[redacted]
Subject: EXT :FW: Comments on Cybersecurity Framework
Date: Thursday, March 9, 2023 1:28:20 PM

CAUTION: This email originated from **outside** your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders.

FYI

[redacted]
Sent: Wednesday, March 1, 2023 2:54 PM
To: cyberframework <cyberframework@nist.gov>
[redacted]
Subject: Comments on Cybersecurity Framework

Hello NIST Framework Team,

My comments are limited to 4 areas:

1. While there are many NIST personnel associated with ISO/IEC standards, there are several standards in draft format that warrant NIST's attention: 27404, IoT labeling; and PWI-5192, Guidelines for a SOC immediately come to mind.
2. Updating the framework to reflect the improvements in NIST 800-53 REV. 5. I am specifically interested in "Vulnerability Management" to include vulnerability report intake capability, mitigation or remediation of the vulnerability and then alerting the customer base to the need for updates or upgrades. (See ISO/IEC 29147:2018 and ISO/IEC 30111:2019.)
3. Encourage transparency, where possible, to allow the consumer/customer to conduct their own assessment of the status of compliance with CSF. The fully compliant manufacturer or vendor would likely advertise their status.
4. Software Bill of Materials (SBoM) is not as helpful as it sounds. SBoM only reflects the status of a simple product at a point in time. Consider including an entry for a PBoM (Production (or product) Bill of Materials. A PBoM should include the entire production cycle, identify the dependencies, and represent the entire production cycle. This type of information would support the vendor in determining which products contain vulnerable code and the vendor alerting the consumer that their software needs updating. (Log4j)

Thank you for encouraging comments.

Best regards,

Laurie Tyzenhaus

Laurie Tyzenhaus

Senior Member of the Technical Staff
CERT/CC – The Software Engineering Institute