LINEAGE
TECHNOLOGIES
Cyber security: American made.

August 26, 2014

Ms. Diane Honeycutt
Mr. Adam Sedgewick
National Institutes of Standards & Technology
100 Bureau Drive, Stop 8930
Gaithersburg, Maryland 20899

Ms. Honeycutt/Mr. Sedgewick:

Lineage Technologies, LLC appreciates having the opportunity to comment on the implementation of the NIST Framework for Improving Critical Infrastructure Cybersecurity.

The Framework is an excellent tool for addressing cyber security. Two features distinguish the Framework in terms of adoption. The first deals with assigning risk. The second deals with the unfortunate nature of current affairs, namely that intrusions and losses are continuing unabated despite the release of the Framework.

Where risk calculations are determined to be de-minimis, firms generally eschew action.

When firms implement thorough reviews of risk, and examine applicable standards and best practices they often discover the limits to which they can go on their own to meet cyber security threats (see Q4). The interconnected nature of businesses today requires broad adoption of Framework components for cyber security to be achieved. Thus, even when firms determine the threat they are exposed too, and take measures to insulate themselves they remain exposed.

Halting and inconsistent implementation of cyber security measures is the result, although circumstances are likely to improve as adoption spreads.

Currently, most firms choose to absorb the risk of cyber intrusions, as a cost of doing business, recognizing that their actions alone cannot deter/prevent such attacks. This was reflected in the conclusions of the World Economic Forum-Insight Report: <u>Risk and Responsibility in a Hyperconnected World</u>, (copy attached). That report concluded:

1. *For most companies across sectors and regions cyber resilience is a strategic risk;*
2. *Executives believe they are losing ground to attackers;*
3. *Large companies lack the facts and processes to make effective decisions about cyber resilience;*
4. *Concerns about cyber-attacks are starting to have measurable negative business implications in some areas; and*

5. *Substantial actions are required from all players in the cyber resilience ecosystem.*

Anxiety surrounding cyber security was also evident in comments made to the Senate Committee on Armed Services July 10, 2014 by Admiral William Gortney at his confirmation hearing to command NORTHCOM:

> *"…it is may professional opinion that we are a little bit behind – we as a nation are behind in our ability to defend critical infrastructure…I think the greatest threat that we have is the cyber threat…to our critical infrastructure, to the power grid, to our banking system."*

Admiral Gortney's comments mirror those of Chairman of the Joint Chiefs of Staff, General Martin Dempsey. Earlier that month he stated:

> *"We have sectors within our nation that are more ready than others,but we do not have a coherent cyber strategy as a nation. And I understand why…there are some big issues involved with achieving that kind of coherence – issues related to privacy and cost, information sharing and all of the liabilities that come from an absence of legislation to incentivize information sharing"*

Some have argued that the Framework has the potential to shape standards not only for critical infrastructure firms but also for all firms doing business in the US, creating a legally binding standard-of-care.[1] Evidence of this will have to await the development of case law.

McAfee noted different security and risk management motivators for securing intellectual property among firms located around the world in its 2011 report: Underground Economies: Intellectual Capital and Sensitive Corporate Data Now The Latest Cybercrime Currency.[2] In an earlier assessment McAfee found that regulations are the key motivator in security decisions made by firms located in Dubai, Germany, Japan, UK and US, while firms in India and China listed competitive advantage as their key motivator. Notwithstanding these conclusions, many argue that regulations will stifle effective interventions by inculcating static compliance (box checking) rather than adaptive cyber security measures.

These comments point to the need to do substantially more to ensure that the Framework and its components are adopted. Absent a broad adoption of the Framework, regulations may be needed to stimulate adoption.

Answer to specific Questions posed by NIST are listed below:

Current Awareness

[1] With Permission of Scott J. Shackelford, JD, Ph.D., on behalf of himself and Andrew A. Proia, JD, Brenton Martell, JD, Amenda

[2] http://www.ndia.org/Divisions/Divisions/Cyber/Documents/rp-underground-economies.pdf.

Q1 What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations?

A1 Awareness among organizations representing critical infrastructure components is strong. Some such as the Utilities Telecommunications Council, Aerospace Industries Association, American Chemistry Council, American Bankers Association, American Bar Association, National Association of Investment Companies, American Petroleum Institute, National Defense Industry Association etc. have engaged in significant outreach to their members, presenting conferences, and providing advice and counsel while also working with NIST and DHS to address issues of concern. Broad awareness was also generated from consideration of cyber specific rules by DOD, EPA, FERC, FCC, GSA and other federal Departments and Agencies, although the Administration's decisions to rely primarily on the NIST Framework to inculcate cyber security responses by industry has muted their effect.

Awareness among large firms is almost universally accepted, but greatly overstates the case. In 2014 Lineage Principals spoke at conferences covering cyber security, aviation security, petroleum refining, chemical plant security, and protection of electric power and transmission/distribution facilities. At each of these events, we encountered large company executives who were charged with cyber security (CIOs, CISOs, VPs for O&M, Facilities, etc.). Many had an understanding of the Framework, its structure and/or content. However, we learned that they rely upon third-party providers for their IT and so were relying upon their vendors to provide necessary security enhancements. Outsourcing of such services is sound from a business perspective, but illustrates why understanding of the threat by firms, large and small, does not always result in direct and immediate adoption of Framework principles. Until everyone takes ownership of the threats to which they are exposed, adopting the Framework will be a haphazard affair.

This is worse for medium sized and small businesses. SBA, and the House and Senate Committees on Small Business have each beseeched NIST to create more outreach mechanisms to address the needs of this community. If there is a critique of the NIST Framework outreach effort so far, it is that NIST has not done enough to reach this community. This is not to say that NIST has not engaged medium sized and small business, but that those efforts have not been sufficient. Among the items being sought by this community are clear examples of processes firms can use to design and deploy cyber security measures. While this runs contrary to the voluntary nature of the Framework, NIST must recognize that often times medium sized and small businesses do not have the time or resources to evaluate standards and best practices, and develop workable cyber security plans on their own. They can, however, adopt plans that are developed for them. Therefore, NIST should invest in developing a number of transferable plans to cover firms that need such support (see answer to Q7).

The need for this was made abundantly clear in the Target breach, where an air conditioning and heating contractor's IT system became the conduit through which assailants gained access to Target's point-of-sale system, and enabled the theft of confidential information affecting over 100 million persons.

In an industrial context, Boeing has adopted a program of shared cyber situational awareness where its partners/suppliers must move from a safety culture to a culture of safety and security. Adherence to cyber security standards is an essential component of their program. What is instructive is that Boeing wants active engagement with the US Government through public-private research partnerships to reach this goal. Clearly, this speaks to the need for more engagement.

<u>Q4</u> **Is there general awareness that the Framework:**
a. Is intended for voluntary use?
b. Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cyber security factors into risk assessment?

<u>A4a.</u> YES! Many of the firms we encounter view the NIST Framework as something they can look at, but for reasons of cost, complexity, or resignation to threats, leads them to postpone adoption. Scholars will debate the wisdom of this stance. We believe that delay in adoption will persist until contracts, case law or regulation makes adherence to cyber security standards mandatory.

<u>A4b.</u> Our exposure involves CIOs, CISOs, and VPs for O&M and Facilities. Within this community we have observed that there is significant tension within firms regarding cyber security investments and other corporate priorities. Despite considerable new investment in continuous monitoring, kill-chain processes, and adjusting prices for their products and services to factor in cyber threat expenses and to offset losses, significant new breaches and data thefts continue. In practical terms, the standards and best practices referenced by the Framework, when implemented, have not yielded consistent and measureable improvements in security. Data losses by those considered the very best at cyber security (e.g. DHS, DOE, DOT, Ebay, etc.) speak volumes about the difficulty in securing IT systems. This is noted often as the main disincentive to investing in more security. McKinsey reports in its June 2014 **<u>Why senior leaders are the front line against cyberattacks</u>** *"that understanding the issue is quite different from effectively addressing it. A number of structural and organizational issues complicate the process of implementing business-driven, risk-management oriented cyber security operating models, and that sustained support from senior management can ensure progress and ultimately mitigate the risk of cyberattacks."* This is particularly so where supply-chain matters is concerned. Many customers believe that they will remain victims of taint and counterfeit components, systems and software so long as supply chains originate from abroad.

Q5. **What are the greatest challenges and opportunities – for NIST, the Federal government more broadly, and the private sector – to improve awareness of the Framework?**

A5. Lineage believes NIST must do more to illustrate practical methods for implementing the Framework. One of the most compelling examples of how NIST might go about this is found in DOE's Energy Sector Control Systems Working Group (ESCSWG) April 2014 recommendations to utilities contained in: **Cybersecurity Procurement Language for Energy Delivery Systems.** While mirroring elements of the standards and best practices referenced by the Framework, this document serves as a simple, practical exemplar. The simplicity of this document is found in proposed procurement language users can immediately incorporate in their contracts:

"2.4.3 The Supplier shall not, unless specifically requested by the Acquirer, allow multiple concurrent logins using the same authentication credentials, allow applications to retain login information between sessions, provide any auto-fill functionality during login, or allow anonymous logins, unless specifically requested by the Acquirer."

"2.9.1 The Supplier shall identify heartbeat signals or protocols and recommend which should be included in network monitoring. At a minimum, a last gasp report from a dying component or equivalent shall be included in network monitoring."

"2.7.3 The Supplier shall provide a method to restrict communication traffic between different network security zones. The Supplier shall provide documentation on any method or equipment used to restrict communication traffic."

It cannot be overstated that a hand-up such as this is far better than a broad treatise. The Framework has more to do with treatises, and should be altered, to the extent possible, to reflect the DOE document format.

Our comments apply as well to many of the questions contained in the RFI found in the second category: *Experiences With the Cybersecurity Framework.* In the interest of brevity we have not repeated them.

Respectfully ours,

Thomas R. (Tom) Goldberg
Principal
Lineage Technologies, LLC
1455 Pennsylvania Avenue, NW
Suite 400
Washington, DC 20004-1017
(202) 744-4509