From:	[redacted] via 800-171comments
To:	800-171comments@list.nist.gov
Cc:	[redacted]
Subject:	[800-171 Comments] Microsoft response - NIST 800-171 Pre-Draft Call for Comments
Date:	Monday, September 19, 2022 10:24:14 AM
Attachments:	DRAFT NIST 800-171 r3 Comments - Microsoft Corporation.pdf

Dear NIST colleagues,

Thank you for the opportunity to provide comments for the NIST 800-171 Pre-Draft publication. Please see the attached response and let me know if you have any questions. We look forward to future updates and drafts. I apologize for sending today vs. Friday, I thought it went out of my email box but apparently was left in my drafts folder. Thanks for understanding.

https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/draft#:~:text=The%20comment%20period%20is%20open%20through%20September%2016%2C,Protecting%20CUI%20project%20site%20after%20the%20due%20date

Thanks
Janet Jones

NIST SP 800-171 Rev. 3: Pre-Draft
Comments of Microsoft Corporation

September 16th, 2022

Microsoft appreciates the opportunity to respond to the initial draft of the NIST SP 800-171 Framework. We applaud the framework's goals and direction. The prior revisions provide a strong foundation from which to build trustworthy systems and incorporates many essential elements of a strong risk management framework appropriate for the unique risks that CUI in Nonfederal systems can pose and which Federal contractors need more broadly. The framework can be strengthened by clarifying the complex nature of handling CUI and what that means for organizations across different sizes and providing more detailed guidance about how organizations can apply and implement NIST 800-171 protections while accommodating the variety of architectures and technology. Microsoft provides recommendations on these topics and other priority issues below. We look forward to continuing to support NIST in this work which will be of significant value to the supply chain that the United States Government [USG], as well as an important contribution to across the country and globe.

Clarifying the complex nature of handling CUI and how to apply the framework

For the 800-171 framework to be successful, it must provide Federal Agencies and their contractors with appropriate guidance that enables the proper categorization and selection of assets [systems, people, and processes] that handle CUI. There are significant risks associated with the inadequate protection of non-CUI data and assets which are derived or interconnected with CUI systems. We believe there is an opportunity to provide greater clarity about the nature of these risks and how to address this. Specifically, we recommend the following:

- Clarity around the categorization and selection of appropriate controls across 2nd and 3rd order assets based on the degree of logical *and* physical isolation in place from assets that contain CUI.
- Clarity around the requirements for nonfederal organizations to obtain assurances on external service providers assets that have direct connection to CUI assets or assets which provide security capabilities. We recommend NIST includes formal definitions for Cloud Service Provider, Managed Service Providers (MSP), Managed Security Service Providers (MSSP) that can provide a standardized taxonomy across the USG.
- Provide greater flexibility to federal agencies and nonfederal organizations in the selection of controls that are applicable to their architecture and deployment model. To achieve this, we recommend NIST adapts the framework to align with organizationally defined values and control overlays. *Additional comments related to this topic can be found in the following section.*

Accommodating the variety of architectures and technologies

Almost all nonfederal organizations rely to some degree upon Cloud Service Providers (CSPs), Managed Service Providers (MSPs), and/or Managed Security Service Providers (MSSPs. We recommend NIST revises the framework to improve alignment between the frameworks and NIST 800-53 to provide greater consistency, familiarity, and interoperability between nonfederal organizations that exist in the ecosystem. While we recognize that the framework includes several controls which are specific to the protection of CUI, we recommend that NIST strives to use SP 800-53 controls. This model will drive alignment between FISMA, FedRAMP, NISPOM, and other NIST publications (e.g., 800-161). Specifically, we recommend the following:

- *Organization-defined values* – enabling organization-defined values will provide federal agencies the ability to assign parameters as it deems appropriate, or in instances where they do not, nonfederal organizations the ability to clearly identify when then are required to define it themselves.
- *Control Overlays* – The inclusion of control overlays will enable NIST, Federal Agencies, nonfederal organizations, and external service providers the ability to create overlays and associated supplemental guidance which are appropriate for their needs. We see significant opportunities for overlays to address challenges that arise from creating a framework that can be universally implemented and assessed agnostic

of any technology or environment. There are several specific overlays we see the need for: Cloud-native/only, On-premises, Manufacturing and Operational Technology
- NFO Controls – We recommend that NIST specifies all controls which it feels are necessary in protecting CUI in nonfederal systems into the body of the framework and not tailored out.

Comment on specific controls

In addition to the thematic comments above, Microsoft wishes to address several specific controls:

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

- We recommend that this control is removed or brought into alignment with other NIST and government-wide guidance[1].
- Additionally, Microsoft recommends that NIST allow for Passwordless approaches that involve strong phishing-resistant MFA, as a suitable alternative to a password.

3.7.5. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete

- Microsoft recommends, in accordance with OMB's guidance and industry best practices, that MFA be required everywhere by default, and permitted by temporary or isolated exception.
- Additionally, Microsoft recommends that SMS-based MFA is not considered an approved MFA with respect to meeting MFA requirements.

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organization systems and communicating via some other connection to resources in external networks (i.e., split tunneling)

- We recommend NIST removes or clarifies the control language and guidance based on feedback from customers and industry peers. There is significant confusion and misunderstanding in this controls application to cloud-based devices and systems.

3.13.11 Employ FIPs-validated cryptography when used to protect the confidentiality of CUI

- We recommend NIST provide substantial guidance or references to enable organizations to better understand the FIPs-validation program and how to approach implementation of this control from a customer / third-party perspective.

[1] Office of Management and Budget (OMB), page 5 M-22-09 Federal Zero Trust Strategy (whitehouse.gov)