Information Technology
Industry Council

December 12, 2013

Adam Sedgewick
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Via e-mail to: csfcomments@nist.gov

RE: ITI comments in response to NIST RFI: "Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework"

Dear Mr. Sedgewick:

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to your RFI of October 29, 2013, "Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework."

ITI is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry. ITI's members comprise the world's leading technology companies, with headquarters worldwide. Cybersecurity is rightly a priority for all governments. We share the goal with governments of improving cybersecurity and therefore our interests are fundamentally aligned. As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. Further, our members are global companies located in various countries. Most service the global market and have complex supply chains in which products are developed, made, and assembled in multiple countries across the world. As a result, we acutely understand the impact of governments' policies on security innovation and the need for U.S. policies to be compatible with – and drive – global norms.

ITI commends the President for directing NIST to lead the development of a voluntary framework, in cooperation with the private sector, to reduce cyber risks to critical infrastructure. We also appreciate NIST's commitment to partnering with the private sector on this task.

1.0 FRAMEWORK INTRODUCTION

Although many people and organizations are likely quite familiar with the Framework's goals, expected benefits, audience, structure, and the like, those basics are not explained as clearly as they could be. This could be particularly problematic for small-and-medium-sized enterprises (SMEs) that have been less involved in working with NIST on the Framework and thus are not as familiar with it. To encourage the greatest degree of understanding and use of the Framework, the introduction should clearly present these and other key concepts. As such, ITI has the following observations and recommendations regarding the introduction.

Voluntary nature of the Framework should be emphasized. The voluntary nature of the Framework should be explained clearly in the very beginning of the document. Currently the term "voluntary" appears only once in the narrative, on line 67 in the Introduction. Even in this case, the language simply states the Executive Order (EO) "calls for the development of a voluntary Cybersecurity Framework…. For assisting organizations…." It needs to be clearer that use/adoption, while strongly encouraged for various reasons, is truly voluntary.

Benefits of Framework use by individual organizations should be clearer. The introduction should make clearer to organizations of all sizes the potential benefits to them—namely to their businesses and employees—of adopting the Framework. The introduction currently is focused on benefits to U.S. national and economic security. While critically important to our country, this likely is not compelling enough to an average small-business owner to convince him/her to spend the time and resources to adopt the Framework. The "Message to Senior Executives on the Cybersecurity Framework" in the August 28 Framework discussion draft included many compelling arguments for individual organizations in this regard (see lines 13-24 of the discussion draft). NIST should consider reinstating the "Message to Senior Executives" in the Framework, and also include these points some other way early in the Framework's introduction.

Relationship to current practices should be clearer. Lines 100-104 explain that "the Framework complements, and does not replace, an organization's existing business or cybersecurity risk management process and cybersecurity program." As NIST and others in the Administration have stated, many entities have very robust cybersecurity processes and programs that may already accomplish much if not all of what is outlined in the Framework. The document should more clearly tell the reader that, if this is the case for their organization, they may decide not to make any changes based on the Framework, and that is an acceptable "use" or "adoption" that can be communicated to any interested stakeholders.

Scope/applicability to non-CI entities should be clearer. The introduction's first paragraph explains the Executive Order "calls for the development of a voluntary cybersecurity Framework …. for assisting organizations responsible for critical infrastructure (CI)…," making it apparent that CI owners and operators are the main Framework targets. However, NIST, and the Administration generally, have stated numerous times a hope that all organizations in the United States voluntarily utilize the Framework, including SMEs and those that are not CI owners/operators. The introduction should explicitly state that the Framework is intended to be a tool for any entity of any size that wishes to improve its cybersecurity, in addition to its primary/initial target of CI entities (per the EO). Absent this caveat up front, there is a large chance many SMEs may believe they could or should not use or benefit from the Framework. The introduction could also discuss the process for modifying the Framework in the future should the definition of CI or key elements change over time.

Scope/prioritization of Framework use should be clearer. While the Framework is designed to be used by any entity of any size that wishes to improve its cybersecurity, the document should provide suggestions as to potentially effective ways to implement the Framework, given the reality of limited resources and the EO's direction that the Framework be cost-effective. In particular, the Framework should note that, for entities choosing to use it, their highest priority

should focus on those processes and IT/cybersecurity-related assets directly involved in the delivery of CI services. Such guidance will allow organizations to focus their available resources towards achieving the objectives of the EO—protection of CI. An organization can, of course, apply the Framework more broadly to achieve other business benefits and can expand the application of the Framework to other areas over time as resources enable.

Introduction should explain the use of global standards. Lines 84-89 correctly explain the reasoning behind the Framework's use of existing standards, guidance, and best practices. Reasons for the use of voluntary global standards should be added here (the justification can be taken from Appendix C, C6, "international alignment"), for a few key reasons, not least of all because global standards, as explained in C6, benefit security and trade.

Equally importantly is the message this will send to foreign governments who are carefully watching the Framework's development and who might emulate its approach in their policy environments. We would support them doing so, because it would create consistent and cohesive approaches across geographies as well as a commitment to the global standardization process, public-private partnerships, and a voluntary, as opposed to regulatory, approach. However, given the already existing misunderstandings many foreign governments and foreign audiences generally have about the Framework—many mistakenly believe NIST is writing new standards for the U.S. economy or feel that NIST is not utilizing global standards—clarifying up front that the Framework points to global standards is imperative. This misconception about the Framework is also shared by many in the press, domestically as well as internationally, so a clear statement about its pointing towards global standards (and why) can potentially shape how the Framework is described around the world.

Finally, the importance of global standards to cybersecurity is a message for U.S. policymakers as well. We are heartened that current NIST and Administration staff involved in the Framework and EO understand and are committed to the role of global standards in improving cybersecurity. Future staff involved in any Framework updates, however, may not understand the importance of this approach. Thus, we must state this for our own audience.

"Choose your own end-state" nature of the Framework should be clearer. Lines 100-108 introduce the tier concept (about which ITI has further comments, below) but lack clear messaging that an organization can choose its own target level of security. One thing that could discourage Framework adoption, particularly among SMEs, would be the misperception that the only acceptable outcome for users is a "tier 4" level. We recognize NIST wants each adopting organization to decide its own tier level based on an understanding of the nature of its business and risks. For example, being at "tier 2" could be wholly appropriate for a given organization. Thus, the introduction should clarify that success for an individual organization is to improve its cybersecurity posture, not to achieve a particular tier per se. Putting that point closer to the front will help readers to understand that any steps they take to improve cybersecurity—even at "tier 1"—are important. The text here also should make clearer that cybersecurity is not an end state, but rather based on risk management.

A workable definition of Framework "Adoption" must be found. The definition of "adoption" has been a large topic of conversation and source of concern within industry. We know NIST, and the Administration generally, understand these concerns as you work to find an appropriate definition. ITI recommends the Administration consider the definition of "adoption" that NIST distilled from the Fifth Cybersecurity Workshop in Raleigh, North Carolina: [1]

An organization adopts the framework when it uses the Cybersecurity Framework as a key part of its systematic process for identifying, assessing, prioritizing, and/or communicating:

- *Cybersecurity risks,*
- *Current approaches and efforts to address those risks, and*
- *Steps needed to reduce cybersecurity risks as part of its management of the organization's broader risks and priorities.*

If it is not appropriate for NIST to incorporate a definition directly into the Framework, it should be otherwise incorporated into related documents being developed by the Department of Homeland Security (DHS) for the Voluntary Program (EO Section 8).

2.0 FRAMEWORK BASICS

Some portions of this section could benefit from reorganization and/or editing.

Section 2.1—Framework Core. Lines 224-231 describe "category" and "subcategory" as used in the Framework. We suggest NIST change "category" and "subcategory" to "outcome" and "action," respectively, throughout the document, because the latter terms much more explicitly identify what these are. Changing these terms would particularly improve the clarity of the narrative in sections 1.0, 2.0, and 3.0, where "category and subcategory" are used often.

Line 242 begins a description of the five Framework Core Functions. ITI recommends they be edited to be explained, followed by their outcomes. Below is an example of our suggestion.

> Identify – Develop the institutional understanding to manage cybersecurity risk to organizational systems, assets, data, and capabilities. *(move up this section to here ➔)* **The activities in the Identify Function are foundational for effective implementation of the Framework. Understanding the business context, resources that support critical functions and the related cybersecurity risks enable an organization to focus its efforts and resources. Defining a risk management strategy enables risk decisions consistent with the business needs or the organization.**
>
> The Identify Function includes the following categories of outcomes: Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.

Section 2.2 – Framework Profile. Section 2.2 suggests using a Framework profile for internal risk management activities to "establish a roadmap for reducing cyber risk," but it is not clear

[1] Update on the Development of the Cybersecurity Framework, December 4, 2013, at http://www.nist.gov/itl.upload/nist_cybersecurity_framework_update_120413.pdf

how an organization would do that, despite the graphic on p. 8. This section should more clearly state that an organization should have two profiles—current and target—and that the organization should use the gaps between the profiles to create a roadmap to improve cybersecurity. In addition, line 305 notes there are existing target profiles, but the Framework includes no examples. Examples (or where to find them) would help the reader understand how to create their own target profile and thus improve cybersecurity.

In terms of using a Framework profile outside an organization, as is contemplated by Section 3.3, we note that, because there is no methodology for creating a profile, profiles cannot validly be compared between organizations. While the uses of a Framework profile expressed in Section 3.3 are valuable, it would be difficult for them to be effective or accurate absent such a common methodology. We suggest a methodology for creating a Framework profile be developed for Version 2.0 of the Framework and that suggestions on potential external uses of profiles also be reserved until then.

Section 2.3 – Framework Implementation Tiers. We applaud the concept of a maturity model in the Framework, but without a common methodology for how tiers are determined and without a statement on the scope of how they may be used, in particular by external parties, the tiers could create unintended anticompetitive consequences.

First, because the Framework does not outline a methodology for how to calculate and apply tiers, tiers do not provide a basis to compare two organizations. However, tiers nonetheless are likely to become factors in procurement and purchase contracts. Second, some ITI members have voiced concerns that the Framework implementation tiers will be used by CI owners and operators to try to push liability onto their vendors. For example, despite the voluntary nature of the Framework, a CI owner or operator nonetheless could require in its contracts that its vendors be "tier 4," even if that is otherwise an unnecessary level for those vendors, and use that stipulation to shift blame onto vendors if something goes wrong. Such potential usage of the tiers runs counter to the very idea that the tiers are a maturity model, that different tiers will be appropriate for different businesses, and that the tiers should be self-determined based on the company's posture vis-à-vis CI and its own organizational goals.

To try to minimize such unintended consequences, ITI suggests NIST specify that the tiers are for internal use only as part of an organization's cybersecurity risk management process. NIST also should include a methodology for determining tiers. We understand this could be a very challenging task given that the Framework is to be issued in February 2014, and industry stands ready to contribute ideas and expertise to NIST to try to create a workable methodology by then. If time constraints make adding a methodology to this version impossible, we would then welcome working with NIST to create a methodology to be included in Version 2.0.

3.0 HOW TO USE THE FRAMEWORK

The examples provided here of how to use the Framework are very helpful and should also be summarized in the introduction, or in an executive summary.

See our comments on Section 2.2, which refer to related concerns with Section 3.3 (Communicating Cybersecurity Requirements with Stakeholders), namely communicating information about profiles.

APPENDIX A- FRAMEWORK CORE

As we noted earlier, key elements of the framework—its voluntary, "choose-your-own end state" nature—need to be made more clearly in the narrative. These points also should be restated in the paragraph introducing Appendix A/the Core (lines 458-464). The Appendix A introduction also should remind the reader that the normative references are designated as examples across the spectrum of cybersecurity risk that are not necessarily appropriate to the needs of every organization. Without such a preamble, the table could mistakenly be read as a laundry list of requirements.[2] Finally, it should state that the normative references are localized to the private sector, or clearly identify those that are public sector examples.

As noted in our comments on Section 2.1, we suggest changing the terminology of the second and third columns from "category" and "subcategory" to "outcome and action," respectively.

Specific comments on certain subcategories and normative references follow.

- **Subcategories ID-AM-1 and ID-AM-2—Physical devices, systems, software platforms, and applications within the organization are inventoried (p. 13).**
    - *Comment:* Beyond the problem of identifying what qualifies as software or applications "within" an organization, read broadly this is a near-impossible standard for any reasonably sized business. Inventorying every device, server, and every piece of software that might be included on a device or server is a monumental undertaking.
- **Subcategories ID-RA-1 and ID-RA-2—Asset vulnerabilities are identified and documented and threats to organizational assets are identified and documented (p. 15).**
    - *Comment:* Without qualification this suggests that entities are expected to identify every possible vulnerability or threat implicated by every asset they own or manage. Instead, the more reasonable alternative would be that an organization should have mechanisms in place for detecting and responding to threats and vulnerabilities, with the understanding that no mechanism for detecting vulnerabilities is perfect.

[2] We understand that these points will be made in the narrative (Introduction and Sections 1.0, 2.0, and 3.0). However, there is a chance some users could consult only the table and not look back to the narrative.

- **Subcategory PR-DS-6—Intellectual property is protected (p. 19).**
  - *Comment:* The scope of intellectual property (IP) protection contemplated by this subcategory is unclear. Without clarity, this could also be read to impose unexpected IP liability.
- **Subcategory PR-DS-7—Unnecessary assets are eliminated (p. 19).**
  - *Comment:* If "assets" is read broadly to encompass software as suggested by the above, this becomes an impossible task. It is unclear how an organization would determine whether or not each and every piece of software is necessary, nor what kind of inventory system would reasonably allow administrators to manage this task. This runs counter to how most, if not all, organizations in the software context operate.
- **Subcategories DE-CM-4 and DE-CM-5—Malicious code is detected and unauthorized mobile code is detected (pp. 22-23).**
  - *Comment:* Again, without qualification these framework components could be read to require unreasonably that an organization must detect all such threats.
- **Informative reference CSC6 (found in PR-IP-2 [p. 19] and PR-PT-3 [p. 20]).**
  - *Comment:* We are concerned about NIST's reference to CSC6, which suggests that users ask for source code for static analysis or try to use object code analysis.[3] Giving code creates security risks for customers, while analysis of object code tends to be of limited use to an outside party, as only the vendor can address whatever issues these might find. Further, the state-of-the-art of these tools can lead to false positives/outputs. Most importantly, these portions of CSC6 hint at product development processes, something as a general matter NIST had rightly avoided. NIST should drop the reference to CSC6 in these two places.

APPENDIX B- METHODOLOGY TO PROTECT PRIVACY AND CIVIL LIBERTIES

The Framework Core (Appendix A) lists five Functions – Identify, Protect, Detect, Respond, and Recover – that are designed to cover cybersecurity activities across all CI sectors. Each Function is then further broken down into Categories and Subcategories. Generally, the Framework Core is intended to enable organizations to more effectively manage their cybersecurity risk. Using

[3] -- How to Implement: "6. Configuration/Hygiene: Test in-house-developed and third-party-procured web and other application software for coding errors and malware insertion, including backdoors, prior to deployment **using automated static code analysis software.** If source code is not available, **these organizations should test compiled code using static binary analysis tools.** In particular, input validation and output encoding routines of application software should be carefully reviewed and tested."

--Procedures to Implement: "**Source code testing tools**, web application security scanning tools, and object code testing tools have proven useful in securing application software, along with manual application security penetration testing by testers who have extensive programming knowledge and application penetration testing expertise."

--Control 6 Test: "In addition to the web application vulnerability scanner, the evaluation team **must also run static code analysis tools** and database configuration review tools against Internet-accessible applications to identify security flaws **on a monthly basis."**

the same five Functions – Identify, Protect, Detect, Respond, and Recover, Appendix B outlines a methodology designed to address privacy and civil liberties considerations in connection with the operation of a cybersecurity program.

The current detailed methodology in Appendix B is not limited to activities relating to a cybersecurity program. Rather, as currently drafted, Appendix B appears to address all of an organization's activities that might implicate privacy and civil liberties considerations. The activities covered by Appendix B should be limited in scope to only those privacy and civil liberty considerations implicated by cybersecurity activities. Also, as currently written, the methodology in Appendix B appears to utilize an inflexible principles-based approach that does not provide organizations with sufficient latitude to develop practices and procedures relating to privacy that are appropriate to their organization.

Accordingly, ITI points to the table submitted by Hogan Lovells and encourages NIST to adopt this alternative privacy methodology.[4] The table can be inserted at the end of the Framework's narrative, prior to Appendix A.

The table submitted by Hogan Lovells contains an alternative privacy methodology that captures the essential privacy protections organizations should consider in connection with cybersecurity risks while appropriately omitting the references to privacy that are not directly implicated by cybersecurity activities. In short, this approach would allow an organization to consider privacy implications concurrently with cybersecurity risks. As a result, organizations will be able to implement a privacy methodology and will not be deterred from adopting an overly broad privacy methodology. The approach we propose meets the EO's call for a privacy methodology, while at the same time provides industry with the necessary built-in flexibility to adopt the methodology.

APPENDIX C- AREAS FOR IMPROVEMENT

We appreciate NIST's goal to identify areas where any additional standards may be needed and to work with the private sector to create those standards and ensure they do not manifest themselves through duplicative and unnecessary controls which hamper compliance and add unnecessary costs.

Of the eight areas listed in this section, we have the following comments:

- C6, "international alignment." As noted in our comments on the Framework introduction, C6, "international alignment," does not fit in this section. It is a (correct) justification why the Framework points to global standards and should be in the introduction. If NIST included it in Appendix C because NIST believes more work should be done, this reasoning is unclear.

[4] The methodology submitted by Hogan Lovells is available at http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf.

CONCLUSION

ITI would like to again thank NIST for its commitment to partnering with the private sector to improve cybersecurity. ITI also would like to commend the Administration for having integrated so much of the input it has received from industry over the past few years on this topic, and for its willingness and eagerness to consistently engage with our companies and the ICT industry generally on how government and industry can work together to improve cybersecurity. The commitment to industry outreach in this regard is an excellent example of the effective public-private partnerships that are essential to improving cybersecurity.

We hope that our comments will receive due consideration. We are available at any time to elaborate on our comments and our suggestions. ITI and its members look forward to continuing to work with NIST and the Administration generally to improve America's cybersecurity posture. Please continue to consider ITI a resource on cybersecurity issues moving forward.

Thank you very much for your consideration.

Sincerely,

Danielle Kriz
Director, Global Cybersecurity Policy