From: Greg Jaeger
Date: Mon, Apr 10, 2017 at 11:54 PM
Subject: ATI feedback for the Draft Cybersecurity Framework v1.1
To: cyberframework@nist.gov

ATI is pleased to provide feedback on the Draft Cybersecurity Framework v1.1 in the attached document. We look forward to further participation with NIST and the Cyber Security community to mature the overall security posture.

Regards,

Greg

Greg Jaeger
Senior Program Manager
Advanced Technology International
315 Sigma Drive, Summerville, SC 29486

[Attachment Below]

FEEDBACK ON THE NIST CYBER SECURITY FRAMEWORK V1.1

10 APRIL 2017

Overview

ATI's feedback includes overall recommendations with some specific comments. The general observation is that the Cyber Security Framework (CSF) is heavily textual and can greatly benefit from illustrations that can better explain concepts while reducing the narrative footprint. Foremost is the Cyber Security Framework's relationship to the Risk Management Framework (RMF) and government and ISO standards. The Cyber Security community frequently asks if the CSF will replace the RMF; more effort is needed to dispel this confusion. Another area where illustrations or charts can improve reader comprehension is in the interplay of the (5) Functions; these may also require Use Cases to demonstrate where multiple functions overlap and closely integrate.

Most version 1.1 changes are disproportionately applicable to Supply Chain Risk Management (SCRM). The overall impression of the SCRM changes is they seem inappropriate and break the readability of the framework. The RMF references identified in the new SCRM categories are already captured in other Categories. Moreover, no SCRM categories do not warrant the dense narratives and misapplied sections in the document body. The framework's appeal as a flexible, lightweight utility has been eroded with SCRM specificity. Predictably, CSF v1.1, in its draft form, is less likely to be adopted by other IT communities including Agile and DevOps. More details are explained in the comments below.

Specific Questions

1. Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?
    a. Framework Version 1.1 does not sufficiently explain the concurrency and simultaneity of the five core functions. The CSF has helped codify risk classification during information gathering, communication and prioritization to the client/customer. However, the core functions are commonly interpreted as cybersecurity lanes/roles with varying priorities. The CSF functions should be recognized as simultaneous activities that require cross-collaboration. We have observed active programs where the stakeholders (PM, operations, IAO, contractors, hosting provider, etc.) establish monolithic activities under the guise of compliancy and accountability lines. When the functions are confluent (continuous collaboration, monitoring, trend analyses, etc.) then cybersecurity is elevated from an annual compliance checklist to a security posture. In other words, the current framework matrix implies a siloed view of each core function that, when aligned to responsibilities and accountability roles, will likely be satisfied by disparate groups which stifles collaboration and weakens an overall cybersecurity awareness posture. Recommend the framework document emphasize and illustrate the significance and importance of concurrent and continuous activity across all five functions.
    b. The draft v1.1 framework continues to self-define as applicable to "critical infrastructure" which unfortunately obfuscates its applicability in all IT fields. For example, the CSF is directly applicable to the DevOps community which has increasing popularity because it emphasizes continuous monitoring, feedback and improvement using teams that share information and collaborate across defined roles. The CSF can remedy this oversight with examples, use cases and/or implementation strategies that

describe how the functions and categories are applicable across all roles (Design/Development, Operations/Security, and Program/Risk Management).

2. How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?
    a. The cybersecurity ecosystem is excessively focused on compliancy before security for which the CSF unwittingly encourages. This is an unfortunate consequence resulting from government agencies prescribing standards, frameworks or methodologies. The disclosures that indicate the CSF is "voluntary" are largely ignored. The compliancy checklist lure is exacerbated by an emphasis on recurring assessments to achieve higher implementation tiers. A recommendation to counter this trend is to include Use Cases that describe the "so what" of the requisite actions. For example, consider "*IS.AM-2 Software platforms and applications within the organization are inventoried"*. The category references NIST 800-53 CM-8 which lists so many attributes that the need for automation is assumed; largely, because the risk is focused on networks with a large array of devices. An excessive attribute list might lead to a false sense of value; more data must be better. Equally, the attribute list may be inadequate if the system owner cannot adequately identify vulnerable components from the inventory. A Use Case can best illustrate the utility of the IS.AM-2 and recommend questions, attributes, and artifacts that validate the inventory results can be usable to measure and reduce risks.
3. For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?
    a. n/a
4. For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?
    a. n/a
5. Does this proposed update adequately reflect advances made in the Roadmap areas?
    a. The Framework Roadmap has not been updated since February 2014 although it claims to be a "living document" that "will continue to be updated and improved as industry provides feedback on implementation." The original Roadmap predates the release of Cybersecurity Framework v1.0 and should be revisited in concert with the CSF updates.
    b. The information sharing objective was not achieved. Metrics and measures to increase security posture was not improved through smoothing comments or adding additional regulations. The latter action provides a road to compliance, not cybersecurity. Rather than update to the latest Federal governance and guidance, the Framework should be extended to provide more explicit, regulatory-driven measurable/observable benchmark/criterion.
    c. Rather than a checklist assessment, the framework should/could encourage objective-based evidence to look for with an ability to demonstrate and assess efficiencies. These objective criteria met requires more than a check. For example, consider: *PR.IP-10 Response and recovery plans are tested.* Taken with the required NIST 800-53 CP-4, IR-3, and PM-14 requirements; the criteria must evaluate the effectiveness and readiness of the plans to realistic, plausible scenarios. Incident Response plans must complement the detection, monitoring, collaboration, and reporting sub-processes and provide triggers to a Disaster Response, Reconstitution, Planning. The CSF category and

outcomes are weak when described without qualifications to observable, evidence criteria.

6. Is there a better label than “version 1.1” for this update?
    a. n/a
7. 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?
    a. Several of the roadmaps pertain to “information sharing”; however, sharing information does not address the real problem of timely, accurate and complete information. An independently led consortia should tackle specific barriers that inhibit (or slow) cybersecurity “information sharing”. From our recent experience, real events highlight significant gaps in determining vulnerabilities, notifications, exploit techniques, mitigations and solutions that warrant information across all Functions and involving all stakeholders. Over dependency to the National Vulnerability Database and similar vulnerability notification processes is a path of failure for proactive and timely protection.

Additional Comments:

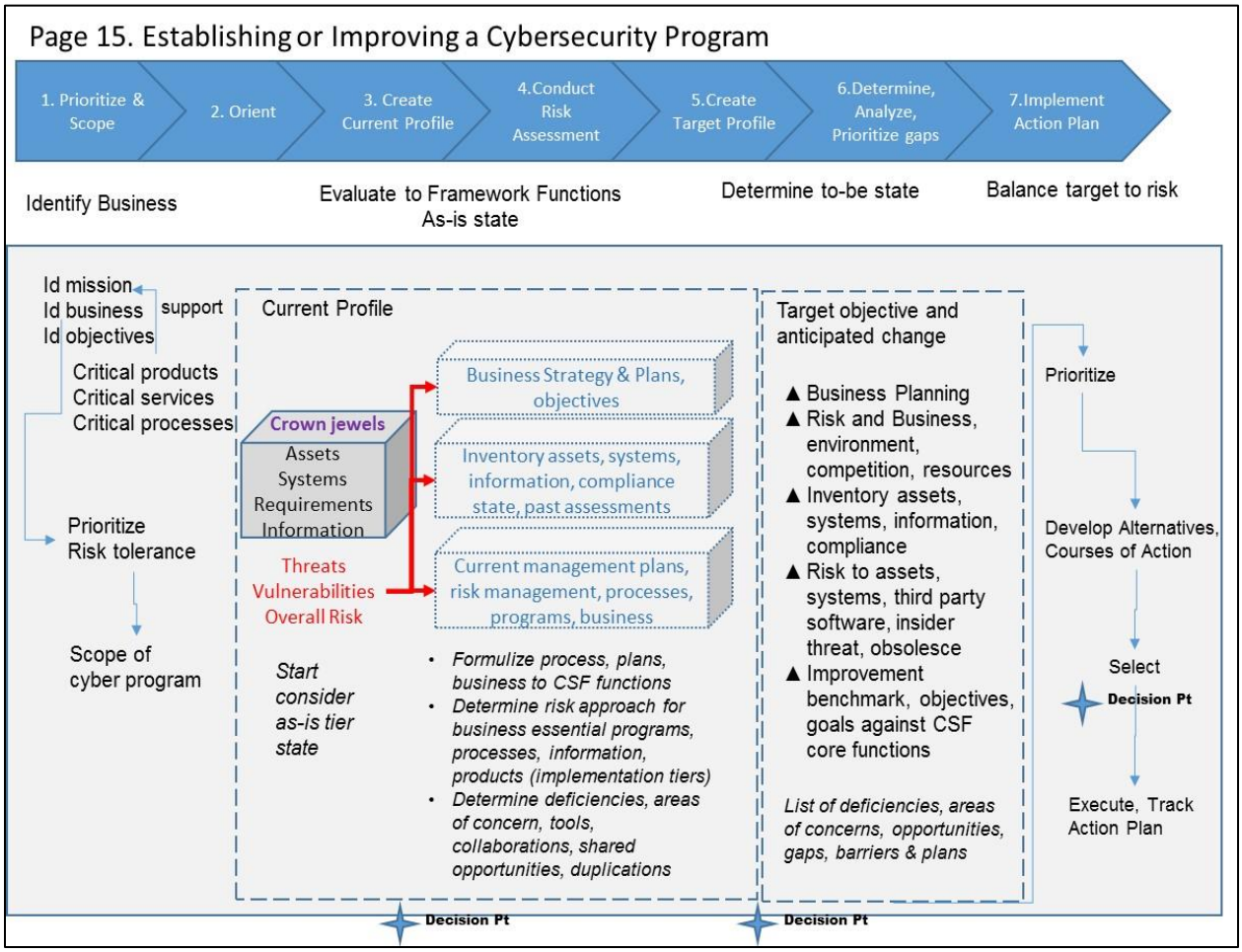
1. Framework Implementation Tiers provide definitional elements to assess or characterize the organizations risks, processes, and programs.
    a. As stated, tiers do not represent maturity level. The 'tiers' should be more demonstrative as based on objectives, and thereby characterize the risk and effectiveness level (if not a maturity level) based on the product, process, business evaluated. Risk is a function of likelihood and impact and some process and products are not as significant if loss or compromised as others; therefore the profile determination is most critical to determine. To help distinguish the obvious community confusion in respect to these tiers and falsely align with Capability Maturity Model Integrated (CMMI) maturity levels, recommend the four tiers be renamed for what they represent:
        i. "Partial" to represent an unbalanced across business and partial applied to select program/system.
        ii. "Risk Informed" to "Risk Awareness" to represent awareness to risk management across multiple programs/systems however not repeatable or shared across programs and systems. Due to contracts, there are credible reasons why this is adequate for some businesses.
        iii. Change "Repeatable" to "Compartmentalized" to separate confusion with CMMI and more accurately reflect that cybersecurity requires collaborations with clients/customers/teams that must complement on products/process/systems. In this tier, cybersecurity in depth is strong at each level (infrastructure, application, enterprise, and perimeter).
        iv. Lastly, "Adaptive" should be "Institutionalized" reflecting the company collaborative use of threats, indicators, techniques to orchestrate standard suite of tools, processes, and people across many systems/products/programs.
    b. An illustration would better communicate the scope of the Implementation Tiers rather than long, textual narrative with convoluted sentences to describe this difficult and

often confused section. Recommend changing the title and language (see above) and provide as a table. Further, improve this section with a list of questions with answers to characterize and understand the risks and what is and is not being performed, coordinated, and integrated into complimentary processes.

   c. The statement "Implementation Tiers allow organizations to understand how they fit into the larger cybersecurity ecosystem" is inaccurate when each organization has unique risks and measuring methods. The Implementation Tiers now read like a maturity model that organizations can be compared against. If the tiers are strictly intended for self-assessment then claims of inter-organizational comparison should be stricken.
   d. The Cyber SCRM additions to the Tiers are too niche. Enterprises should assess all risks for which supply-chain risks are a subset. Recommend striking the SCRM additions in the Tiers.

2. The Supply Chain Risk Management (SCRM) changes are too specific and detract from the utility of the framework.
   a. The Cyber SCRM additions do not flow. SCRM is an important, less managed, and critical element in the cybersecurity program however is just one of many elements that must be within (and across) the Software Development Life Cycle (SDLC) decisions and protection. Recommend appropriate discussions on risk management and mitigation of open source, COTS, and supply side software that does present unique challenges in your program/system/business.
   b. The Buying Decisions section is specific to SCRM additions and seems to be out of place in the CSF. If this section must be retained then it should be combined in the Stakeholder/SCRM/Acquisition section.
3. Measuring and Analysis
   a. Section 4.0 states "The ability of an organization to determine cause-and-effect relationships between cybersecurity and business outcomes is dependent on the accuracy and precision of the measurement systems (i.e., composed of the "resources" highlighted in ID.AM-5)." The examples in ID.AM-5 implies the relationships are purely mechanical (simple) when there is much more involved such as described in 800-53 RA-3 (Risk Assessment). Recommend striking the statement or more accurately describing how an organization can determine cause-and-effect relationships.
   b. This section seems to be written directly for the SCRM with an emphasis on trust relationships among stakeholders. Metrics, measurement and analysis are intrinsic functions in all organizations and aligned with business goals and objectives at the corporate, client, legal, partner and industry levels. Recommend a rewrite of this section with the premise that cyber security is part of the core requirements that must be measured and collectively assessed to determine overall risk.
   c. The "Stakeholder" section would be better served if it described how stakeholder roles are symbiotic and overlap to address the core CSF functions.
4. Recommendation to provide diagram versus long narratives
   a. The (7) steps for Establishing or improving a cybersecurity program can benefit with an illustration. Recommend the (7) steps be aligned with Business Strategy Planning

instead of an isolated set of activities that somehow feeds business decisions later. The following rough, brainstormed diagram is a starting point.



Contacts:

Greg Jaeger
Program Manager

Brian Eleazer
System Engineer