From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] NSA CSD Critical Comments - SP800-171-172
Date: Friday, September 16, 2022 8:53:59 AM
Attachments: CSD-NIST800-171-172-response.docx

Hello,

Please see the attachment for CSD's critical comments for SP800-171-172. The submitter is Matthew Seligman, NSA Cybersecurity Collaboration Center.

Please confirm receipt and let me know if there are any questions or concerns.

Thanks!
Erica

Erica Richards
Executive Assistant to Mr. Matt Seligman
Deputy Chief, Cybersecurity Collaboration Center
[redacted]

NSA Cybersecurity Directorate Input to Call for Input on NIST 800-171 and 172

Comment: Include SR1 – SR4 from 800-53 as the minimum SCRM requirement; Include SBOM requirement in 800-171

Justification: Under EO 14028, there is a focus on security and integrity of critical software. The EO calls out software bill of materials as one of the requirements to enhance the security of the software supply chain. We need a whole of government approach to include supporting nonfederal systems and organizations. Also, we need greater assurance that baseline products used in nonfederal systems and organizations do not include malicious components that will impact the confidentiality of CUI (e.g. data exfiltration triggered by hidden malicious components that becomes active).

Comment: Add a technical control similar to DNS filtering (also known as protective DNS) to control family 3.13 (System and Communications Protections) or 3.14 (System and Information Integrity) for 800-171

Justification: This is a simple, sound technical control for SMBs to implement that provides insight into malicious traffic that would otherwise go undetected through other technical and operational controls.

Comment: In 800-172 3.14.6e, we recommend that organizations are required to leverage threat intelligence from government organizations or ISACs within their SRMA,

Justification: This further defines where the threat intelligence should come from further ensuring the threat intelligence used by their teams is both pertinent to their industry and likely of greater value overall.