Reference Docket: NIST-2022-0001, Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Colleagues,

The CISA CyberStat program is pleased to provide the following comments in reference to the NIST Cybersecurity RFI dated 02/22/2022, as published in the Federal Register on that date.

CISA, through the CyberStat program, assists agencies in protecting their systems, networks, and data. The leaders of the CyberStat program are pleased to enjoy a collaborative relationship with NIST's subject matter experts. The current NIST resources help the CyberStat program to fulfill its existing objectives including:

- increasing effectiveness of information security programs at agencies;
- providing a consistent approach for development and maintenance of information security programs required to protect agencies' critical cybersecurity activities; and
- empowering agencies to achieve policy-based goals.

We look forward to the opportunity to work together on further development and advancement of NIST cybersecurity resources, including the next generation of the Cybersecurity Framework and associated materials.

<u>Specific Considerations in Response to Question 4</u>

- The definitions for the five core functions should be updated to include a specific reference to planning for and engineering resilience into systems prior to the Recover pillar. As NIST has shown with other categories (e.g., Recovery Planning), preparation activities need to occur long before they are needed. Organizations must make plans in advance about how to operate in a degraded or debilitated state, so it would be helpful to direct those outcomes in the Protect function.
- Framework guidance should acknowledge, and stress to the reader, that organizations operate in a contested cyber environment. Current guidance describes benefits of improvement but may not provide the necessary sense of urgency for today's adversarial risk landscape.
- Mission assurance should be addressed in all the pillars. CSF Step 1 begins with understanding of mission, but subsequent steps and guidance do not tie back to those organizational vision, mission, or goals.
- The Detect function should include outcomes that consider the fact that intrusions are not always detected. Outcomes should help prepare for adversary persistence and long-term presence.
- Could the detect pillar be changed to incorporate known exploited vulnerabilities? An organization wouldn't have to detect an incident in their own network before increasing their protections. Knowledge of a new threat vector in the wild would be enough to warrant higher levels of assurance.

- Regarding Framework Implementation Tiers, Tier 4 could discuss how to maximize resilience.
- Our program recommends that the concept of Zero trust architecture should be included within the Framework guidance and Core.
- Finally, the Core subcategories would benefit from factoring in progressive improvement. An example is the federal “Maturity Model for Event Log Management” as described in OMB Memorandum M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf [gcc02.safelinks.protection.outlook.com])

Thank you for the opportunity to contribute to the Request for Information. CISA looks forward to working together with NIST to expand and improve cybersecurity, supply chain risk management, and other resources for federal agencies.

Kim A. Isaac, CISSP
Cybersecurity Division
DHS Cybersecurity and Infrastructure Security Agency