Recommendations* (January 2013)

The Commission's March 20, 2013, notice refers to an earlier notice of inquiry as follows:

> Taking a broader look at network reliability, in 2011, the Commission released a *Notice of Inquiry* in this docket which sought comment on the reliability, resiliency, and continuity of our Nation's communications networks, including broadband technologies. Among other topics, we inquired about "the ability of communications networks to provide continuity of service during major emergencies, such as large-scale natural and man-made disasters."[9] The Commission also discussed a variety of actions it could take "to foster improved performance with respect to the reliability and continuity of operations." Observing that "access to communications services increasingly becomes a matter of life or death" during natural or human-caused disasters, the Commission emphasized that "[p]eople dialing 9-1-1, whether using legacy or broadband-based networks, must be able to reach emergency personnel for assistance." Through this proceeding, the Commission sought to develop a record aimed at strengthening communications networks and ensuring that emergency communications services are available when they are needed most. (Emphasis supplied; footnotes omitted.)

For the earlier inquiry, see: In the Matter of Reliability and Continuity of Communications Networks, Including Broadband Technologies, *et al*., *Notice of Inquiry*, PS Docket No. 11-60, *et al.*, 26 FCC Rcd 5614 (2011).

The Commission's finding that access to communications services increasingly becomes a matter of life or death during natural or human-caused disasters surely supports an activist approach to cyber-security for the PSBN, as cyber-attacks can result in "human-caused disasters" that, when made upon the PSBN could leave first responders without "access to communications services" at the very time that such access "increasingly becomes a matter of life or death."

[10] In this connection, see, by way of example: http://www.federalnewsradio.com/241/3264785/Report-offers-pathway-for-cyber-reform-without-legislation; http://fcw.com/articles/2013/03/27/cybersecurity-without-congress.aspx; and SafeGov, *Measuring What Matters: Reducing Risk by Rethinking How We Evaluate Cybersecurity* (March 2013), http://www.safegov.org/media/46155/measuring_what_matters_final.pdf

[11] The E-Government Act (P.L. 107-347) recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act is entitled the Federal Information Security Management Act (FISMA).

because (i) the PSBN constitutes a federal information system or will be so interconnected with federal information systems that the prescription of at least minimum information security requirements is necessary to improve the security of federal information and information systems;

- NIST should also consider coordination with the Federal Communications Commission regarding the cyber-security of the PSBN because the Commission has shown substantial leadership in addressing the matter of the reliability of public safety communications facilities[12];

- The criticality of cyber security to the effective availability of the PSBN is such that the matter of the protection of the PSBN against cyber-attacks must be addressed from the outset as an integral element of the design of the architecture of the PSBN because cyber-security cannot be addressed effectively after a network architecture has been adopted or implemented;

- FirstNet has adopted a network architecture that is potentially materially flawed from a cyber-security standpoint; and

- The efforts of NIST and the support of the Secretary of Commerce to assure that the PSBN is not vulnerable to cyber-attacks should include, but not be limited to, the efforts of NIST in relation to the Cybersecurity Framework.

RCC's interest in the second topic derives from RCC's hope that cyber-security standards and principles will be widely adopted across various sectors and applied rigorously to RCC's core area of expertise, *i.e.*, public safety communications, including, but not limited to, the PSBN. On the second topic, it is the gravamen of the RCC Response that the development of the Cybersecurity Framework would benefit from an overview provided by a proposed structure for the Framework.

[12] In this connection, again see: Federal Communications Commission, Notice of Proposed Rulemaking, *In the Matter of Improving 9-1-1 Reliability, PS Docket No. 13-75 and Reliability and Continuity of Communications Networks, Including Broadband Technologies, PS Docket No. 11-60* (March 20, 2013); the Report of the Public Safety and Homeland Security Bureau, Federal Communications Commission, *Impact of the June 2012 Derecho on Communications Networks and Services, Report and Recommendations* (January 2013); and In the Matter of Reliability and Continuity of Communications Networks, Including Broadband Technologies, *et al*., *Notice of Inquiry*, PS Docket No. 11-60, *et al*., 26 FCC Rcd 5614 (2011).

*II. **Background to the First Topic***

The RCC Response is not the first occasion on which RCC has expressed its concerns regarding the cyber-security aspects of the PSBN. In writing in relation to FirstNet-proposed conceptual architecture for the PSBN (the "FNNC"), RCC wrote:

> The vulnerability of US infrastructure, including, but not limited to, the electricity transmission grid and distribution systems, transportation facilities, financial networks, government networks, and telecommunications systems to cyber-attacks is an issue of the greatest national concern and has been highlighted recently by a speech by the secretary of Defence, Leon E. Panetta, who warned that the United States was facing the possibility of a "cyber-Pearl Harbor."[13] Under no circumstances can the vulnerability of the country to such an attack be increased by the approach to the design of the critical PSBN. The present state of thinking in relation to the FNNC does not consider protecting the PSBN from cyber-attack and other security breaches. The FNNC relies upon connections between and among (i) critical public safety facilities, (ii) public safety users, (iii) the PSBN, and (iv) as many as six commercial wireless carriers and satellite service providers. Those connections could provide cyber-attack pathways that may enable the penetration of any interconnected network or facility to expand to a penetration of some or all of those interconnected networks and facilities, including the PSBN and critical public safety facilities.[14]

RCC is hardly alone or first in expressing concern for the security of the PSBN.[15] That concern is, as has been indicated, directly reflected in Title VI and has been recognized by commenters that have devoted substantial resources to supporting the proper development of the PSBN.[16]

---

[13] See report of Secretary Panetta's speech in the *New York Times*, October 12, 2012. See also the report respecting a particular cyber-attack in the *Wall Street Journa*l, October 13, 2012.

[14] RCC Consultants, Inc., ***Notice of Inquiry National Telecommunications and Information Administration Docket No:*** *120928505-2505-01,* ***RIN:*** *0660-XC002* ***Development of the Nationwide Interoperable Public Safety Broadband Network, Response of RCC Consultants, Inc.*** (October 22, 2013), pp. 14-15

[15] RCC's concern in this respect extends to all mission critical information and communications infrastructure and applications which, as a result of their interconnection with the PSBN, may become vulnerable to cyber-attacks if the PSBN is not itself secure.

[16] On cyber threats to federal information infrastructure generally and related matters, see: Government Accountability Office ("GAO"), *Testimony before the Committee on Homeland Security, House of Representatives, Cybersecurity, Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats, Statement of Gregory C. Wilshusen, Director, Information Security Issue*s (GAO-10-834T) (2010); and GAO, Report to Congressional Requesters, Cybersecurity, Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative (GAO-10-338) (2010). See also: GAO, *Testimony before the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Government Affairs, U.S. Senate, Cybersecurity, A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges, Statement of Gregory C. Wilshusen, Director, Information Security Issue*s (GAO-13-462T) (2013); GAO, *Testimony Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, Cybersecurity, Threats Impacting the Nation* (GAO-12-666T)

Thus, for example, the National Public Safety Telecommunications Council ("NPSTC") has written in relation to the PSBN:

> Public safety processes sensitive information on a daily basis, which requires robust security measures to ensure integrity, confidentiality, privacy protection, and information assurance. A nationwide public safety broadband network would be an obvious target for cyber attack. This fact requires that extensive security measures be enacted to prevent attacks on the network to include but not be limited to cyber-attacks, physical site security, and denial of service.[17]

These concerns of RCC, NPSTC, and others are completely consistent with Executive Order 13636 of February 19, 2013:

> Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats.[18]

RCC is very much aware of the long history of NISTs contributions to the field of cyber-security[19] and is not alone in believing that NIST has a material contribution to make in relation

---

(2013); GAO, *Testimony Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, Cybersecurity, Continued Attention Needed to Protect Our Nation's Critical Infrastructure, Statement of Gregory C. Wilshusen, Director, Information Security Issue*s (GAO-11-865T) (2011); GAO, *Testimony Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives, Cybersecurity, Continued Attention Needed to Protect Our Nation's Critical Infrastructure and federal Information Systems, Statement of Gregory C. Wilshusen, Director, Information Security Issue*s (GAO-11-463T) (2011); and The White House, *Cyberspace Policy Review* (2009). See also: Clarke, Richard A., *et ano*., *Cyber War, The Next Threat to National Security and What to Do about It* (New York 2010); Brenner, Joel, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York 2011); Reverson, Derek S. (Editor), *Cyberspace and national Security: Threats, Opportunities, and Power in a Virtual World* (Washington, DC 2012); Rosenzweig, Paul, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (Santa Barbara 2013)

[17] NPSTC, ***Public Safety Broadband High-Level Launch Requirements***, Statement of Requirements for FirstNet Consideration (December 7, 2012) ("NPSTC Launch Requirements") See also: Likewise, Textron Systems has observed that "[s]ecurity planning is a key element of the PSBN. The PSBN will be used in scenarios where system security is of utmost importance to its functionality, especially as this national network for first responders is an ideal target for bad actors." Textron Response, p. 13

[18] Executive Order 13636—Improving Critical Infrastructure Cybersecurity" 78 FR 11739 (February 19, 2013) ("Executive Order 13636"), Section 1 For a discussion of Executive Order 13636, see: Fischer, Eric A., *et al*., Congressional Research Service, (CRS 7-5700, R42984) (2013).

[19] In this connection, RCC is, by way of examples, familiar with NIST, *DRAFT Security and Privacy Controls for Federal Information Systems and Organizations (Final Public Draft)* (NIST Special Publication 800-53 Rev 4) (2013); NIST, *DRAFT Electronic Authentication Guideline* (NIST Special Publication 800-63-2) (2013); NIST, *DRAFT Glossary of Key Information Security Terms* (NIST IR-7298 Rev. 2) (2012); NIST, *Notional Supply Chain Management Practices for Federal Information Systems* (NISTIR 7622) (2012); NIST, *Information Security: Guide for Conducting Risk Assessments* (2012); NIST, *DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices* (NIST Special Publication 800-164) (2012); NIST, *DRAFT Guide to Intrusion Detection and Prevention*

to the development and protection of the PSBN. Northrup Grumman Informations Systems, Inc., in its response to an NTIA notice of inquiry regarding a conceptual architecture proposed by FirstNet for the PSBN, wrote:

> We recommend that NIST identify areas of study related to network architecture that seek to define quickly the key FNN-ENC elements we have defined in our response including: security, identity management, and application delivery. … NIST has done an exemplary job with public safety broadband LTE interoperability testing … . Finally, NIST should continue their work with public safety, federal agencies, and industry in defining the technical requirements and standards for the [PSBN].[20]

III. The RFI, the Cybersecurity Framework, the PSBN, and the Suggested Role of NIST

RCC understands that, under Executive Order 13636, the Secretary of Commerce is given the responsibility to direct the Director of NIST to develop the Cybersecurity Framework, and the Department of Homeland Security, in coordination with sector-specific agencies, will then establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities. In RCC's view, there is no reason to make the Framework's applicability a matter of voluntary adoption by FirstNet. The possibilities of intrusion and compromise in an open application development environment all but guarantee they will occur. FirstNet is a federal agency, and such reluctance as there may be, under current administration policy, to the federal government's requiring the adoption of cyber-security protection standards by private enterprise owners of critical infrastructure has no application to the PSBN, which is a creation of federal legislation and federal funding.[21]

Systems (IDPS) (NIST Special Publication 800-94 Rev. 1) (2012); NIST, *DRAFT Guidelines for Managing and Securing Mobile Devices in the Enterprise* (NIST Special Publication 800-124 Rev 1) (2012); NIST, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (NIST Special Publication 800-137) (2011); NIST, *Information Security, Guide for Security-Focused Configuration Management of Information System*s (NIST Special Publication 800-128) (2011); NIST, *Guide to Securing WiMAX Wireless Communications* (NIST Special Publication 800-127) (2010); NIST, *Guidelines for Smart Grid Cyber Security* (NIST Interagency Report 7628) (2010); NIST, *Technical Guide to Information Security Testing and Assessment* (NIST Special Publication 800-115) (2008); NIST, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices* (NIST Special Publication 800-60 Rev. 1) (2008); NIST, Performance Measurement Guide for Information Security (NIST Special Publication 800-55 Rev. 1) (2008); NIST, *Computer Security: Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A* (NIST Special Publication 800-27 Rev A) (June 2004); NIST, *Building an Information Technology Security Awareness and Training Program* (NIST Special Publication 800-50) (2003); and NIST, *Generally Accepted Principles and Practices for Securing Information Technology Systems* (NIST Special Publication 800-14) (1996).

[20] NG Response, p. 25

[21] In this regard, consider:

> "It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and

The Department of Homeland Security ("DHS") is responsible for overseeing the protection of the dot gov (.gov) domain and is building a cyber security team to secure the nation's digital assets and protect against cyber threats to critical infrastructure and key resources. The Department of Defense ("DoD") is responsible for the dot mil (.mil) domain (and other military networks) and is pursuing the Defense Industrial Base Cyber Security Information Assurance ("DIB CS/IA") program to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

One problem RCC sees is that the PSBN may fall into a gap in federal efforts to protect critical infrastructure that belongs to the federal government. DHS and DoD may take decisions for certain critical federal assets, but not specifically the PSBN, and the PSBN would be treated improperly if, in relation to cyber security, that network was grouped with the critical infrastructure in private hands that is the subject of the RFO and Executive Order 13636. The Secretary of Commerce with the support of NIST has the power and capability to fill that gap pursuant to FISMA.

Another problem RCC sees is that the PSBN may be viewed as critical infrastructure as to which, as a matter of policy, incentives must or should be provided in order to adopt cyber-security protection measures.[22] There is no reason under FISMA or Executive Order 13636 for the PSBN to be so viewed.

In RCC's view, the PSBN should receive the attention in relation to cyber security in substantially the same as or even a greater degree than that which has been given the electric transmission grid and the information technology systems incorporated into the operations of the transmission grid, which are sometimes referred to as a "smart grid."[23] NIST is well aware of

---

> economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."

This quotation from Executive Order 13636, Section 1, makes clear that the restraint of that order is directed to critical infrastructure other than federal critical infrastructure.

[22] In this connection, see: NIST, Notice of Inquiry: Incentives To Adopt Improved Cybersecurity Practices (March 28, 2013)

[23] The Energy Policy Act of 2005 (Energy Policy Act) gave the Federal Energy Regulatory Commission ("FERC") authority to oversee the reliability of the bulk power system, including authority to approve mandatory cyber-security reliability standards.

The North American Electric Reliability Corporation (NERC), which FERC has certified as the nation's Electric Reliability Organization, developed the Critical Infrastructure Protection (CIP) cyber security reliability standards. On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP reliability standards, while concurrently directing NERC to develop significant modifications addressing specific concerns.

Additionally, the electric industry is incorporating information technology (IT) systems into its operations – commonly referred to as smart grid – as part of nationwide efforts to improve reliability and efficiency. There is concern that if these efforts are not implemented securely, the electric grid could become more vulnerable to attacks and loss of service. To address this concern, the Energy Independence and Security Act of 2007 (EISA) gave FERC

the concern that, if these efforts are not implemented securely, the electric grid could become more vulnerable to attacks and loss of service because the Energy Independence and Security Act of 2007 (EISA) gave FERC and NIST responsibilities related to coordinating the development and adoption of smart grid guidelines and standards. These facts reinforce for RCC its suggestions for an activist and expanded role for NIST in relation to cyber-security concerns for the PSBN not only because of NIST's general expertise in this area, but specifically because the work in protection of the electric transmission grip (and the smart grid) seem to have utility in relation to cyber-security protection for the PSBN.[24] FISMA offers a clear path especially as the PSBN falls jurisdictionally within the Department of Commerce together with NIST.

and the National Institute of Standards and Technology (NIST) responsibilities related to coordinating the development and adoption of smart grid guidelines and standards.

[24] FERC, Final Order, *Mandatory Reliability Standards for Critical Infrastructure Protection* (Docket No. RM06-22-000; Order No. 706, January 18, 2008) (122 FERC ¶ 61,040) sets forth eighth mandatory standards for critical infrastructure protection ("CIP"), all of which may provide a sound starting point for the development of standards applicable to the PSBN: (i) CIP-002-1 – Critical Cyber Asset Identification; (ii) CIP-003-1 – Security Management Controls; (iii) CIP-004-1 – Personnel and Training; (iv) CIP-005-1 – Electronic Security Perimeter(s); (v) CIP-006-1 – Physical Security of Critical Cyber Asset; (vi) CIP-007-1 – Systems Security Management; (vii) CIP-008-1 – Incident Reporting & Response Planning; and (viii) CIP-009-1 – Recovery Plans for Critical Cyber Assets.

IV. The Need for an Expanded Role for NIST in relation to the Cyber Security of the PSBN: The Apparent Indifference of FirstNet

In September 2012, FirstNet issued a presentation setting forth a concept for the PSBN or, what is referred to in that presentation as the "FirstNet Nationwide Network" or "FNN."[25] The FNN was the subject of a notice of inquiry issued by NTIA[26] to which many interested parties supplied comments, many quite critical of the FNN concept.[27] There has been no indication from FirstNet that the original version of the FNN concept has been in any material respect modified in relation to cyber-security issues or otherwise.

The FNN Presentation describes the roles and responsibilities of FirstNet,[28] but ominously no mention is made of FirstNet's responsibility under Title VI to "ensure the safety, security, and resiliency of the [PSBN], including requirements for protecting and monitoring the network to protect against cyberattack."[29]

The FNN Presentation grounds the FNN concept in a connection to the commercial wireless industry, describes the FNN concept substantially in commercial terms (*e.g.*, costs, revenues, sales volumes, subscribers, and product lines), and makes no reference to cyber-security or a requirement therefor.[30] The FNN concept of relying upon commercial wireless carriers has been criticized because of its consequences in terms of reliability and security,[31] but that criticism does not appear to have deterred FirstNet continuing reliance upon the FNN concept.

The essentially commercial orientation of the FNN concept (and the related indifference to cyber-security concerns) is reinforced by the presentation made public by FirstNet in relation to the development of applications and devices.[32] The Applications Presentation reflects a commercial rather than public safety approach with its references to addressable markets,

---

[25] Farrill, F. Craig, First Responders Network Authority, Presentation to the Board, FirstNet Nationwide Network (FNN) Proposal (September 25, 2012), http://www.ntia.doc.gov/files/ntia/publications/firstnet_fnn_presentation_09-25-2012_final.pdf (the "FNN Presentation")

[26] Notice of Inquiry on FirstNet Conceptual Network Architecture (October 1, 2012) http://www.ntia.doc.gov/files/ntia/publications/firstnet_noi_10042012.pdf

[27] Comments on Nationwide Interoperable Public Safety Broadband Network NOI, http://www.ntia.doc.gov/federal-register-notice/2012/comments-nationwide-interoperable-public-safety-broadband-network-noi

[28] FNN Presentation, pp. 5-6

[29] Section 6206(b)(2)(A)

[30] FNN Presentation, p. 7

[31] In this connection, see for example: "Although the FNN will and should leverage off of commercial networks and municipal assets to the greatest extent possible, these networks cannot inherently be relied upon to provide the needed security and reliability that is required for first responders. Instead, it will be incumbent on the national FNN architecture to provide centralized network security, cybersecurity, identity management and management of user priorities and quality of service at the outset. These functions must coordinate and interoperate with local capabilities." NG Response, pp. 1-2

[32] Applications and Devices Project, FirstNet Applications Services (December 11, 2012) (the "Applications Presentation"), http://www.ntia.doc.gov/files/ntia/publications/11dec12_firstnet_app_presentation_-_final.pdf

monetizing applications, developer mindshare and economics, applications ecosystems, MasterCard, and VISA.[33] Security and authentication are mentioned, not discussed, and placed on a par with payment and settlement.[34] The "[h]igh level application network architecture" includes multiple connections to the public Internet from the PSBN, state and local networks, state and local applications and data a FirstNet application server, a FirstNet API/data gateway, and agency databases.[35] No serious consideration is given to a security perimeter for the PSBN or to mediating and controlling public safety user connections to databases through the networks of the agencies for which they work. The Applications Presentation appears to assume that public safety user should or will be given public Internet access even though the prevailing practice in relation to public safety trunked radio systems is to restrict generally the access of users to the public switched telephone network. It seems highly unlikely that operational considerations will permit, if they can prevent, public safety users' general access to the public Internet. The Applications Presentation, which appears to contemplate the development of applications "available to the general public,"[36] seems to assume commercial users on the PSBN for whom unlimited internet access is an important consideration.

The apparent casualness of FirstNet's approach to applications security surely suggests that an agency with greater expertise in cyber-security should take a leading role in protecting the PSBN in this respect. RCC is not alone in its confidence in NIST for that role.[37] FirstNet

[33] Application Presentation, pp. 2 and 4
[34] Application Presentation, p. 6
[35] Applications Presentation, p. 5
[36] Applications Presentation, p. 7
[37] "When an FNN user downloads an application from a hosted environment, he/she needs assurances that the application will function as advertised and that the application does not contain any malicious code that will either impede their public safety mission or compromise the network and data integrity as the application is utilized to provide its requisite functionality. There must be a process in place where applications are submitted to a Certification Authority for verification and approval prior to delivery to the FNN user community. This approval process ensures both consistent quality of application and that applications do not contain harmful code that would, at best degrade handset performance and at worst, compromise the network and data integrity of the FNN at critical moments potentially affecting both the safety of the public and the public safety professional.

"Finally, application developers need to be given clear guidance on what network services are available from FirstNet so that they can develop the necessary applications to meet mission functions. This is best done by implementing open and standard protocols whenever possible but that are managed and monitored by an independent, respected, integrity-driven organization. It is our strong position that the NIST should be this authority. By taking on this mission, NIST should set standards for code quality to include:

- Ensure no malicious code is contained within an application
- Ensure that an application does not significantly reduce battery life of a device
- Ensure that applications are free from memory leaks that could degrade overall performance
- Ensure that applications only use approved APIs and library calls
- Ensure required network resources are used properly via proper QoS integration
- Ensure applications do not put unneeded strain on network resources and services." (Emphasis supplied.) NG Response, p. 23

"Applications and their developers need to understand their specific security requirements in terms of confidentiality, integrity, and availability with respect to the specific mission requirements that the application is

shows no awareness of the many reference available on the Internet to the ease of hacking into or jamming LTE as well the vulnerability of COTS subscriber devices. Thought-of-as-protected phones can be enabled for LTE access without intervention by or knowledge of a wireless carrier.[38] If an active and smart hacker community that spans the globe freely disseminates this kind of information, focused cyber-terrorist may take advantage of not only vulnerabilities of a network, but also those of the subscriber devices to access a network to cripple network capacity on a site or a group of sites.[39] The information available from FirstNet regarding the FNN concept includes no recognition of these concerns and certainly no effort to address them.

The FNN Presentation asserts that the FNN concept which is to "Create a Diverse Nationwide Network with Multiple Wireless Networks and Systems" has, as one of its advantages "Higher reliability."[40] Putting aside the facts that commercial networks have not been consistently reliable[41] and that their reliability characteristics are not entirely independent because of reliance upon certain facilities (*e.g.*, towers) in common, reliability is not meaningful without a cyber-security component that the FNN concept does not address.[42]

---

fulfilling. Many of these can be published by NIST in an interface document for use by the development community. This document should contain the core functions of defining requirements around ensuring the data the application is sending and receiving is getting to the appropriate, authorized recipients, can be trusted when it arrives, and that can be secured from access by others. There will be great challenges to meet these requirements but by no means can they be trivialized and unequivocally must be recognized and respected. The more security requirements FNN can support, the easier it is for application developers; however, it is unreasonable to have FNN support all required security features as use of these applications will be both on the FNN and, through roaming agreements, commercial systems. This again requires that the applications are fully verified, vetted, and certified to ensure their security posture is maintained in a mixed access environment. NIST, with proper direction, support, and funding, will be uniquely suited to support this mission. Further, NIST must be given the appropriate authority to both grant and deny the publishing of applications to the FNN hosted environment." (Emphasis supplied.) NG Response, p.24

[38] See: http://techcrunch.com/2012/11/23/how-to-enable-4g-lte-on-the-google-nexus-4/.

[39] See: http://www.techspot.com/news/50817-inexpensive-jammers-can-block-4g-lte-across-entire-cities.html.

[40] FNN Presentation, p. 8

[41] "Public Safety has a well-understood but poor quality of experience on commercial networks during times of disaster and other incidents that create high network demand. Over the past several years, concepts like priority and quality of service have been described to Public Safety as methods to improve their quality of experience on either a commercial or private network. In our experience, Public Safety may require a more robust implementation of Quality of Service than currently implemented on commercial carrier networks due to the extreme conditions that this network must continue to function under." Comments of Nokia Siemens Networks US LLC [to NTIA Notice of Inquiry] (the "NS Comments"), http://www.ntia.doc.gov/files/ntia/nokia_siemens_networks_comments_11-08-12.pdf, p. 19

[42] "The interests of the public safety community are best served by approaching the security requirements of the FNN in a holistic manner that addresses public safety's fundamental mission of protecting property and saving lives. As a case in point, public safety first responders depend on the 24x7 availability of their communications network to carry out their mission; inextricably linking reliability and security to the public safety networks. Weak and compromised network security undoubtedly reduces reliability and hence, availability. Without the proper security measures in place, no amount of reliability features, such as site hardening and backup power, can assure the highest degree of availability required of the public safety communications networks." NG Response, p. 5

The FNN Presentation asserts that a stand-alone PSBN would have "Lower Reliability,"[43] but this point is unproven from either a physical reliability standpoint or a cyber-security standpoint. On balance, public safety communications networks have proven to be more reliable from a physical standpoint than commercial wireless networks, and a stand-alone PSBN could have greater security from cyber-attacks than a network of network because the connection between the PSBN and the public Internet (the central pathway for cyber-attacks[44]) could be more effectively secured in the case of a stand-alone PSBN. [45]

---

[43] FNN Presentation, p. 9

[44] "A Public Safety network faces a different class of threats than commercial networks due to the critical nature of its subscriber base. As commercial use of this network is not envisioned, Nokia Siemens Networks encourages the FirstNet Board to fully segregate and firewall the network from as many outside influences as possible. NS Comments, p. 14

[45] "The FNN concept, as described in the FNN Presentation (pp. 11 and 15-19) relies upon connections between and among (i) critical public safety facilities, (ii) public safety users, (iii) the PSBN, and (iv) as many as six commercial wireless carriers and satellite service providers. Those connections could provide cyber-attack pathways that may enable the penetration of any interconnected network or facility to expand to a penetration of some or all of those interconnected networks and facilities, including the PSBN and critical public safety facilities." RCC Consultants, Inc., ***Notice of Inquiry National Telecommunications and Information Administration Docket No:*** *120928505-2505-01,* ***RIN:*** *0660-XC002* ***Development of the Nationwide Interoperable Public Safety Broadband Network, Response of RCC Consultants, Inc.*** (October 22, 2013), pp. 14-15

In this connection, see: "Nokia Siemens Networks believes that "Securing the Radio Access Network (RAN)" consists of three very distinct and critical components that should be part of a minimum security specification for FirstNet: User Access Security, Transport Security, and Trusted Environment (found internal to the eNodeB). All three of these components are required to reach a minimum acceptable level of security. Properly implemented transport security includes support of PKI, secure device identity (found internal to the eNodeB), operator identity management (PKI), IPSec, management protocols that are secure and secure file transfer for the management planes, and firewalls. Secure Device identity is critical in protecting from such issues as cloning and actual radio infrastructure. Thus minimizing risks by requiring authenticated and integrity protected code (Signed Software) and ensuring a process that ensures radios can only boot in a secure boot mode and are booting genuine and verified vendor code would need to be a minimal requirement. The carrier networks do not implement all of the above components uniformly on existing infrastructures. For example, some networks may lack:

- A single PKI Infrastructure in place managing operator identity and devices.
- A uniform transport security implementation between eNodeB interfaces and core network (Security Gateways) for a traffic plane.
- A system in place to ensure integrity of code on radio units, that those radios will only boot in protected mode, and that the radios allowed on the network are only those authenticated radios.

A lack of appropriate levels of security in the architecture of FirstNet puts FirstNet and its user community of first responders at risk of eavesdropping (e.g. , Foreign Nation Intelligence Units), unauthorized access of sensitive first responder data (e.g., Criminal Elements) or worse, infrastructure attacks by terrorist or other elements that could result in failure of key network components and a loss of use of the network by first responders at a critical time (e.g., during a terrorist attack). Nokia Siemens Networks recommends that FirstNet develop strong security specifications in the short term that address, at a minimum, User Access, Transport and Trusted Environment Security in a manner that is consistent with industry groups (e.g., 3GPP) and U.S. Government standards being currently developed within the Department of Defense (DoD) and apply those specifications to any decisions taken with regard to the architecture taken by FirstNet. Further elaboration of these points is available in a document submitted by Nokia Siemens Networks to the Technical Advisory Board for First Responder Interoperability at the Federal Communications Commission (FCC). NS Comments, pp. 20-22 (Emphasis supplied.) [The references to "PKI" are to "Public Key Infrastructure," an aspect of cryptography, which in relation to LTE is defined in 3GPP *3GPP TS 33.310, Universal Mobile Telecommunications System (UMTS); LTE; Network Domain Security (NDS); Authentication Framework (AF)* (Version 9.5.0 Release 9).]

The FNN Presentation claims that the FNN concept "achieves the major aspects of the desired nationwide wireless network," but, apparently, in FirstNet's view, protection against cyber-attacks is not a "major aspects of the desired nationwide wireless network," as cyber-security is unmentioned.

The FNN Presentation claims that the FNN concept "Solves Several Critical Issues,"[46] but cyber-security is not among those "critical issues." In summarizing the benefits of the FNN concept, the FNN Presentation makes no reference to cyber-security.[47]

Given "the absolute certainty that the FNN will be a high profile target" and the consequent "imperative that its components and interfaces must be protected, monitored, and threats identified and eliminated in real time,"[48] the lack of concern on the part of FirstNet in relation to the cyber-security of the PSBN is inexplicable and alarming and, frankly, dangerous.

The lack of concern on the part of FirstNet in relation to the cyber-security of the PSBN is all the more inexplicable, alarming, and dangerous given the fact that, in May 2012, the Technical Advisory Board for First Responder Interoperability (the "TAB") published the final version of its recommended minimum technical standards,[49] which included substantial substantive requirements and recommendations in relation to security[50] and expressly recognized the "duty of FirstNet … to ensure the safety, security, and resiliency of the NPSBN, including protecting and monitoring the network against cyber attack."[51]

On this point, see also: "As a dominant global broadband wireless standard, LTE has been identified as the advanced communications platform for establishing a truly interoperable, highly scalable and cost-efficient nationwide public safety broadband network. However, the use of open and globally deployed standards, such as Internet Protocol (IP) that forms the core of the LTE-based public safety broadband wireless networks, considerably increases the vulnerability of these networks to malicious attacks, further underscoring the need for robust security mechanisms to protect these networks. The proof lies in the ever increasing number and sophistication of cyber attacks on ubiquitous IP-based technologies. Equally significant, the requirements of commercial carriers to secure their wireless networks and user communications may not be as stringent as those required by public safety. The implementation of LTE technology over these networks will not address the security and reliability requirements of public safety emergency communications; hence, the need to integrate additional security and identity capabilities. These features include: network domain security, user domain security and application domain security. Each of these contributes to critical aspects of end-to-end security and, if not implemented properly, may expose the network and public safety users to disruptive and malicious cyber attacks. Even with these additional features, user information is protected only within the domain of the LTE network and not end-to-end from the user device to the public safety network operations and data center. As discussed earlier, additional security solutions would need to be integrated with the LTE technology to enable end-to-end secure communications that complies with the security requirements of public safety communications." NG Response, pp. 5-6

[46] FNN Presentation, p. 20

[47] FNN Presentation, p. 21

[48] NG Response, p. 8

[49] TAB, *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Interoperable Public Safety Broadband Network: Final Report* (May 22, 2012) (the "TAB Report")

[50] TAB Report, Section 4.8, Security

[51] TAB Report, p. 79

The TAB Report, which in relation to cyber-security relies heavily upon NIST's work in that field,[52] adopts NIST's early recommendation of a layered approach to cyber security.[53] Most critically in the context of this RCC Response, the TAB Report recognizes the inadequacy of the required cyber-security standards applicable to commercial wireless LTE networks.

> Evolution of the cyber security architecture warrants special attention. Given the prolific level of deployment of LTE on a worldwide basis, this technology standard will experience unprecedented levels of cyber threats. Cyber threats that are successful against commercial LTE networks may pose a direct threat on the cyber security of the NPBSN, particularly if the NPSBN is implemented with the same vulnerabilities that enabled successful attacks on commercial networks.[54] Given the NPSBN's mission, it is prudent to expect that evolution of cyber threats will occur at a faster pace than evolution of 3GPP[55] and other standards used in the NPSBN. This is evidenced in commercial markets by the rapid pace at which software vendors distribute security patches compared to the much slower pace at which standards are published and put into practice. …[56]
>
> Due to the expected threat profile that the NPSBN will be faced with …, the Interoperability Board recommends that Intra-Domain security controls that are considered optional by 3GPP be required for the NPSBN network deployment. …[57]

None of the many recommendations of the TAB Report seem to be reflected in the FNN concept, which, in certain respects, appears to disregard those recommendations and to so integrate the PSBN with the networks of commercial wireless carriers that the vulnerabilities of those networks seem assuredly imported into the PSBN if implemented in accordance with the FNN concept. These conclusions are all the more surprising given that the TAB Report in its final form had been available for six months before the public announcement of the FNN concept. While the TAB Report may not be binding upon FirstNet, it does not appear that Section 6206, which established the TAB and required the TAB Report and its approval by the FCC, intended that the TAB Report be ignored by FirstNet.

The issuance by NPSTC in December 2012 of the NPSTC Launch Requirements[58] does not appear to have caused reconsideration by FirstNet of the vulnerability of the PSBN if

---

[52] TAB Report, pp. 79 and 80
[53] TAB Report, p. 80
[54] This warning is of the greatest importance given the commercial wireless network dependencies of the FNN concept. This issue may be greater than dependencies because of the intended interconnections between commercial wireless networks and the PSBN under the FNN concept.
[55] For the 3GPP, see: http://www.3gpp.org. The work of 3GPP in relation to LTE security standards is included in the 3GPP's 33 Series standards, for which, see: http://www.3gpp.org/ftp/Specs/html-info/33-series.htm.
[56] TAB Report, p. 81
[57] TAB Report, p. 86
[58] NPSTC, ***Public Safety Broadband High-Level Launch Requirements***, *Statement of Requirements for FirstNet* Consideration (December 7, 2012) Earlier drafts of that report were available to FirstNet before the issuance of the FNN Presentation.

deployed pursuant to the FNN concept despite the recommendations and concerns reflected therein.[59]

The NPSTC Launch Requirements recognize that: "No single interface to the NPSBN will present a greater risk to the operation of the network then [sic] the connections to the public Internet."[60] In Table 98, Internet Access Service Monitoring Requirements,[61] the NPSTC Launch Requirements set forth four specific requirements:

1. The NPSBN SHALL monitor and protect against threats at any provided Internet access points within the NPSBN trusted zone whether the access is for internal NPSBN users or for providing access to mobile NPSBN-Us.[62]

2. The NPSBN SHALL prohibit the connection or use by any device, server, or component within the trusted zone of an unrestricted or unmonitored public Internet access connection.

3. The NPSBN SHALL allow PSENs[63] to provide Internet access to their users as long as the boundary protection guidelines between the NPSBN and the PSEN are followed and adhered to.

4. The NPSBN SHALL have the ability to restrict or even terminate the public Internet connections to the trusted network if it is deemed that the public Internet has become a threat to operations.

The FNN concept does not appear to incorporate any of the foregoing safeguards, and, moreover, the FNN concept as heretofore described by FirstNet may simply be inconsistent with the implementation of those safeguards because of (i) the dependencies under the FNN concept between the PSBN and wireless carrier networks, which are connected to the public Internet and generally provide unmonitored and unrestricted access thereto under the FNN concept and (ii) the connections between the PSBN and the public Internet contemplated by the FNN concept.

The FNN concept may reasonably be viewed as a threat to the cyber-security of the PSBN, and that fact, coupled with FirstNet's undaunted and continuing commitment to the FNN concept, is the basis for RCC's concern respecting this aspect of the PSBN and RCC's appeal to NIST to bring cyber-security sensitivity to the PSBN that FirstNet seems so plainly unable to provide or is so uninterested in providing.

[59] NPSTC Launch Requirements, Section 5
[60] NPSTC Launch Requirements, Section 5.11. p. 94
[61] NPSTC Launch Requirements, Section 5.11, p. 94
[62] Nationwide Public Safety Broadband Network Users
[63] Public safety Enterprise Networks

V. A Possible Structure of the Cybersecurity Framework and the Centrality of Connections between Critical Infrastructure and the Public Internet

The RFI sets forth a number of questions regarding the major areas about which NIST seeks comment. RCC believes that all of those questions probe relevant and useful areas of inquiry. RCC also believes that the questions leave certain gaps that might be useful to fill in order that the comprehensiveness of the Cybersecurity Framework is assured.

In RCC's view, one effective approach to avoid gaps in inquiry is to provide a possible structure for the Framework for consideration because comprehensiveness may be more easily considered in the context of a structure than in the context of a range of particular questions. For that reason, RCC offers a possible structure for the Cybersecurity Framework. However, RCC well and truly recognizes that there are many knowledgeable and experienced commentators who will have different and quite possibly better ideas on structuring the Framework.

RCC genuinely hopes that RCC's proposed structure will serve, if not necessarily as a model for final structure of the Framework, as a stimulus for discussion and as a demonstration of the utility of early consideration of the structure of the Framework. RCC claims little by way of originality in relation to the structure proposed for the development of which RCC has drawn freely upon numerous sources, including, but not limited to, the RFI and the range of subjects probed by the questions therein provided as well as NIST's early and pioneering work on cyber-security.[64] RCC's contribution, if any, rests in its effort to offer a reasonably comprehensive structure, which incorporates contributions from many sources and which may serve to organize thinking in relation to the development of the Cybersecurity Framework and its related effort to provide a preliminary bibliography for a large majority of the subject matters of the sections of the proposed structure.

RCC's proposed structure for the Cybersecurity Framework follows and includes an element-by-element description that includes, in certain instances, information responsive to particular questions posed by NIST in the RFI as well as references.

A. Sections of General Application (Cross-Sector Considerations)

(1) Background Matters

The Definitions Used in the Cybersecurity Framework: This section would provide a comprehensive glossary of cyber-security terms used in the Cybersecurity Framework and

[64] For example, NIST, *Computer Security: Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A* (NIST Special Publication 800-27 Rev A) (June 2004); and NIST, *Generally Accepted Principles and Practices for Securing Information Technology Systems* (NIST Special Publication 800-14) (1996)

otherwise. A clear definitional structure would provide a useful foundation for the Framework and reduce the potential for vagueness and ambiguity. There are useful places to start, including ISO/IEC 27000:2012,[65] which provides an overview and the vocabulary of information security management systems, Congressional Research Service R42507, which provides a list of glossaries of cyber-security terms,[66] and Australian Government Information Security Manual: Controls,[67] which contains glossaries of abbreviations and terms. These sources are, of course, in addition to NIST's own work on cyber-security and defining relevant terms[68] and various other sources.[69]

Current Cyber-Security Sources and Methods and Their Utility:

The section will provide information responsive to certain of the questions posed by NIST[70] and is intended to serve as a repository of information provided in responses to the RFI. This section may or may not survive the final form of the Cybersecurity Framework because the Framework may consist solely of recommended standards and policies and may not encompass all standards and policies to which consideration was given.

Significant bibliographical compilations regarding cyber-security are available.[71] NIST itself has provided a useful introduction to cyber-security standards.[72] In addition, there are

[65] International Standards Organization/International Electrotechnical Commission ("ISO/IEC") 27000 , Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary (Second Edition) (2012) See also: ISO/IEC 27031:2011 which describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity. See also: ISO/IEC 17000, Conformity assessment -- Vocabulary and general principles (First Edition) (2004).

[66] Tehan, Rita, Congressional Research Service, *Cybersecurity: Authoritative Reports and Resources* (CRS 7-7500, R42507) (2013), Table 16. Glossaries of Cybersecurity terms

[67] *Australian Government Information Security Manual: Controls* (2012)

[68] NIST, *DRAFT Glossary of Key Information Security Terms* (NIST IR-7298 Rev. 2) (2012); NIST, *Computer Security: Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A* (NIST Special Publication 800-27 Rev A) (June 2004), and, particularly, Appendix A, Definitions; and NIST, *Information Security: Guide for Conducting Risk Assessments* (2012), Appendix B, Glossary.

[69] Klimburg, Alexander (Editor), *National Cyber Security Framework Manual* (NATO Cooperative Defence Centre of Excellence Tallinn 2012), Section 1.2, Cyber Terms and Definitions; and [69] National Security Agency, Information Assurance Solutions, Technical Directors, *Information Assurance Technical Framework* (Release 3.1) (2002), Appendix B, Glossary

[70] The RFI asks, *inter alia*, what standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels and seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

[71] Those compilations include: Tehan, Rita, Congressional Research Service, *Cybersecurity: Authoritative Reports and Resources* (CRS 7-7500, R42507) (2013), especially Tables 17-31; *Australian Government Information Security Manual: Controls* (2012), pp. 296-298; and GAO, *Report to Congressional Requesters, Critical Infrastructure Protection, Cybersecurity Guidance Is Available, but More Can Be Done to Promote its Use* (GAO-12-92) (2011), particularly for industry-specific standards. See also, NIST, *Notional Supply Chain Management Practices for Federal Information Systems* (NISTIR 7622) (2012), Appendix C

certain bodies of work that are interesting and, in certain respects, comprehensive and offer their own structures for a cyber-security framework.[73] These include:

- *Australian Government Information Security Manual* in three parts (the "AGISM"):
    - *Australian Government Information Security Manual: Executive Companion* (2012);
    - *Australian Government Information Security Manual: Principles* (2012); and
    - *Australian Government Information Security Manual: Controls* (2012);
- The NSA Information Assurance Technical Framework[74];
- The NATO National Cyber Security Framework Manual[75];
- The ISO/IEC 2700 Series Standards:
    - ISO/IEC 27001:2005,[76] which specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks and the requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof;
    - ISO/IEC 27002:2005,[77] which establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization and outlines objectives and controls in the

[72] Scarfone, Karen, Benigni, Dan, and Grance, Tim, *Cyber Security Standards* (2009), http://www.nist.gov/customcf/get_pdf.cfm?pub_id=152153

[73] These authorities are among those upon which RCC has drawn in the development of its proposed structure for the Cybersecurity Framework. See also: Andress, Jason, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (2011); Goodrich, Michael, *Introduction to Computer Security* (2010); Killmeyer, Jan, *Information Security Architecture: An Integrated Approach to Security in the Organization* (Second Edition) (2006); and Sherwood, John, *Enterprise Security Architecture: A Business-Driven Approach* (2005)

[74] National Security Agency, Information Assurance Solutions, Technical Directors, *Information Assurance Technical Framework* (Release 3.1) (2002)

[75] Klimburg, Alexander (Editor), *National Cyber Security Framework Manual* (NATO Cooperative Defence Centre of Excellence Tallinn 2012)

[76] ISO/IEC 27001, Information technology - Security techniques - Information security management systems – Requirements (First Edition) (2005)

[77] ISO/IEC 27002, Information technology -- Security techniques -- Code of practice for information security management (First Edition) (2005)

following areas of information security management: security policy; organization of information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition, development and maintenance; information security incident management; business continuity management; and compliance;

- ISO/IEC 27003:2010,[78] which focuses on the design and implementation of an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2005 and describes the process of ISMS specification and design from inception to the production of implementation plans;

- ISO/IEC 27004:2009,[79] which provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001;

- ISO/IEC 27005:2011,[80] which provides guidelines for information security risk management and is designed to assist the satisfactory implementation of information security based on a risk management approach;

- ISO/IEC 27006:2011,[81] which specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021:2011[82] and ISO/IEC 27001:2005;

- ISO/IEC 27007:2011,[83] which provides guidance on managing an information security management system ("ISMS") audit program, on conducting the audits, and on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011:2011[84];

[78]ISO/IEC 2700, Information technology -- Security techniques -- Information security management system implementation guidance (First Edition) (2010)
[79] ISO/IEC 27004, Information technology -- Security techniques -- Information security management – Measurement (First Edition) (2009)
[80] ISO/IEC 27005, Information technology - Security techniques - Information security risk management (Second Edition) (2011)
[81] ISO/IEC 27006, Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems (Second Edition) (2011)
[82] ISO/IEC 17021Conformity assessment -- Requirements for bodies providing audit and certification of management systems (Second Edition) (2011)
[83] ISO/IEC 27007, Information technology -- Security techniques -- Guidelines for information security management systems auditing (First Edition) (2011)
[84] ISO 19011, Guidelines for auditing management systems (2011)

- ISO/IEC TR 27008:2011,[85] which provides guidance on reviewing the implementation and operation of controls, including technical compliance checking of information system controls, in compliance with an organization's established information security standards;

- ISO/IEC 27010:2012,[86] which provides guidelines in addition to guidance given in the ISO/IEC 27000 family of standards for implementing information security management within information sharing communities and provides controls and guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organizational and inter-sector communications;

- ISO/IEC 27031:2011,[87] which describes the concepts and principles of information and communication technology ("ICT") readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity;

- ISO/IEC 27032:2012,[88] which provides guidance for improving the state of cyber-security and explains the unique aspects of cyber-security and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection ("CIIP");

- ISO/IEC 27033-1:2009,[89] which provides an overview of network security and related definitions and defines and describes the concepts associated with, and provides management guidance on, network security, which, as defined, includes the security of devices, security of management activities related to the devices, applications/services and end-users, and the security of the information being transferred across the communication links;

[85] ISO/IEC TR 27008, Information technology -- Security techniques -- Guidelines for auditors on information security controls (2012)
[86] ISO/IEC 27010:2012, Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications (First Edition) (2012)
[87] ISO/IEC 27031, Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity (First Edition) (2011)
[88] ISO/IEC 27032, Information technology -- Security techniques -- Guidelines for cybersecurity (first edition) (2012)
[89] ISO/IEC 27033-1, Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts (First edition) (2009)

- ISO/IEC 27033-2:2012,[90] which provides guidelines for organizations to plan, design, implement and document network security;

- ISO/IEC 27033-3:2010,[91] which describes the threats, design techniques, and control issues associated with reference network scenarios and provides detailed guidance on the security threats and the security design techniques and controls required to mitigate the associated risks; and

- ISO/IEC 27035:2011,[92] which provides a structured and planned approach to detect, report and assess information security incidents; respond to and manage information security incidents; detect, assess and manage information security vulnerabilities; and continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities; and

- The IEC 62443 Series Standards:

  - IEC/TS 62443-1-1:2009,[93] which is a technical specification that defines the terminology, concepts and models for Industrial Automation and Control Systems ("IACS") security;

  - IEC 62443-2-1:2010,[94] which defines the elements necessary to establish a cyber security management system ("CSMS") for industrial automation and control systems ("IACS") and provides guidance on how to develop those elements;

  - IEC/TR 62443-3-1:2009,[95] which provides a current assessment of various cyber-security tools, mitigation counter-measures, and technologies that may effectively apply to the modern electronically based IACSs regulating and monitoring numerous industries and critical infrastructures and describes several categories of control system-centric cyber-security technologies, the types of products available in those categories, the pros and cons of using those products in the automated

[90] ISO/IEC 27033-2, Information technology -- Security techniques -- Network security -- Part 2: Guidelines for the design and implementation of network security (First edition) (2012)
[91] ISO/IEC 27033-3, Information technology -- Security techniques -- Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues (First Edition) (2010)
[92] ISO/IEC 27035, Information technology -- Security techniques -- Information security incident management (First Edition) (2011)
[93] IEC/TS 62443-1-1, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models (First Edition) (2009)
[94] IEC 62443-2-1, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program (First Edition) (2010)
[95] IEC/TR 62443-3-1, Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems (First Edition) (2009)

IACS environments relative to the expected threats and known cyber vulnerabilities, and preliminary recommendations and guidance for using these cyber-security technology products and/or countermeasures; and

- IEC/PAS 62443-3:2008,[96] which establishes a framework for securing information and communication technology aspects of industrial process measurement and control systems including its networks and devices on those networks and provides guidance on a plant's operational security requirements.

- International Telecommunication Union ("ITU"):

  - 800 Series Standards on Security for Open Systems Interconnection;

  - 1000 Series Standards on Information and Network Security;

  - 1100 and 1300 Series Standards on Secure Applications and Services; and

  - 1200 and 1500 Series Standards on Cyberspace Security and Cybersecurity Information Exchange.

Legal and Regulatory Requirements: This section would review the current legal, regulatory, and regulatory reporting requirements in the United States (*e.g.*, local, state, national, and other) for organizations relating to Cybersecurity and would set forth standards and practices in relation to compliance with such legal and regulatory obligations.[97] For information regarding federal laws relating to cyber-security, certain publications of the Congressional Research Service may prove helpful.[98]

Privacy and Civil Liberties Issues: This section would address the many privacy and civil liberties issues for which cyber-security standards and practices have implications and

[96] IEC/PAS 62443-3, Security for industrial process measurement and control - Network and system security (First Edition) (2008)

[97] In this connection, see, for example: Williams, Barry L., *Information Security Policy Development for Compliance* (2013)

[98] Doyle, Charles, Congressional Research Service, *Cybersecurity: Cyber Crime Protection Security Act (S. 2111, 112th Congress) – A Legal Analysis* (CRS 7-5700, R42403) (2013); and Fischer, Eric A., Congressional Research Service, *Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions* (CRS 7-5700, R42114) (2012) See also: Tehan, Rita, Congressional Research Service, *Cybersecurity: Authoritative Reports and Resources* (CRS 7-7500, R42507) (2013); Finklea, Kristin M. *et ano.*, Congressional Research Service, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement* (CRS 7-5700, R43547 (2012); Liu, Edward C. *et al*., Congressional Research Service, *Cybersecurity: Selected Legal Issues* (CRS 7-5700, R42409) (2012); and Grama, Joanna Lyn, *Legal Issues in Information Systems* (2010).

would set forth standards and practices. This issue is addressed in a number of reports and studies.[99]

(2) Threats, Targets, and Dependencies

Threat/Risk Assessment and Management for Critical Infrastructure: This section would address standards, practices, and processes for the identification and assessment of cyber-security threats, for the identification of targets of such threats, and the dependencies of elements of critical infrastructure upon one another where those dependencies expand the range of threats of concern applicable to any particular elements of critical infrastructure. This section would also address the related risk management issues and the standards, practices, and processes applicable thereto. This section would also include the information provided in response to the RFI regarding present practices with respect to how organizations define and assess risk generally and cyber-security risk specifically. The literature, including standards, applicable to risk assessments generally is vast.[100]

Security Management Challenges: This section would contain a distillation of the information supplied in response to the RFI that reveals what organizations see as the greatest

[99] Those reports and studies include: NIST, *DRAFT Security and Privacy Controls for Federal Information Systems and Organizations (Final Public Draft)* (NIST Special Publication 800-53 Rev 4) (2013); ACLU, *Written Statement of Michelle Richardson Legislative Counsel, American Civil Liberties Union, Washington Legislative Office On "DHS Cybersecurity: Responsibilities to Protect the Nation's Critical Infrastructure" Before the House Homeland Security Committee* (2012); Liu, Edward C. *et al*., Congressional Research Service, *Cybersecurity: Selected Legal Issues* (CRS 7-5700, R42409) (2012); Bipartisan Policy Center, *Cyber Security Task Force: Public-Private Information Sharing* (2012); The Constitutional Project, *FAQs on Cybersecurity and Privacy* (2012); Grama, Joanna Lyn, *Legal Issues in Information Systems* (2010); and Nojeim, Gregory T., "Cybersecurity and Freedom on the Internet," 4 *Journal of National Security & Policy* 119 (2010).

[100] See, by way of examples, the following references that relate specifically to cyber-security: NIST, *Information Security: Guide for Conducting Risk Assessments* (NIST Special Publication 800-30, Revision 1) (2012) (which includes a very useful bibliography on risk assessment); ISO/IEC 27005, Information technology - Security techniques - Information security risk management (Second Edition) (2011); NIST, *Guide to Applying the Risk Management Framework to Federal Information Systems (NIST Special Publication* 800-37) (2010); NIST, *Managing Information Security Risk* (NIST Special Publication 800-39) (2011); Landoll, Douglas, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments* (Second Edition) (2011); Kouns, Jake, *et ano*., *Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams* (2010); Peltier, Thomas R., *Information Security Risk Analysis* (Third Edition) (2010); Gibson, Daril, *Managing Risk in Information Systems* (2010); Whitman, Michael E., et *ano*., *Management of Information Security* (2010); Kairab, Sudhanshu, *A Practical Guide to Security Assessments* (2004); and NIST, *Risk Management Guide for Information Technology Systems* (NIST Special Publication 800-30) (2002). For information on Octave and the CERT Resilience Management Model from the Software Engineering Institute, see: http://www.cert.org. See, also by way of examples, the following references that relate to risk assessment generally: Young, Carl, *Metrics and Methods for Security Risk Management* (2012); *ISO 31000, Risk management – Principles and guidelines* (First Edition) (2009); *IEC/ISO 31010, Risk management – Risk assessment techniques* (First Edition) (2009); *ISO Guide 73, Risk management—Vocabulary* (First Edition) (2009); Project Management Institute, *Practice Standard for Project Risk Management* (2009); Australia and New Zealand Standard on Risk Management, *AS/NZS 4360* (2004); Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management* (2004); H.M. Treasury, *The Orange Book, Management of Risk – Principles and Concepts* (2004); Federation of European Risk Management Associations, *A Risk Management Standard* (2002);

challenges in improving cyber-security practices across critical infrastructure and what organizations see as the greatest challenges in developing a cross-sector standards-based framework for critical infrastructure. This section would contain cross-references to the sections within the Framework that address the identified challenges.

Critical Cyber Asset Identification and Dependencies between Elements of Critical Infrastructure: To the extent not otherwise addressed in the Framework, this section would provide standards and practices applicable specifically to critical cyber asset identification and to the identification of critical cyber and other assets that are interdependent with and upon other critical physical and information infrastructures, including critical assets associated with the telecommunications, energy, financial services, water, and transportation sectors. This section would also provide standards and practices applicable to the analysis of those interdependencies.[101]

(3) Information Security Governance Issues

Information Security Engagement: This section would explore the roles and responsibilities of all stakeholders in relation to the assurance of cyber-security for critical infrastructure and would set forth standards and practices defining those roles for government engagement, industry engagement, and for out-sourcing of responsibilities.[102]

Security Management Policies and Organizational Issues: This section would distill the information provided in response to the RFI in relation to described organizations' policies and procedures governing risk generally and cyber-security risk specifically, how senior management communicates and oversees these policies and procedures, where organizations locate their cyber-security risk management program offices, and the extent to which cyber-security risk is incorporated into organizations' overarching enterprise risk management process. This section would also address the state of current practice and best practices in relation to the separation of business from operational systems, the use of encryption and key management, the identification and authorization of users accessing systems, asset identification and management, monitoring and incident detection tools and capabilities, incident handling policies and procedures, mission/system resiliency practices; and security engineering practices; roles and

[101] One possible starting point for this critical infrastructure/key resource ("CI/KR") identification might be the database used for scoring risk and determining Urban Area Security Initiative ("UASI") grant eligibility, for which, see: GAO, Memorandum to Congressional Committees, *Subject: Homeland Security Grant Program Risk-Based Distribution Methods:Presentation to Congressional Committees - November 14, 2008 and December 15, 2008* (December 23, 2008); and GAO, Memorandum to Congressional Requesters, *Homeland Security Grants: Observations on Process DHS Used to Allocate Funds to Selected Urban Areas* (February 7, 2007).

[102] A useful starting place may be the AGISM, which addresses these issues in Parts II and III. See also: GAO, *Report to Congressional Addressees, Cyber Security, National Strategy, Roles, and Responsibilities Need to Be Better defined and More Effectively Implemented* (GAO-13-187) (2013).

responsibilities. These subject matters and the to-be-associated standards and practices would be addressed in the relevant specific sections of the Framework as outlined below.[103]

Cyber-Security Objectives, Cyber-Security Strategy, the Matter of Prioritization, and the Integration of Budgetary Issues: This section would consider what performance goals organizations adopt to ensure their ability to provide essential services while managing cyber-security risk and to set forth standards and practices applicable to the proper definition of cyber-security objectives.[104] This section would also address the development of cyber-security strategy to meet the identified cyber-security objectives and the related issues of the prioritization of objectives from a practical standpoint and the integration of budgetary considerations into the determination and execution of cyber-security strategy.[105]

Information Security Documentation: This section would address standards and practices in relation to the documentation of information security strategy, information security policy, security risk management plans, standard operating procedures, incident response plans, emergency procedures, and business continuity and disaster recovery plans.[106]

Change Management and Configuration Management: This section would address standards and practices applicable to change and configuration management from a cyber-security standpoint.[107]

---

[103] On governance issues, see, for example: ITU, *ITU-T, X.1054, Information Technology – Security Techniques – Governance of Information Security* (2012); Gibson, Daril, *Managing Risk in Information Systems* (2010); Whitman, Michael E., et *ano*., *Management of Information Security* (2010); Johnson, Robert, *et ano*., *Security Policies and Implementation Issues* (2010); EC-Council, *Network Defense: Security Policy and Threats* (2010); Brotby, Krag, *Information Security Governance: A Practical Development and Implementation Approach* (2009) For information on COBIT, A Business Framework for Governance and Management of Enterprise IT, see: http://www.isaca.org.

[104] In this connection, see: Wheeler, Evan, *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up* (2011); Gibson, Daril, *Managing Risk in Information Systems* (2010); Whitman, Michael E., et *ano*., *Management of Information Security* (2010); and NIST, *Guide to Developing Security Plans for Federal Information Systems* (NIST Special Publication 800-18) (2006)

[105] In this connection, see: NIST, *Integrating IT Security into the Capital Planning and Investment Control Process* (NIST Special Publication 800-65) (2005).

[106] In this connection, see again: Wheeler, Evan, *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up* (2011); Gibson, Daril, *Managing Risk in Information Systems* (2010); Whitman, Michael E., et *ano*., *Management of Information Security* (2010); and NIST, *Guide to Developing Security Plans for Federal Information Systems* (NIST Special Publication 800-18) (2006)

[107] In this connection, see: NIST, *Information Security, Guide for Security-Focused Configuration Management of Information System*s (NIST Special Publication 800-128) (2011); Watts, Frank B., *Engineering Documentation Control Handbook: Configuration Management and Product Lifecycle Management* (Fourth Edition) (2011); and Aiello, Robert *et ano*., *Configuration Management Best Practices: Practical Methods that Work in the Real World* (2010). See also: CMII Research Institute – Institute of Configuration Management ("CMII"), CMII-100D, *CMII Standard for Enterprise Configuration Management* (2010); CMII, *CMII-105C, CMII Standard for Product Configuration Management* (2010); *IEEE Standard 828, IEEE Standard for Software Configuration Management* (2005); and *ANSI/EIA Standard 649-A, National Consensus Standard for Configuration Management* (2004).

System Certification/Accreditation and Auditing of the Effectiveness of Cyber-Security Protection: This section would address the associated issues of certification/accreditation of systems and the auditing of systems and provide standards and practices applicable thereto.[108]

Benchmarking: This section would set forth standards and practices with respect to the use of benchmarking to assure that cyber-security efforts meet best practices.[109]

Standards' Setting Nationally and Internationally: This section would distill the information provided in response to the RFI relating to what role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cyber-security conformity assessment. This section would also set forth standards and practices in this respect.[110]

Research and Development in Relation to Cyber-Security: This section would give consideration to standards and practices for commitments to research and development in relation to cyber-security.[111]

(4) Information Security Monitoring

Vulnerability Management and Security Effectiveness Testing, Penetration Testing and Other Techniques and Practices Applicable to Security Effectiveness Testing: This section would set forth standards, policies, and practices for the testing and management of cyber vulnerability. This section would consider the use of ethical hacking as a vulnerability assessment tool and the methods of malicious hackers and how they can be blocked.[112]

---

[108] In this connection, see: ISO/IEC TR 27008, Information technology -- Security techniques -- Guidelines for auditors on information security controls (2012); Davis, Chris, *et al.*, *IT Auditing: Using Controls to Protect Information Assets* (Second edition) (2011); NIST, *Guide for Assessing the Security Controls in Federal Informations Systems and Organizations* (NIST Special Publication 800-53A) (2010); Jackson, Chris, *Network Security Auditing* (2010); ISACA, *IS Standards, Guidelines and Procedures for Auditing and Control Professionals* (2008); and ITU, *ITU-T, X.816, Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework* (1995).

[109] In this connection, see: Whitman, Michael E., et *ano*., *Management of Information Security* (2010).

[110] In this connection, see: Williams, Barry L., *Information Security Policy Development for Compliance* (2013).

[111] On R&D generally in relation to cyber-security, see: Maughan, Douglas, *et al.*, "Introducing the federal Cybersecurity R&D strategic plan," 19 *The Next Wave* 3 (2012); and Government Accountability Office ("GAO"), *Report to Congressional Requesters, Cybersecurity, Key Challenges Need To Be Addressed to Improve Research and Development* (GAO-10-446) (2010)

[112] In this connection, see: Allen, Lee, *Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide* (2012); McClure, Stuart, *et al.*, *Hacking Exposed 7: Network Security Secrets & Solutions* (2012); Engebretson, Patrick, *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy* (2011); Stuttard, Dafydd, *et ano*., *The Web Application Hacker's Handbook* (Second edition) (2011); Simpson, Michael T., *Hands-On Ethical Hacking and Network Defense* (2010); EC-Council, *Penetration Testing: Security Analysis* (2010); EC-Council, *Penetration Testing: Procedures & Methodologies* (2010); EC-Council, *Penetration Testing: Network & Perimeter Testing* (2010); EC-Council, *Penetration Testing: Network*

Incident Detection Techniques, Continuous Monitoring, Alarms, and Response: This section would set forth standards and practices in relation to the use of incident detection techniques, the need for continuous monitoring, alarms, and response planning for intrusions.[113]

Cyber-Security Measurement Methods and Practices Applicable to Measuring of the Effectiveness of Cyber-Security Protection: This section would consider and set forth standards and practices in relation to cyber-security measurement methods and the measuring in practice of the effectiveness of cyber-security.[114]

(5) Personnel Security

Information Security Awareness and Training: This section would provide standards and practices relating to information security awareness and training for personnel.[115]

Authorizations, Security Clearances, and Briefings: This section would provide standards and practices relating to authorization practices, security clearance practices, and access to briefings of personnel.[116]

Threat Testing (2010); EC-Council, *Penetration Testing: Communication Media Testing* (2010); EC-Council, *Network Defense: Security and Vulnerability Assessment* (2010); EC-Council, *Network Defense: Security Policy and Threats* (2010); EC-Council, *Ethical Hacking and Countermeasures: Attack Phases* (2009); EC-Council, *Ethical Hacking and Countermeasures: Threats and Defense Mechanisms* (2009); EC-Council, *Ethical Hacking and Countermeasures: Secure Network Infrastructures* (2009); EC-Council, *Ethical Hacking and Countermeasures: Linux, Macintosh and Mobile Systems* (2009); EC Council, *Ethical Hacking and Countermeasures: Web Applications and Data Servers* (2009); and NIST, *Technical Guide to Information Security Testing and Assessment* (NIST Special Publication 800-115) (2008).

[113] In this connection, see: NIST, *DRAFT Guide to Intrusion Detection and Prevention Systems (IDPS)* (NIST Special Publication 800-94 Rev. 1) (2012); NIST, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organization*s (NIST Special Publication 800-137) (2011); NIST, *Contingency Planning Guide for Federal Information Systems* (NIST Special Publication 800-34 Revision 1) (2010); Whitman, Michael E., *Principles of Incident Response and Disaster Recovery* (2006); Northcutt, Stephen, *et ano.*, *Network Intrusion Detection* (Third Edition) (2002); and ITU, *ITU-T, X.816, Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework* (1995)

[114] In this connection, see: Brotby, W. Krag, *et ano*., *PRAGMATIC Security Metrics: Applying Metametrics to Information Security* (2013); Hayden, Lance, *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data* (2010); Young, Carl, *Metrics and Methods for Security Risk Management* (2010); Brotby, W. Krag, *Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement* (2009); Brotby, Krag, *Information Security Governance: A Practical Development and Implementation Approach* (2009); NIST, *Performance Measurement Guide for Information Security* (NIST Special Publication 800-55 Revision 1) (2008); Black, Paul E., et al., "Cyber Security Metrics and Measures," in Voeller, John G. (Editor), *Wiley Handbook of Science and Technology for Homeland Security* (2008); and Jacquith, Andrew, *Security Metrics: Replacing Fear, Uncertainty, and Doubt* (2007).

[115] In this connection, see: Department of Energy, *Essential Body of Knowledge (EBK), A Competency and Functional Framework For Cyber Security Workforce Development* (2011); Herold, Rebecca, *Managing an Information Security and Privacy Awareness and Training Program* (Second Edition) (2010); and DHS, *IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development* (2007), http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2007-12/ISPAB_Dec7-BOldfield.pdf; NIST, *Building an Information Technology Security Awareness and Training Program* (NIST Special Publication 800-50) (2003)

The Use of the Internet: This section would provide standards and practices relating to use by personnel of the Internet as that issue concerns cyber-security.[117]

(6) Physical Security for Information Systems

Communications Infrastructure, Communications Systems and Devices, Other Critical Cyber Assets: Appropriate sections would provide standards and practices in relation to the physical security of relevant networks, systems, and devices, where physical security bears materially upon cyber security.[118]

(7) Information Technology Security

Product and Media Security: Appropriate sections would provide standards and practices in relation to product and media security, where such security bears materially upon cyber security. [119]

Software Security: This section would address standards and practices in relation to software security and the certification of applications for use.[120]

Email Security: This section would address standards and practices applicable to email and the security aspects thereof.[121]

Access Control: This section would provide standards and practices in relation to access control.[122]

Cryptography: The subject matter of this section is self-evident and beyond the scope of the RCC Response.

---

[116] In this connection, see: AGISM, Parts II and III.
[117] In this connection, see again: AGISM, Parts II and III.
[118] In this connection, see again: AGISM, Parts II and III.
[119] In this connection, see again: AGISM, Parts II and III.
[120] In this connection, see: Howard, Michael, *et al., 4 Deadly Sins of Software Security: Programming Flaws and How to Fix Them* (2009); and McGraw, Gary, *Software Security: Building Security In* (2006).
[121] In this connection, see: NIST, *Guidelines on Electronic Mail Security* (NIST Special Publication 800-45 Version 2) (2007). See also: AGISM, Parts II and III.
[122] In this connection, see: NIST, *DRAFT Electronic Authentication Guideline* (NIST Special Publication 800-63-2) (2013); Whitman, Michael E., et *ano*., *Management of Information Security* (2010); Ballad, Bill, *et al., Access Control, Authentication, and Public Key Infrastructure* (2010); ITU, *ITU-T, X.813, Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework* (1996); ITU, *ITU-T, X.815, Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework* (1995); ITU, *ITU-T, X.814, Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework* (1995); ITU, *ITU-T, X.812, Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework* (1995); and ITU, *ITU-T, X.811, Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework* (1995).

Cross-Domain Security and Electronic Security Perimeter(s): This section would provide standards and practices with respect to cross-domain security and the related matter of electronic security perimeter maintenance and would extend to the use of gateways, firewalls, cross-domain solutions, diodes, and related matters.[123]

Intrusion Prevention: This section would provide standards and practices to be employed to assure or minimize intrusions.[124]

Scanning and Analysis Tools: This section would set forth standards and practice for the use of port scanners, vulnerability scanners, packet sniffers, filters, and trap and trace techniques.[125]

(8) Data Security, Transfers, and Content Filtering

Data Security, Data Transfer Policies and Procedures, and Content Filtering: Appropriate sections would provide standards and practices in relation to the data security and the related matters of data transfer policies and procedures as well as content filtering.[126]

(9) Working Off-Site

Mobile Devices, Working Outside the Office, and Working from Home: Appropriate sections would provide standards and practices in relation to the indicated aspects of off-site work and their relationship to cyber-security.[127]

B. Sections Having Industry-Specific Application

Identification of Industry Sectors with Specific Cyber-security Requirements: One starting place for the identification of industry sectors with specific cyber-security requirements

[123] In this connection, see: Whitman, Michael E., et *ano*., *Management of Information Security* (2010); EC-Council, *Network Defense: Perimeter Defense Mechanisms* (2010); NIST, Guidelines on Firewalls and Firewall Policy (NIST Special Publication 800-41 Revision 1) (2009); NIST, *Security Guide for Interconnecting Information Technology Systems* (NIST Special Publication 800-47) (2002); and Northcutt, Stephen, *et al.*, *Inside Network Perimeter Security* (Second Edition) (2002). See also: AGISM, Parts II and III.

[124] In this connection, see: NIST, *DRAFT Guide to Intrusion Detection and Prevention Systems (IDPS)* (NIST Special Publication 800-94 Rev. 1) (2012); and Whitman, Michael E., et *ano*., *Management of Information Security* (2010).

[125] In this connection, see: Whitman, Michael E., et *ano*., *Management of Information Security* (2010); and Simpson, Michael T., *Hands-On Ethical Hacking and Network Defense* (2010).

[126] In this connection, see: AGISM, Parts II and III; and Johnson, Robert, *et ano*., *Security Policies and Implementation Issues* (2010).

[127] In this connection, see: AGISM, Parts II and III.

is the National Infrastructure Protection Plan prepared by DHS and the related sector-specific plans.[128]

Industry-Specific Current Cyber-Security Sources and Methods and Their Utility: RCC understands that NIST is particularly interested in standards and practices that have cross-sector applicability.[129] Nevertheless, RCC believes not inconsistently with the RFI, that consideration of industry-specific standards is necessary and proper. Certain sectors are particularly critical because their security and the special techniques applicable thereto affect the overall cyber-security of all critical infrastructure, *e.g.*, the information technology sector and the communications sector, and other sectors are so fundamental because their security and the special techniques applicable there affect the overall operations of all or substantially all sectors of critical infrastructure, *e.g*., the electric power sector. Accordingly, industry-specific standards and practices must be considered if the Cybersecurity Framework is to be truly comprehensive.

This section, like that applicable to cross-sector standards and practices in relation to cyber-security may or may not survive the final form of the Cybersecurity Framework because the Framework may consistent solely of recommended standards and policies and may not encompass all standards and policies to which consideration was given.

---

[128] See: DHS, *National Infrastructure Protection Plan, Partnering to enhance protection and resiliency* (2009); *Banking and Finance, Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Pla*n (2007); *Chemical Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan* (2010); *Commercial Facilities Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan* (2010); *Communications Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan* (2010); *Critical Manufacturing Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan* (2010); *Dams Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan* (2010); *Defense Industrial Base, Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Pla*n (2007); *Energy Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan* (2010); *Food and Agriculture Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan* (2010); *Information Technology Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan* (2010); *National Monuments and Icons Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan* (2010); *Nuclear Reactors, Materials, and Waste Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan* (2010); *Transportation Systems, Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Pla*n (2007); and *Water, Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Pla*n (2007). See also, with respect to the transportation systems sector, the following DHS reports on segments of that sector: Aviation Modal Annex, *Freight Rail Modal Annex, Highway Infrastructure and Motor Carrier Modal Annex, Maritime Modal Implementation Plan, Mass Transit Modal Annex*, and *Pipeline Modal Annex*. On the state of the critical infrastructure protection program generally, see: GAO, *Report to Congressional Requesters, Critical Infrastructure Protection, DHS List of Priority Assets Needs to Be Validated and Reported to Congress* (GAO-13-296) (2013). For an early contribution to this subject, see: The President's Commission on Critical Infrastructure Protection, *Critical Foundations, Protecting America's Infrastructures* (1997)

[129] The RFI asks, *inter alia*, which approaches apply across sectors, how do these approaches take into account sector-specific needs, should there be a sector-specific standards development process or voluntary program, what can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches and expresses NIST's interest in identifying core practices that are broadly applicable across sectors and throughout industry.

Significant bibliographical compilations regarding industry-specific cyber-security standards and practices are available. Thus, for example, substantial industry-specific cyber-security guidance has been collected by the GAO.[130] The following additional materials are organized by industry:

- Communications:
    - ISO/IEC 27011:2008,[131] which defines guidelines supporting the implementation of information security management in telecommunications organizations;
    - GAO, *Report to Congressional Committees, Information Security, Better Implementation of Controls for Mobile Devices Should Be Encouraged* (GAO-12-757) (2012);
    - The European Telecommunications Standards Institute ("ETSI") 187 Series Standards, including:
        - ETSI TS 187 001, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC) Requirements (Version 3.7.1) (2011);
        - ETSI TR 187 002, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC) Threat Vulnerability and Risk Analysis (Version 3.1.1) (2011);
        - ETSI TS 187 003, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture (Version 3.4.1) (2011); and
        - ETSI TR 187 014, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); eSecurity; User Guide to e TVRA web-database (Version 2.1.1) (2009); and
    - ETSI 102 165 Series Standards, including:
        - ETSI TS 102 165-1, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and

[130] GAO, *Report to Congressional Requesters, Critical Infrastructure Protection, Cybersecurity Guidance Is Available, but More Can Be Done to Promote its Use* (GAO-12-92) (2011)

[131] ISO/IEC 27011, Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (2012)

protocols; Part 1: Method and proforma for Threat, Risk Vulnerability Analysis (Version 4.2.3) (2011); and

- ETSI TS 102 165-2, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures (Version 4.2.1) (2007).

- NIST Publications:

  - NIST, *DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices* (NIST Special Publication 800-164) (2012); and

  - NIST, *Guide to Securing WiMAX Wireless Communications* (NIST Special Publication 800-127) (2010).

- ITU[132]:

  - 800 Series Standards on Security for Open Systems Interconnection;

  - 1000 Series Standards on Information and Network Security;

  - 1100 and 1300 Series Standards on Secure Applications and Services; and

  - 1200 and 1500 Series Standards on Cyberspace Security and Cybersecurity Information Exchange.

- Financial Services:

  - ISO/IEC TR 27015:2012[133] provides information security guidance complementing and in addition to information security controls defined in ISO/IEC 27002:2005 for initiating, implementing, maintaining, and improving information security within organizations providing financial services.

- Power Industry:

  - The IEC 62351 Series Standards:

[132] Previously-referred-to standards series

[133] ISO/IEC TR 27015, Information technology -- Security techniques -- Information security management guidelines for financial services (Fist Edition) (2012)

- IEC/TS 62351-1:2007,[134] which provides an introduction to various aspects of information security as applied to power system operations and is relevant to smart grid issues;

- IEC 62351-2:2008,[135] which covers the key terms used in the IEC 62351 series;

- IEC/TS 62351-3:2007,[136] which specifies how to provide confidentiality, tamper detection, and message level authentication for SCADA and telecontrol protocols that make use of TCP/IP as a message transport layer;

- IEC/TS 62351-4: 2007,[137] which specifies procedures, protocol extensions, and algorithms to facilitate securing ISO 9506 - Manufacturing Message Specification ("MMS") based applications;

- IEC/TS 62351-5:2009,[138] which specifies messages, procedures and algorithms for securing the operation of certain protocols;

- IEC/TS 62351-6:2007,[139] which specifies messages, procedures, and algorithms for securing the operation of certain other protocols;

- IEC/TS 62351-7:2010,[140] which defines network and system management ("NSM") data object models that are specific to power system operations and are used to monitor the health of networks and systems, to detect possible security intrusions, and to manage the performance and reliability of the information infrastructure; and

- IEC/TS 62351-8:2011,[141] which relates to the access control of users and automated agents to data objects in power systems;

[134] IEC/TS 62351-1, Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues (First edition) (2007)
[135] IEC 62351-2, Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms (First edition) (2008)
[136] IEC/TS 62351-3, Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP (First Edition) (2007)
[137] IEC/TS 62351-4, Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS (First Edition) (2007)
[138] IEC/TS 62351-5, Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives (First Edition) (2009)
[139] IEC/TS 62351-6, Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850 (First Edition) (2007)
[140] IEC/TS 62351-7, Power systems management and associated information exchange - Data and communications security - Part 7: Network and system management (NSM) data object models (First Edition) (2010)
[141] IEC/TS 62351-8, Power systems management and associated information exchange - Data and communications security - Part 8:Role-based access control (First edition) (2011)

- GAO, *Testimony Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, Cybersecurity, Challenges in Securing the Modernized Electricity Grid, Statement od Gregory C. Wilshusen, Director,, Information Security Issues, and David C. Trimble, Director, Natural Resources and the Environmen*t (GAO-12-507T) (2012);

- FERC, Final Order, *Mandatory Reliability Standards for Critical Infrastructure Protection* (Docket No. RM06-22-000; Order No. 706, January 18, 2008) (122 FERC ¶ 61,040), which sets forth eighth mandatory standards for critical infrastructure protection ("CIP"): (i) CIP-002-1 – Critical Cyber Asset Identification; (ii) CIP-003-1 – Security Management Controls; (iii) CIP-004-1 – Personnel and Training; (iv) CIP-005-1 – Electronic Security Perimeter(s); (v) CIP-006-1 – Physical Security of Critical Cyber Asset; (vi) CIP-007-1 – Systems Security Management; (vii) CIP-008-1 – Incident Reporting & Response Planning; and (viii) CIP-009-1 – Recovery Plans for Critical Cyber Assets; and

- NIST, *Guidelines for Smart Grid Cyber Securit*y (NIST Interagency Report 7628) (2010).

VI. Conclusion

RCC hopes that the RCC Response will be useful to NIST in connection with NIST's Development of the Cybersecurity Framework. RCC further hopes that the RCC Response will encourage and guide NIST in relation to taking a very active role in assuring the cyber-security of the PSBN.

Respectfully submitted,

RCC Consultants, Inc.
100 Woodbridge Center Drive, Suite 201
Woodbridge, NJ 07095

http://www.rcc.com

To contact RCC in connection with the RCC Response, please contact Carl Robert Aron, caron@rcc.com, John Facella, jfacella@rcc.com, or Terry Wright, twright@rcc.com.