Trustwave®
Government Solutions

NIST CYBERSECURITY RFI

National Institute of Standards and Technology (NIST), Commerce.

Thank you for the opportunity to provide comment to the National Institute of Standards and Technology (NIST), NIST Cybersecurity RFI.

Use of the NIST Cybersecurity Framework

1. The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.

    - The five functions are of significant value to organizations who are relatively immature and new to cybersecurity as it provides a simple lens through which to understand the field and the areas in which they are likely to require investment.
    - The five functions do not clearly correspond to groups of risk, however, and a clearer connection between the ISO27001 risk-based approach would be valuable for organizations who are seeking to use both frameworks (and/or indeed who are effectively mandated to use both frameworks by different groups of stakeholders).
    - We believe the framework should add a clear and comprehensive database security program with proactive database security measures that include continuous vulnerability assessment and remediation, database privileged access visibility and control, and continuous database activity monitoring to alert and respond to anomalous database activity. These efforts should be applicable no matter where the databases reside (on premise, in the cloud, or a hybrid environment). Additional scrutiny should be applied to testing systems that utilize that data. Infrastructure, whether web, network, or end client that display that data should be tested regularly by trusted third parties that specialize in security.

2. Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?

- In practice, many organizations deploy the NIST CSF with a limited consideration of their own risk. Unlike the ISO 27001 concept of a risk assessment clearly flowing through to a Statement of Applicability, indicating the controls that relate directly to risks, the NIST CSF is generally approached as being a more prescriptive set of controls irrespective of risk.
- The most significant advantage of the framework is the five functions, and the simplicity and clarity that it allows in communication to non-cyber-security professionals including Boards of Directors
- Work on metrics is an area that would add significant value to the industry. At present metrics programs often get caught between qualitative assessments of maturity (which are often based on proprietary assessment methodologies) and quantitative measurements that have limited real-world value (e.g., Number of attacks; number of blocked messages etc)

3. Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).

    - The main challenge organizations currently face is the typical marketplace challenge of needing the demand-side and supply-side to agree on an approach. We currently have the 'demand side' requesting various certifications and reports, including ISO27001 certification, SOC2 reports, Security Scorecard/BitSight /UpGuard reports, independent audits, penetration test findings from CREST certified providers, ISO27017, 27018, Shared Security Assessment Questionnaires, and CSA-STAR registry entries. Many organizations are using whatever security framework they see the best commercial returns on; and until greater consistency exists in the market, demand it will be hard for a single framework to get overall traction.

4. Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.

    - We believe that more work on both automated and manual metrics would be a valuable addition/extension.
    - Additional clarity around Tiers and how they relate to more broadly used/accepted models of Capability Maturity Models would also support broader adoption.

5. Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.

    - This should not be a negative impact provided that with the release of the new version, practical materials are released to enable/support the transition to the new framework.

6. Additional ways in which NIST could improve the Cybersecurity Framework or make it more useful.

    - Anything that helps address the issues above in terms of integration/interaction with other standards and frameworks in the market.
    - Strengthen Vulnerability Management Posture - Vulnerability assessment (VA) technology has existed for more than 25 years. Vulnerability management is considered a fundamental security operational process recommended by standards like the National Institute of Standards and Technology (NIST) and is performed by nearly every industry. VA technology is mature and has developed over a long period of time. There are however, important differences in the toolsets and what they are designed to do.
        - While traditional VA solutions focus on assessing systems more broadly, there are also solutions that provide specific expertise to a particular set of IT assets, such as databases and data stores. As Gartner points out in their 2021 Gartner Market Guide for Vulnerability Assessment, "In-depth assessments of databases and applications, such as ERP systems (e.g., SAP or Oracle), are not widely supported in traditional VA solutions." In the past decade, the market has seen a merger of dynamic application security testing (DAST) tools, designed for web applications, into traditional VA solutions. The same cannot be said about database scanning. Traditional, broad-based VA solutions have included database scanning as a mere checkbox for compliance and do not achieve the level of protection we recommend as necessary to protect the data held in the databases the government uses.

Cybersecurity Supply Chain Risk Management

11. National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?

- Establishing some clear definitions and categories of supply chain risk would be a good start. At present we have a conflation of three very different issues:
    - Geopolitical issues around the trustworthiness of technology platforms.
    - The assessment and management of risks related to the security of service providers (e.g., Law firms, SaaS businesses etc); and
    - The software and technology supply chain issues as highlighted by Log4J, Solarwinds, RSA and more.
- Each of these 3 categories have a fundamentally different approach/response required and are of differing levels of relevance to different types of businesses.

12. Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (*e.g.* pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that

may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.

- Extending the typical Defense in Depth approach to this issue is recommended, and particularly with a focus on the Detect/Respond elements. Very few organizations would be positioned to do real validation of something like the SolarWinds firmware prior to deploying it into their environment – realistically the detection of such a compromise is going to arise through monitoring of the behavior of that technology.
- Specify Vulnerability Management areas - While traditional VA solutions focus on assessing systems more broadly, there are also solutions that provide specific expertise to a particular set of IT assets, such as databases and data stores.
- Enhance control of user and application access to sensitive data, at the data layer (not just perimeter). In addition, the implementation of the proper tools to provide protection of and access to sensitive data held in both structured and unstructured data stores.

13. Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider achieving greater assurance throughout the software supply chain, including for open-source software?

- Clarifying the viability (or not) of Security Scoring approaches – e.g., Security Scorecard, BitSight, UpGuard, would be helpful. A significant number of organizations rely on these models without any real understanding of what the numbers mean or their relevance/accuracy to assess a specific threat.

Trustwave and Trustwave Government Solutions provides leading cyber security software, consulting and professional services; including threat hunting, digital forensics and incident response, and managed security services to a range of commercial and federal entities. Trustwave and Trustwave Government Solutions brings over 20 years of expertise working with the public and private sectors on cyber security challenges.

Adam Rak
Sr. Director, Government Relations
Trustwave Government Solutions