National Defense Industrial Association

Promoting National Security Since 1919

2111 Wilson Boulevard, Suite 400
Arlington, VA 22201-3061
(703) 522-1820 • (703) 522-1885 Fax
www.NDIA.org

13 December 2013

Information Technology Lab
ATTN: Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Dear Mr. Sedgewick:

The National Defense Industrial Association ("NDIA") Cyber Division is pleased to offer these comments pursuant to the National Institute of Standards and Technology's Request for Comments on the Preliminary Cybersecurity Framework ("preliminary Framework"), which was created pursuant to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."

About NDIA:

NDIA is a non-profit organization and America's leading Defense Industry association, with more than 1,700 corporate members and over 96,000 individual members. Our members belong to the entire spectrum of the Defense Industrial Base (DIB), from large to small businesses. The primary objective of NDIA's Cyber Division is to contribute to the national security of the United States by promoting communication and interaction between the DIB, civilian government and military on matters related to Cyber domain policy, legislation, requirements and technology. Our members believe that the cybersecurity framework needs to be both risk and performance based and recognizes that risk management is a foundation principle of homeland security.

The Preliminary Framework Successfully Addresses the Needs of Various Sectors:

The National Institute for Standards and Technology (NIST) has done an admirable job in assembling a framework that allows each critical infrastructure industry impacted under the Executive Order to frame its cybersecurity responsibilities under risk-based principles that meet an individual company's cybersecurity needs. The preliminary Framework accounts for the level of cybersecurity maturity and complexity that each critical infrastructure industry participant faces and provides privacy protection models that will help each member build appropriate protections into their cybersecurity practices. As a voluntary framework, it is up to each participant to incorporate the practices that best fit their industry and to provide feedback to NIST and other sector members on the effectiveness of the framework strategies and to suggest further practices that can enhance the framework going forward.

2111 Wilson Boulevard, Suite 400
Arlington, VA 22201-3061
(703) 522-1820 • (703) 522-1885 Fax
www.NDIA.org

Sharing, Liability Protection, and Incentives Should be Anticipated by the Framework:

Adoption of the voluntary framework will be made easier by the tiered layers of participation in the Framework Core, allowing an immature organization to create a relevant set of services and processes aligned with their unique operational support needs, and a mature organization to do some form of mapping and gap filling, or confirm the viability of their cybersecurity. Despite all of the good efforts from Private Sector and Government contributors, the Framework is just one component of a predictive cybersecurity process that should also include:

- Effective information sharing between government and private sector partners, including classified information, in real time.
- Information sharing liability protection to safeguard companies that participate in information sharing activities in good faith.
- Appropriate incentives for companies to develop proactive, preventive and predictive capabilities for cyber defense.

While these three crucial components must be properly addressed by legislation, the preliminary framework should anticipate the implementation of these components in order to avoid drafting a framework that will become dated once legislation is passed. For example, the Framework Core's functions to identify, protect, detect, respond and recover would be enhanced by information sharing. A business following the preliminary framework would not understand that the government may have tools to help manage and/or interpret risk.

The Framework's "Voluntary" Purpose should be Emphasized Better:

The language of the preliminary framework should also be revised to make clear that the framework should not inadvertently create mandatory checklists out of sub-categories as a matter of convenience for a lack of current application experience by end users, regulators or industry associations. This is contrary to the spirit of the NIST framework and Executive Order 13636, which ordered the framework created. In order to avoid unintended consequences from such an approach, we recommend that as implementation proceeds, NIST should also publicly communicate and provide relevant, practical examples of how to apply a tiered approach with detailed explanations of the risk maturity that defines each tier. More mature companies, organizations and agencies may have an existing understanding of the concept, but for less mature companies, organizations and agencies, further feedback could be helpful in order to understand how to scale within the framework.

Among some of our DIB members, there is also a risk that the cybersecurity framework will not be cost-effective and will be disruptive to their businesses if government agencies misinterpret the purpose of the framework. With regard to federal government contracting, the development of the

2111 Wilson Boulevard, Suite 400
Arlington, VA 22201-3061
(703) 522-1820 • (703) 522-1885 Fax
www.NDIA.org

voluntary framework is a critical first step in developing best practices for cybersecurity and information protection. But we strongly recommend that NIST ensure that the "voluntary" framework envisioned by Executive Order 13636 not become a "mandatory" or "de facto" requirement for future contracts by specifically addressing federal agencies in the framework. The purpose of the framework is to create voluntary best practices at the discretion of *companies* and not federal agencies. Of course, federal agencies seeking to include cybersecurity elements as requirements in their contracts can utilize the framework to determine where the greatest risks lie and create tailored acquisition requirements based on that assessment. This includes assessing what should be flowed to lower tiered subcontractors in the cyber supply chain, what exists within current infrastructure roles, and the government's role in managing and administering contracts with cybersecurity requirements. The framework can thus be the foundation document for referenced best practices (i.e., those in the NIST framework) in which each contract requirement can be verified and validated, but these best practices should serve only as a guide until the requisite acquisition rules are published.

We note that recent DFAR regulations have now set a floor for basic cyber housekeeping for DoD contractors for use in situations where unclassified controlled technical information is residing on or transiting contractor information systems. These regulations were implemented after public comment and are independent of the cybersecurity framework – which is the process that we support. We expect further acquisition rules and best practices to develop over time to meet different cybersecurity contract demands, some of which may align with the NIST framework, but others that may not, for many reasons unrelated to the adoption of a common framework.

Other Comments:

Our members also suggested the following, more detailed, additions to the Framework for NIST's consideration:

1. The Framework should specify the roles and responsibilities of operators of critical infrastructure and the suppliers who manufacture the products to minimize misinterpretation that all security lies with "products" and or all security lies with the "operators" of the products.

2. In order to better express existing practice, the Framework should reference Building Security In Maturity Model (BSIMM) as a de-facto security standard in its informative reference list.

3. To better strengthen cybersecurity, the Framework should promote a continuous improvement process. Not until the Respond and Recover phase is there a reference about improvement and then it does not take into account explicit lessons learned. Nor is there an acknowledgement that when there are organizational changes like a new acquisition or a major change in assets that the organization should determine if the current security posture is still adequate.

4. The Framework lacks specific Adoption/Conformity guidelines. Such guidelines would provide organizations with a standard process to assess the maturity of its implementation of the

2111 Wilson Boulevard, Suite 400
Arlington, VA 22201-3061
(703) 522-1820 • (703) 522-1885 Fax
www.NDIA.org

Framework Functions and Profiles. Organizations are invited to "self assess" compliance and assign current and target tiers, but there are no objective criteria for the assessments, thus no common language between organizations. Since supply chain cybersecurity is a growing concern, creating a common set of standards/criteria and language for the private sector is essential to grow trust.

5. The Framework needs to emphasize the importance of a skilled cybersecurity workforce to raise the level of technical skills of those who operate critical infrastructure. An organization's skilled workforce should be part of the Framework Core. Currently, it is relegated to section C.4 of Appendix C. Consider including an informative reference list which contains cybersecurity certifications and corresponding summaries of competencies that each certification provides to help organizations understand their current and future needs.

6. The privacy standards that NIST sets out in Appendix B could be disruptive to a company and create potentially crippling costs. We believe privacy and cybersecurity go hand in hand. Although the inclusion of privacy standards in the Framework is important, a privacy methodology that includes open-ended and burdensome mandates could serve to discourage organizations from adopting the voluntary Framework. For example, the first methodology in Table 3 of Appendix B would require a company to identify Personally Identifiable Information "that may transit the organization's systems, even if the organization does not retain such information." Such a task, which is envisioned for an agency, may be cost prohibitive to a private company and raises many concerns that could force a company to be non-compliant from the outset. We urge NIST to review and revise the Framework's privacy methodologies (Appendix B) to ensure that each methodology is narrowly focused to include and reflect consensus private sector practices relating to privacy. By including an appropriately tailored privacy methodology as part of the Framework base document, rather than an appendix, NIST will encourage the adoption of the Framework and allow an organization to complement its cybersecurity program with a privacy program that addresses privacy issues directly implicated by the organization's approach to cybersecurity.

In summary, the NDIA Cyber Division is very pleased to support, consistent with these comments, NIST's endeavor of building a cybersecurity framework to improve and ensure our critical infrastructure systems are secure. The draft preliminary framework, while still needing important revision, represents another step towards achieving its goal of establishing a baseline for those developing cybersecurity risk management programs for their enterprise. Our members look forward to continued participation in the ongoing effort to protect our companies, our customers, and our nation against cybersecurity threats.