From: Rebecca Allen Diamond
To: cyberframework
Subject: Feedback on the NIST CSF 2.0 Implementation Examples
Date: Thursday, November 2, 2023 4:50:14 PM
Attachments: Outlook-di31lgmo.png

NIST CSF team,

Thank you for the opportunity to submit comments for the NIST CSF 2.0 Implementation Examples document. As users and supporters of the NIST Cybersecurity Framework we appreciate the work done to keep the framework and support material updated and reflective of the evolving cybersecurity landscape.
Overall, we felt the examples are well written with enough specificity to be helpful to a diverse range of organizations. Listed below are our comments on the examples provided in the draft document.

ID.AM-02
The examples provided do not mention microservices. Consider adding examples specifically relating to microservices and containers.
Proposed Additional Examples:
Ex4: Images utilized to instantiate containers should be inventoried, monitored, and routinely patched.
Ex5: Microservice components should be inventoried, monitored, and consistently updated to ensure optimal performance and security.

DE.CM-02:
Ex2: "Review and monitor physical access records (e.g., from visitor registration, sign-in sheets)" does not state what or why records should be reviewed. Consider adding, "to find unusual or suspicious access requests" to the example.
Proposed Update:
Review and monitor physical access records (e.g., from visitor registration, sign-in sheets) to find unusual or suspicious access requests

GV.OC-02:
The examples given use passive voice in the e.g. lists; consider rewording for easier understanding.
Proposed Update:
Ex1: Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., officers, directors, and advisors' performance and risk expectations; employee cultural expectations)
Ex2: Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., customers' privacy expectations, partners' business expectations, regulators' compliance expectations, society's ethics expectations)

GV.SC-05:
Ex4 is a restatement of Ex1, which establishes security requirements based on criticality, and Ex2, which requires inclusion of security requirements in contracts. Ex1 and 2 are more detailed in guidance, consider removing Ex4.

Ex1: Establish security requirements for suppliers, products, and services commensurate with their criticality level and potential impact if compromised
Ex2: Include all cybersecurity and supply chain requirements that third parties must follow and how compliance with the requirements may be verified in default contractual language
Propose Remove: Ex4: Manage risk by including security requirements in contracts based on their criticality and potential impact if compromised

Best Regards,
Becca

Rebecca J Allen Diamond | Content Development Director
Zyston LLC
[redacted]
www.zyston.com