
December 4, 2013

Information Technology Laboratory
ATTN: Mr. Adam Sedgewick
National Institute of Standards and Technology
10 Bureau Drive, Stop 893
Gaithersburg, MD 20899

Mr. Sedgewick:

In general we share the perspectives incorporated in the comments submitted by Mr. Robert Bigman. His comments call for illustration of implementation mechanisms that can be employed. At this stage in the Framework development that is required, either as examples of what the referenced standards mean or as measurable indices that can be audited. NIST should direct its remaining efforts at illustrating Framework implementation approaches so as to incentivize business practice changes and make adoption of cyber security manageable.

The emphasis in the framework on risk assessment is extremely valuable, but may not be a cost-effective route for implementation, especially for small business. The unavailability of staff, expertise, and understanding of threat horizons makes adoption burdensome. For these reasons, we recommend that NIST illustrate common sense business practices that will enable cost-strapped firms to reduce their exposure to cyber threats. We recommend that NIST construct a list of common sense approaches small firms can emulate that address the bulk of threats they are likely to confront (e.g. regularly up-grade software/hardware; keep software licenses up-to-date; religiously download software patches; buy only from OEMS/OCMs and licensed distributors; keep current with government/industry reports regarding software/hardware vulnerabilities; employ trained and certified personnel to manage IT systems; limit access to key information; employ multi-factor authentication and related mechanisms to implement the same; etc.). While NIST is loathe issuing prescriptive instructions, or to favor specific approaches, it must incentivize a compliance culture, and that can be best accomplished through illustration.

This will also serve to help harmonize the Framework with rules and regulations issued by other Departments such as DOD's DFAR modifications to 48 CFR 204, 212, and 252 regarding the "Safeguarding [of] Unclassified Controlled Technical Information". DOD's new rule **does not provide regulatory relief for small businesses**. It requires, at a minimum, compliance with NIST 800-53 or similar standards. By denying small businesses a lower threshold for compliance DOD placed emphasis on "securing the data" and defining that as the Department's principal intent. This emphasis provides a useful focus NIST can adopt. However, it too falls short in helping to provide perspective on practical mechanisms for accomplishing this goal. NIST can provide yeoman's service here by making 800-53 colloquial, and providing basic steps that can lead to this objective without being prescriptive. By so doing, NIST can illustrate processes and procedures that otherwise will frustrate users with images of gargantuan assessment undertakings, 'fortress balance sheets' and complex calculations large firms and enterprises can well afford to develop.

Several of the comments received by NIST clearly call out inconsistencies between sections of the Framework and the appendices that can confuse users. We concur with observations relating to maturity models and mechanisms for scoring; and the inability to address common methods between assessment and flow-down activities. These inconsistencies complicate implementation by businesses in general, and will retard adoption of the program.

Companies' ability to respond to unknown cyber threats is more and more dependent on next generation cyber security technologies. NIST must assure that hardware and software vulnerability fixes and active countermeasures are scored as compliance indices. If DOD, DHS, or other federal Departments or Agencies certify products in this manner, those products should be immediately cataloged as indices for meeting Framework requirements. This will allow NIST to better anticipate and account for hardened IT devices, and more secure software, and their capabilities to close access to adversaries and malefactors.

PII must be baked in to the process as solutions are implemented. The NIST Framework awkwardly presents this issue as a bolt on. The final Framework should make PII a central tenant that must be considered irrespective of approach.

Lastly, we concur with recommendations by others that the Framework be harmonized with other NIST standards. For instance, the Framework fails to mention "data-in-use". When considering data lifecycles (at rest, in motion/transit, in use), this could be interpreted as leaving a "data in use" hole in the Framework.

Sincerely yours,

Thomas R. Goldberg
Principal
Lineage Technologies, LLC