From: **Michael J. Lewis**
Date: Fri, Apr 7, 2017 at 1:50 PM
Subject: International Information Integrity Institute (I-4) Comments to Cybersecurity Framework Draft Version 1.1
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

The International Information Integrity Institute (I-4) welcomes the opportunity to comment upon the Version 1.1 draft of the "Framework for Improving Critical Infrastructure Cybersecurity."
Since its launch in 1986, I-4 has consistently strived to be the world's leading forum for information security professionals. Many members hold senior roles within large, global organizations across a diverse range of industries, with a common dependence upon IT along with sophisticated risk management and security operations. I-4 member organizations operate in critical infrastructure sectors of energy, communications, information technology, financial services, healthcare and public heath, transportation, and government and use the Cybersecurity Framework in myriad ways. A subset of I-4 members welcomes the opportunity to share our perspectives on the draft Framework, first providing a few observations and then answering the seven questions posed in the "Notes to Reviewers on the Update and Next Steps" introduction to the draft.
I-4 members encourage NIST to continue global outreach programs to help align the Cybersecurity Framework with cybersecurity regulations or requirements across the world. A common taxonomy and method benefits multi-national I-4 members who then can use common processes to address cybersecurity issues rather than having to devote scarce resources to managing different nuances of different regimes across the world. Alignment also means that I-4 members are not forced into exclusively using the Cybersecurity Framework but can leverage that work if they are compelled or choose to use other cybersecurity standards.

I-4 members likewise encourage NIST to continue to revise the Cybersecurity Framework Core with updated Informative References and relevant categories and subcategories. One example would be including a new category of "Using Threat Intelligence" under the "Detect" function; sub-categories would include "Automated Indicator Sharing" and "Data Analytics". As virtually all critical infrastructure sectors have at least one Information Sharing and Analysis Center (ISAC) and with the growing acceptance of the STIX/TAXII information sharing specifications, I-4 feels this category is sufficiently defined to be included in the framework core.

I-4 members agree that the new content on Supply Chain is quite useful. Some I-4 members handle critical data of customers and call out a specific set of supply chain activities for their clients and risk management. There is concern, though, as to the precedent set by making Supply Chain a category. Supply Chain, much like "cloud", "internet of things", "mobility" and other themes, can be considered as a "lens", providing context for thinking about cybersecurity. Adding such items as categories replicates common sub-categories (risk assessment for "cloud", "internet of things", and "mobility", "contracts" for "cloud" and "mobility", etc.) and thereby grows the Framework core needlessly.

Supply chain may be a sufficiently important issue that it merits the attention brought by being a separate category but once sufficient progress is made addressing the issue, NIST should consider dropping the supply chain category and distributing the supply chain sub-categories appropriately through the framework core.

The following provides specific answers to the specific questions posted in the "Note to Reviewers on the Update and Next Steps" section of the draft:

- Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?

  [I-4] As stated above, we believe "(using) threat intelligence" is sufficiently mature to be included as its own category within "Detect".

- How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?

[I-4] The updates for "supply chain" provide a good framework for managing this difficult problem. The additional of authentication and identity proofing to the previously named "Access Control" category brings this section more in line with the "Identity and Access Management" programs which most companies have. The measurement text is a good first step in helping to define metrics and measures although additional treatment, either within the framework proper or perhaps better in a guidance document would help step an organization through the process.

- For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?

[I-4] No

- For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?

[I-4] These changes will not cause existing users to drop framework use nor cause those not using to start

- Does this proposed update adequately reflect advances made in the Roadmap areas?

[I-4] Yes although we believe "Automated Indicator Sharing" and "Data Analytics" are mature enough to be included in the framework core as a sub-category to a new Threat Intelligence category within Detect.

- Is there a better label than "version 1.1" for this update?

[I-4] Perhaps (the term is vague) but "version1.1" is good enough.

- Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?

[I-4] Items added to the draft, "Authentication", "Federal Agency Cybersecurity Alignment", and "Supply Train" can be removed. If our recommendation regarding the "Threat Intelligence" category is accepted, then "Automated Indicator Sharing" and "Data Analytics" can likewise be removed. Additional work is needed on "Conformity Assessment".

The “Cybersecurity Workforce” is not specific to the framework; NIST should continue to work this issue via efforts like National Initiative for Cybersecurity Education (NICE) but there may not be a need to maintain this in the framework. “International Aspects, Impacts, and Alignment” is critical but this should be handled within the Introduction to the Framework rather than kept within the Roadmap document.

That would leave “Technical Privacy Standards” as the remaining item from the original Roadmap. One could consider adding Internet of Things as a roadmap issue. Issues which need work in this area are a definition for “Internet of Things” as well as treatment of both Industrial Internet of Things (which business will deploy to gain value) and consumer devices (which will enter the workplace as refrigerators, projectors, thermometers and other such devices are replaced by newer versions.)

Thank you for the opportunity to comment and further the discussion of this important document.

Sincerely,

Michael J. Lewis
Policy and Framework Advisor, Chevron
Chairman, International Information Integrity Institute (I-4) Member Advisory Committee.