From: **Nate Shelter**
Date: Mon, Apr 10, 2017 at 4:53 PM
Subject: NIST Framework Update Comment
To: cyberframework@nist.gov

Hi NIST Framework Team,

On behalf of Tanium, please find attached a comment in response to the NIST Framework update. Please don't hesitate to reach out if you would like to discuss with Tanium any of the issues raised. We are happy to help in any way we can.

Thank you,
Nate

--
Nate Shelter
Strategic Communications Manager
Crosscut Strategies, LLC

[Attachment Copied Below]

FR Doc. 2017-01599
National Institute of Standards and Technology
ATTN: Matt Barrett
1401 Constitution Avenue NW
Washington, DC 20230

Dear Mr. Barrett:

We write in support of the Version 1.1 update to the NIST Cybersecurity Framework. The update is much needed, given the pace at which cyber threats and technology have evolved since it was first released in 2014. Tanium works with many large organizations both inside and outside federal government, including the top 15 banks and the U.S. Department of Defense that use the Framework as a critical foundation for their cybersecurity efforts. This update strengthens that foundation and we strongly encourage NIST to pursue more frequent updates to keep in line with emerging trends. We also applaud NIST for consistent engagement with the private sector throughout the update process; government and industry have much to learn from each other.

Version 1.1 includes two notable updates: expanding the supply chain risk management section, and a new section on metrics and measurement. The expanded supply chain section is a significant improvement. As our world becomes increasingly interconnected, each point along the supply chain offers a potential entry point to an organization's network. NIST has appropriately used government's convening powers to establish a common vocabulary and framework for organizations to communicate their desired cybersecurity requirements to buyers, suppliers, and other partners—all of whom are a potential point of entry into their network.

The addition of a measurements section is also a step in the right direction. Measuring cybersecurity is one of the most effective ways an agency can assess its performance and identify areas for improvement. However, while the Framework provides tiers for metrics, and refers users to controls catalogues like SP 800-53, what's still missing are specific metrics for organizations to measure their performance. We fully understand the strength of the Framework comes from it not being one-size-fits-all, and yet, there are still certain core metrics that all organizations should know, or at least work toward knowing.

Current controls catalogues advise organizations to, for example, inventory their networks—but give no way to measure success. Whether it is in the Framework itself or a separate document, we recommend NIST provide a set of core metrics, based on tier, with an average that organizations should aim toward. NIST should work with industry and government agencies to agree on these metrics, but at a minimum, they should include:

1. The ratio of managed to unmanaged assets
2. The mean time to scan the entire network for vulnerabilities
3. The mean time to patch critical vulnerabilities
4. The mean time to remediate an incident
5. The percentage of systems that that meet compliance standards

Once you're able to measure risk across organizations, using standard metrics and a common language, you can benchmark your performance against peers of similar size, and better understand what target you should be aiming toward. With more rigorous metrics, audits and reporting significantly become more valuable, more useful and more effective in evaluating risk. The cybersecurity insurance market would also become more useful. And, defined metrics give government a better way to move the needle without dictating how to do it, as it could offer a data-backed baseline that sectors, including the government itself, should strive toward.

The Framework also acknowledges that "determining cause-and-effect relationships between cybersecurity and business outcomes is dependent on the accuracy and precision of the measurement systems." This is a critical point for organizations to understand, and an area NIST should expand upon. In many cases, systems of record are neither timely, nor accurate—and without these, metrics are meaningless. Organizations should be able to objectively demonstrate—for example, during an audit—they are getting accurate and timely data to base their metrics on. It is this platform upon which a measurable cybersecurity program can be built.

The Framework has already helped organizations establish a foundation to manage risk. Now it must focus on applying this same rigor to measuring risk. We would be happy to discuss further.

Best regards,

David Damato
Chief Security Officer
Tanium