System 1, Inc.

October 10, 2014

Mr. Adam Sedgewick
U.S. Department of Commerce
1401 Constitution Avenue NW.
Washington, DC 20230

Re: Experience with the Framework for Improving Critical Infrastructure Cybersecurity

Dear Mr. Sedgewick,

System 1, Inc. is pleased to submit this response to the *Request for Information (ROI) Experience with the Framework for Improving Critical Infrastructure Cybersecurity* as it related to supporting efforts to facilitate acceptance of the Cybersecurity Framework. This response is based on System 1's experience and engagement with numerous critical infrastructure entities and their representatives from senior executives and board members to cybersecurity senior managers and practitioners as well as operational leads and engineers. These conversations occurred during face-to-face meetings as part of industry research, paid client engagements, and during the Q&A sessions directed at System 1 senior executives during the course of conference presentations and panel participation.

Understanding that we have a responsibility to 'give back to the industry' we have been constant participants and supporters of NIST's efforts in the development and implementation of the Cybersecurity Framework. We actively participated in the development of both the original NISTIR and the Cybersecurity Framework during the various workshops and working sessions and publicized the Frameworks development and publication during our client engagements, teaching webinars and conference presentations and panels.

System 1 looks forward to continued participation during the evolving implementation and refinement phase of the Framework. If you have any questions regarding the content of this response, please do not hesitate to contact us.

Sincerely,

Ernest W. Wohnig III
Senior Vice President
System 1, Inc.
(703) 216-2986
ewohnig@syst1.com

System 1, Inc.

System 1 Inc. Response to the NIST RFI – Experience with the Framework for Improving Critical Infrastructure Cybersecurity

System 1 Overview

System 1, Inc. is cybersecurity and critical infrastructure security consulting firm which advises business leaders in the federal & state government and critical infrastructure (utilities, oil & gas, and supporting firms) sectors. We provide strategic advice, assistance, and solutions to our public and private sector clients. System 1 aids client senior leadership in focusing on and understanding cyber risk strategy within their larger business risk structure, guide clients in institutionalizing cybersecurity governance and programs, and lead in the development of innovative approaches to address clients' cybersecurity & assurance risk needs.

With deep industry and functional experience System 1's world-class team provides timely, high-impact results through an innovative portfolio of services. We help clients approach the complex and shifting forces that shape the cyber and broader security and assurance environment, assisting them in identifying critical leverage points and developing results-oriented strategies for reduced risk, smarter compliance, better performance, and optimized investments. System 1 personnel are management and technical experts who focus on advancement and change through the prism of people, processes, and technology; providing an integrated solution tailored to each client's unique business risk tolerance, existing organizational risk management processes, and the evolving cybersecurity risk environment.

Current Awareness of the Cybersecurity Framework

1. *What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?*

The concise answer is that awareness is mottled across and within sectors and while the framework has had a solid start, six-months is far too short to provide a true test of voluntary acceptance and implementation for industries that involve refresh rates and planning measured in decades. That said, there has been a substantial and sustained effort by federal agencies and a number of industry specific non-profit associations (ex. ISACs, UTC, ISACA, etc.) to increase general awareness of the frameworks existence

4905 Cedar Croft Drive, Bethesda, MD 20814
Telephone: (301)299-2574 Fax (703)288-0816

and its potential use by industry. Additionally, organizations such as ISACA, have gone further and developed guidelines to bridge the gap between existing industry standards and the Framework.

However, the transition from a broad conceptual understanding to practical application of the Framework continues to be a slow and halting process. This is due to a number of issues including the sheer time required to filter such a model through the diverse industry environment (both in terms of within and across different critical infrastructure sectors); uneven education and awareness of senior board leadership, executives, regulators, and cybersecurity decision makers across many industries; the limits of available federal resources to provide education & awareness further diluted by the apparent lack of focus on domestic industries as federal resources have been devoted to international marketing of the framework before its comprehensive acceptance within the US; and the lack of a substantive approach to incorporating the cybersecurity framework into the overarching business risk models utilized by senior business leadership in developing corporate risk mitigation plans and strategies.

2. *How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?*

Based on our interaction with clients in compensated engagements, uncompensated educations activities for industry, and off-line discussions; the broadest outreach impact has come from industry associations through summits, seminars, conferences, webinars, and one-on-one engagement. The NIST workshops and participation in industry conferences provides industry the opportunity to 'hear directly from the source' but by the very nature of the medium and finite resources of NIST these tend to be small and self-selecting audiences of security professionals and practitioners. Media provides a much more dispersed and generally less detailed understanding of the framework although it is helpful in engendering interest and can cause individuals to seek further information from other sources. The key missing demographic in nearly all cases is the senior executives, board members, CFOs, and COOs who make the majority of risk and resource decisions for businesses.

3. *Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?*

As noted in response to earlier questions, education and acceptance across and within industry sector is varied thus impacting coordination with industry associations and non-profit groups. Additionally, the emphasis seems to have settled at the CISO and senior cybersecurity manager level in the vast majority of cases. The Cybersecurity Framework,

like cybersecurity in general, is often seen as a CIO or IT problem and not appropriately integrated into business' risk approach. This hampers communications and sharing outside of the organization. Also, in many cases when cybersecurity leads for organizations seek to share information and lessons learned they are met with resistance from leadership due to the persistence of concerns regarding liability, privacy regulations, and reputational issues.

4. *Is there general awareness that the Framework:*

    a. *Is intended for voluntary use*

Based on discussions with senior utility executives and cybersecurity managers in the industry, while it is understood that the framework is currently voluntary, industry owners and decision makers are still concerned that forced or de facto adoption may occur in the future. This was exacerbated by the E.O.'s reporting requirement for the federal sector responsible agencies. Additionally, use by state regulators of the Cybersecurity NISTIR previously developed by NIST predisposed many utility representatives to concern.

    b. Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?

As noted in responses to earlier questions, the emphasis seems to have settled at the CISO and senior cybersecurity manager level in the vast majority of cases. The Cybersecurity Framework, like cybersecurity in general, is often seen as a CIO or IT problem and not appropriately integrated into business' risk approach.

    c. Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?

Broadly it is understood that the cybersecurity framework builds on or translates to existing standards and guidelines. In several cases such as with ISACA's guidelines there are efforts to draw direct cross connections between the cybersecurity framework and other standards/models. That said, this fact often brings up the question from clients of why another framework is required and how do they ensure that what they have is consistent/compatible with the framework.

5. *What are the greatest challenges and opportunities—for NIST, the Federal government more broadly, and the private sector—to improve awareness of the Framework?*

As the purpose of the cybersecurity framework is to aid the industry in strengthening cybersecurity, recent targeted events impacting numerous private sector organizations creates openings and increases receptiveness across the sectors for NIST and, more

importantly, industry associations and non-profits to raise awareness of the threat and what entities can do to address it. Due to their greater reach and position as 'trusted advisors' industry associations and non-profits are best positioned to carry the message and educate. A key issue to address is the 'communication up' of cybersecurity risk and its integration into the corporate risk management model. A major challenge for cybersecurity practitioners and even cybersecurity senior leaders like CISOs is the effective communication of the cybersecurity risk to senior executives and boards in a manner that translates to business objectives and risks.

6. *Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?*

There is some international awareness based on media reporting and NIST/DHS overseas junkets, however, the depth of understanding is relatively shallow. Additionally, the very different philosophies viewpoints from which countries or supranational states approach cybersecurity, tends to limits the perceived applicability of the cybersecurity framework in the international arena. How true that is in the practical sense is debatable but the perceptions exists and influences both multinationals and single-state market entities. It tends to be driven by the belief that different states/cultures emphasis different poles of countervailing conditions impacting cybersecurity such as privacy vs national security or state security vs free availability of information.

7. *If your sector is regulated, do you think your regulator is aware of the Framework, and do you think it has taken any visible actions reflecting such awareness?*

N/A

8. *Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework*?

As a cybersecurity consulting firm, System 1 supports utilities and firms in the implementation of the cybersecurity framework as part of their overall cybersecurity program and assist in its integration into the larger business risk management strategy/model. We also partner with industry associations and non-profits to bolster industry awareness through industry conference/summit presentations and webinars addressing best practices for implementation of the cybersecurity framework and lessons learned from recent implementation by our clients and others.

9. *What more can and should be done to raise awareness?*

4905 Cedar Croft Drive, Bethesda, MD 20814
Telephone: (301)299-2574 Fax (703)288-0816

1) Focus limited resources on domestic acceptance. If the framework is not widely accepted within the US, there is little leverage for encouraging international acceptance. This is especially pertinent at such an early stage.
2) Increase coordination with international standards bodies when the time is right (i.e. after greater domestic acceptance); leveraging their capabilities, infrastructure, and international presence will provide greater return on expended resources than 'single-shot' junkets to individual countries.
3) Consider a different assessment assistance model that better leverages the private sector in regard to assisting utilities and other private sector infrastructure owners. One option would be a cost sharing model between the government and the infrastructure owner. Instead of government entities attempting to provide 'free' assessments to a limited group due to resource and time constraints, the government could oversee a program which provided a grant (sharing part of the cost and variable in amount based on established criteria) for initial assessments, which could be performed by private sector firms that compete on price; either preselected by government contract or vetted by application and provided as a pool for selection by the critical infrastructure owner.

Experiences with the Cybersecurity Framework

System 1 has engaged with a number of clients regarding the use of Cybersecurity Framework in addition to numerous other standards, models, and guidelines. The short duration during which the cybersecurity framework has been available in a complete and official form, prevents either our clients or us in making concrete determinations on its application. There has not been enough time to see full implementation and secure even the most basic of performance metrics much less true lessons learned.

1. *Has the Framework helped organizations understand the importance of managing cyber risk?*

2. *Which sectors and organizations are actively planning to, or already are, using the Framework, and how?*

3. *What benefits have been realized by early experiences with the Framework?*

4. *What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?*

5. *Do organizations in some sectors require some type of sector specific guidance prior to use?*

6. *Have organizations that are using the Framework integrated it with their broader enterprise risk management program?*

7. *Is the Framework's approach of major components—Core, Profile, and Implementation Tiers—reasonable and helpful?*

8. *Section 3.0 of the Framework ("How to Use the Framework") presents a variety of ways in which organizations can use the Framework.*

    a. *Of these recommended practices, how are organizations initially using the Framework?*

    b. *Are organizations using the Framework in other ways that should be highlighted in supporting material or in future versions of the Framework?*

    c. *Are organizations leveraging Section 3.5 of the Framework ("Methodology to Protect Privacy and Civil Liberties") and, if so, what are their initial experiences? If organizations are not leveraging this methodology, why not?*

    d. *Are organizations changing their cybersecurity governance as a result of the Framework?*

    e. *Are organizations using the Framework to communicate information about their cybersecurity risk management programs—including the effectiveness of those programs—to stakeholders, including boards, investors, auditors, and insurers?*

    f. *Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties?*

9. *Which activities by NIST, the Department of Commerce overall (including the Patent and Trademark Office (PTO); National Telecommunications and Information Administration (NTIA); and the Internet Policy Taskforce (IPTF)) or other departments and agencies could be expanded or initiated to promote implementation of the Framework?*

10. *Have organizations developed practices to assist in use of the Framework?*

Roadmap for the Future of the Cybersecurity Framework

4905 Cedar Croft Drive, Bethesda, MD 20814
Telephone: (301)299-2574 Fax (703)288-0816

System 1, Inc.

1. *Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?*

The areas identified are comprehensive and due well in addressing technology and personnel (i.e. through workforce) aspects of the cybersecurity challenge but are limited and lacking in regard to the process and organizational environment/culture facets of the problem. Specifically, based on our experience with industry clients we believe the current roadmap misses the opportunity to address the critical issues of senior executive/board member education & awareness and integration of the cybersecurity framework into the broader risk management strategy/model/approach of the business.

2. *Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?*

As noted above, the issue of senior executive/board member education and awareness and integration of the cybersecurity framework into the broader risk management strategy/model/approach of the business is a missed opportunity. Since senior executive/board member are the primary influencers regarding resource allocation within organizations and the corporate risk management strategy/model is the mechanisms by which they make resource allocation decisions and determine acceptable organizational risk tolerance levels, failure to address these in the roadmap creates a 'blind spot' to effective implementation of the cybersecurity framework.

3. *Have there been significant developments—in the United States or elsewhere—in any of these areas since the Roadmap was published that NIST should be aware of and take into account as it works to advance the usefulness of the Framework*

The NIST Roadmap includes Supply Chain Risk Management as one of the Areas for Development, Alignment, and Collaboration. There has been movement on this issue in both the international and domestic arenas. Domestically, DOE released a document titled Cybersecurity Procurement Language for Energy Delivery Systems that addresses the issue in the energy utility space. Sponsored by DOE a group of industry experts developed the document that was then released by the Department of Energy. The document is available at http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014.

Internationally, portions of a new International Organization for Standardization (ISO)/International Electrotechnical Commission standard was recently released. Titled (IEC) 27036 – Information Technology – IT Security Techniques – Information Security for Supplier Relationships, the 4-part standard addresses the practice of managing risks associated with business supplier verticals. Parts one, two, and three of the standard have been approved and published. Part four addressing cloud computing is still in development.

4905 Cedar Croft Drive, Bethesda, MD 20814
Telephone: (301)299-2574 Fax (703)288-0816