From: **Andras Szakal**
Date: Mon, Apr 3, 2017 at 11:31 AM
Subject: IBM Comments to NIST CSF V1.1
To: cyberframework@nist.gov

Please accept IBM's comments on the Request for Information (RFI) from the National Institute of Standards and Technology (NIST), regarding the Cybersecurity Framework V1.1. Generally, the document is evolving in the right direction but would benefit from additional explicit recommendations (contained in comments below). We do think that using a standard such as ISO20243 would make these recommendations more explicit especially considering that the government has deeply invested in that standard.

Please send questions or comments regarding this input to:
Andras R. Szakal
VP & CTO IBM US Federal

Document as a whole:

Need to provide a profile that defines how to efficiently combine traditional supply chain risk, lifecycle management and secure engineering. Using a standard like ISO-20243 would make this much easier and more explicit.

Specific Comments:

1) Location: line 370 - 372
Rationale: Suggest more explicit wording around supply chain risk management

Comment:
Change from: Cyber Supply Chain Risk Management – An organization may not understand the full implications of cyber supply chain risks or have the processes in place to identify, assess and mitigate its cyber supply chain risks.
Change to: An organization may not understand their cyber supply chain risk or have the processes in place to identify, assess and mitigate its cyber supply chain risk.

2) Location: line 386-391
Rationale: Complex sentence and concepts - should try to simplify

Comment:
Change from: Cyber Supply Chain Risk Management – The organization

understands the cyber supply chain risk associated with the products and services that either supports the business mission function of the organization or that are utilized in the organization's products or services. The organization has not formalized its capabilities to manage cyber supply chain risk internally or with its suppliers and partners and performs these activities inconsistently
Change to: Cyber Supply Chain Risk Management – The organization understands its cyber supply chain risk, but has not formalized capabilities and processes to consistently manage cyber supply chain risk internally, or with its suppliers and partners.

3) Location: line 409 - 417
Rationale: More Explicit and descriptive wording

Comment:
Change from: Cyber Supply Chain Risk Management – An organization-wide approach to managing cyber supply chain risks is enacted via enterprise risk management policies, processes and procedures. This likely includes a governance structure (e.g. Risk Council) that manages cyber supply chain risks in balance with other enterprise risks. Policies, processes, and procedures are implemented consistently, as intended, and continuously monitored and reviewed. Personnel possess the knowledge and skills to perform their appointed cyber supply chain risk management responsibilities. The organization has formal agreements in place to communicate baseline requirements to its suppliers and partners.
Change to: Cyber Supply Chain Risk Management – Cyber supply chain risk is managed through an enterprise-wide risk management program, which includes formalized policies, processes, and procedures, which is overseen by an enterprise-wide governance mechanism (e.g., Risk Committee or Council) for all risk in the organization. Policies, processes, and procedures are implemented consistently and regularly monitored and reviewed to make appropriate improvements. Personnel possess the knowledge and skills necessary to perform their cyber supply chain risk management responsibilities. The organization has formal agreements in place with suppliers and partners to communicate, update, and enforce baseline requirements.

4) Location: line 443-450
Rationale: More Explicit and descriptive wording

Comment:
Change from: Cyber Supply Chain Risk Management – The organization can

quickly and efficiently account for emerging cyber supply chain risks using real-time or near real-time information and leveraging an institutionalized knowledge of cyber supply chain risk management with its external suppliers and partners as well as internally, in related functional areas and at all levels of the organization. The organization communicates proactively and uses formal (e.g. agreements) and informal mechanisms to develop and maintain strong relationships with its suppliers, partners, and individual and organizational buyers.

Change to: Cyber Supply Chain Risk Management – The organization can dynamically adapt to emerging cyber supply chain threats using real-time information and leveraging the knowledge and expertise of external suppliers and partners as well as internal resources, from functional areas and at all levels of the organization. The organization communicates proactively and uses formal (e.g., agreements) and informal mechanisms to develop and maintain strong relationships with its suppliers, partners, and individual and organizational buyers.

5) Location: line 357-450
Rationale: Believe that Supply Chain Risk Management is very basic and should come before "Integrated Risk Management" and "External Participation" sub-tier categories.

Comment: Please consider moving the "Supply Chain Risk Management" sub-tier category, from the 4th bullet to the 2nd bullet in each of the four tiers.

6) Location: line 485-486 (Figure 2)
Rationale: Would be good to have a diagram that relates more explicitly to the tiers.

Comment: Consider changing this diagram to add implementation tiers to the actions in the figure.

7) Location: line 602
Rationale: Typo
Comment:
Change from: "better manager"
Change to: "better manage"

8) Location: Line 654
Rationale: It seems that although this section alludes to the fact that there is the opportunity to identify additional Informative References, there is in fact no

defined path to do that. After participating for years in the NIST CSF workshops, advocating the need for referencing existing supply chain security standards and best practices, there are still no informative references for supply chain standards, even in this new revision where supply chain is now addressed.

Comment:
This section states the following: "The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there are few Informative References, if any, for a related activity. To address that need, the organization might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices."
While this explains how you can address gaps it doesn't provide a path or describe the method that is used to get an existing standard included as an informative reference. If there is a path for that process (other than submitting comments to the RFC) it would be helpful to understand what that is, including the decision process for accepting an informative reference.

9) Location: line 673 -674
Rationale: All governance activities could have a negative effect on privacy – not just cybersecurity activities

Comment:
Change from: Nonetheless, an organization's cybersecurity activities also can create risks to privacy and civil liberties when personal information is used, collected, processed, maintained, or disclosed in connection with an organization's cybersecurity activities.
Change to: Nonetheless, an organization's governance and cybersecurity activities also can create risks to privacy and civil liberties when personal information is used, collected, processed, maintained, or disclosed in connection with an organization's cybersecurity activities

10) Location: Appendix A the Table of Function and Category Unique Identifiers – Supply Chain Risk Management ID.SC-2 (Sub-Category column)
Rationale: Suggest not tying it explicitely to information systems since it's not in the definition and that addresses only part of the problem.

Comment:

Change from: ID.SC-2: Identify, prioritize and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment
Change to: ID.SC-2: Identify, prioritize and assess suppliers (and partners) of cyber products, components and services using a cyber supply chain risk assessment and management process.

11) Location: Appendix A the Table of Function and Category Unique Identifiers – Supply Chain Risk Management ID.SC. Applies to the informative reference section(s) in the ID.SC category.
Rationale: Because a new category has been added to the Identity function for supply chain (Supply Chain Risk Management (ID.SC)) along with several sub-categories within that category (ID.SC1-ID.SC5), we expected the informative references that were added for these subcategories to include relevant supply chain security standards.

One of the major drivers for the addition of supply chain is to make sure organizations take into account and address risk from products and services they obtain from others. Accordingly, it's logical and important to suggest that they evaluate their suppliers using the analytic approach of the CSF, which includes normative references to applicable international standards and best practices to reduce that risk. Just as the CSF provides normative references for operators to consider as bench-marks for addressing their risks, so it should provide normative references that are relevant to the risk of products and services they obtain from others.

As an example, ISO/IEC 20243, which was developed by The Open Group and approved by ISO as ISO/IEC 20243 is a standard that defines a set of best practices for product integrity and supply chain security, and includes requirements for suppliers through-out their products' life cycles; design, development, outsourcing, manufacturing, integration, maintenance and disposal.
It was developed through an industry-government partnership with major industry IT providers working in collaboration with the US government (DOD/AT&L, DOD/CIO, and NASA) to create the standard and the O-TTPS certification program that identifies organizations who conform to ISO/IEC 20243.
Adding ISO/IEC 20243, as well as ISO 27036 and NIST SP161 would absolutely increase awareness of the threats that business partners should mutually be concerned about and the behaviors that critical infrastructure operators should be asking of their suppliers during the development of the

products before the products or product updates are brought into critical infrastructure.

Comment: Please add the following to the informative reference sections in ID.SC

ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
ISO/IEC 20243 4.1 – 4.2.1.12
D.SC-2: Identify, prioritize and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment process
ISO/IEC 20243 4.1 – 4.2.1.12, Assessment Procedures for 20243 4.11- 4.22
ID.SC-3: Suppliers and partners are required by contract based on global standards or other global guidelines to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan. NOTE: Also suggested a change to this subcategory, that is adding "based on global standards or *otherwise"* per above.
ISO/IEC 20243 4.2.1.4, 4.2.1.5
ID.SC-4: Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted
ISO/IEC 20243 4.1 – 4.2.1.12, Assessment for 20243 4.11-4.22

ID.SC-5: Response and recovery planning and testing are conducted with critical suppliers/providers
ISO/IEC 20243 4.1.2.4 – 4.1.2.6
11) ALTERNATIVE COMMENT/SUGGESTION RELATED [to 10 above]
It might be more appropriate to include a supply chain sub-category in Protect as well (e.g., PR.SC, and move ID_SC-ID (3-5) subcategories and informative references under that new category in Protect:

For Example: PR.SC "Recommend to suppliers, the use of global standards - that mitigate the risks associated with cyber and supply chain security – during the development and manufacture of the products and services (including updates) that are used by organizations in their critical infrastructures or business enterprises."

PR.SC-1: Suppliers and partners are required by contract to implement appropriate measures based on global standards or other global

guidelines designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan.
ISO/IEC 20243 4.2.1.4, 4.2.1.5
PR.SC-2: Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted
ISO/IEC 20243 4.1 – 4.2.1.12, Assessment for 20243 4.11-4.22

PR.SC-3: Response and recovery planning and testing are conducted with critical suppliers/providers
ISO/IEC 20243 4.1.2.4 – 4.1.2.6