April 25, 2022

The Computing Community Consortium's Response to Request for Information on Evaluating and Improving the NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Written by: Elisa Bertino (Purdue University), Daniel Lopresti (Lehigh University) and Ufuk Topcu (University of Texas at Austin)

This response is from the Computing Research Association (CRA)'s Computing Community Consortium (CCC). CRA is an association of nearly 250 North American computing research departments - academic, industrial and professional societies. The mission of the CCC is to enable the pursuit of innovative, high-impact computing research that aligns with pressing national and global challenges. The CCC brings together a diverse set of individuals representing the broad community to lead initiatives and activities, such as this response.

Updating NIST's "Framework for Improving Critical Infrastructure Cybersecurity" and beginning the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) are both critical enterprises due to rapidly evolving cybersecurity threats and the state of our nation's supply chain ecosystem. Members of the CCC's Security, Integrity and Trust task force came together to call out specific advice such as incentive structures, expanding highlighted functions, non-NIST frameworks and maintaining a flexible framework. Below we offer comments in four specific areas raised in the NIST RFI.

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).

Incentive mechanisms, or the lack thereof, play a significant role in the design and implementation of secure computing technology and cybersystems. Instituting such mechanisms requires answers to a series of questions including, but not limited to, the following: How do we incentivize the production of more secure hardware and software? How do we incentivize individuals to take proper steps to secure their data? How do we disincentivize cybercriminals? How does the insurance market affect the incentives surrounding ransomware and other aspects of cybersecurity? Answers to these questions require contributions from not

only computing researchers but also economists, insurers, legal scholars, and experts in regulation to address the socio-technical dimensions.

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.

Functions listed in the NIST Cybersecurity Framework should be expanded to take into account recent major cyberattacks focusing on data, such as data theft and cryptographic ransomware. Examples include tracking data movements across organizations to detect anomalies in data transfer, content inspection and data-centric risk assessment.

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

We understand that NIST employs a standard Federal RFI process for updates to guidelines like the CyberSecurity Framework. We seem to be approaching a time, however, where multi-year turnaround cycles are not sufficiently nimble in face of the evolving threat landscape. AI/ML-driven threats, in particular, can be targeted, fielded, and evolved much more rapidly than traditional cyber threats that are crafted, programmed, and deployed by human adversaries. While it is good to see that the current framework incorporates notions of “continuous improvement” (DE.DP-5, RS.IM-2, RC.IM-2) and “lessons learned” (RS.IM-1, RC.IM-1), we believe that more explicit attention should be paid to the unique autonomous and rapidly evolving threat models posed by AI/ML adversaries.

8. Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources? Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?

The use of the MITRE ATT&CK framework would be useful due to the fact that the NIST Cybersecurity Framework offers a very detailed perspective from the attacker point of view. In the MITRE framework each step of the attack includes a detailed list of attack vectors. The attack vectors could be used as a basis to determine whether the functions proposed in the NIST document are able to protect against them, and thus help to extend/refine the NIST Cybersecutiry functions.