From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] NDIA Comment: SP 800-171
Date: Friday, September 16, 2022 5:10:55 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
NDIA Comment on NIST SP 800-171 (FINAL VERSION).docx

Good Afternoon Mr. Ross,
Please disregard the earlier comments that were submitted.

Please see attached to this email the comments that NDIA would like to provide.

V/R,
Jeff Goldberg

NDIA
At the Heart of the Mission Since 1919

Jeff Goldberg
Director, Regulatory Policy
Arlington, Virginia
[redacted] | NDIA.org

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • [redacted] • [redacted] • NDIA.org

September 12, 2022

Mr. Ron Ross
Computer Security Resource Center
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: NIST SP 800-171 Rev. 3 (Draft)

Mr. Ross:

The National Defense Industrial Association (NDIA) represents more than 1,800 corporate members and over 66,000 individual members from small, medium, and large defense contractors. Our members and their employees feel the impact of any policy change made to how the United States equips and supports its warfighters. As requested, we are providing our comments on the referenced NIST (National Institute of Standards and Technology) SP 800-171 Revision.

Protecting controlled unclassified information (CUI) is a much bigger topic than just NIST SP 800-171. NDIA believes that the Government and industry should work together to ensure that such information when processed by the Defense Industrial Base (DIB) is secure. To that end, we suggest that NIST hold a public meeting to discuss any potential changes to NIST controls with the DIB, NDIA, and other associations in the Council of Defense and Space Industry Associations (CODSIA) and potential paths for resolution. This discussion also should include how best to tailor NIST controls internationally where such controls may conflict with foreign law. This is a significant implementation challenge for many contractors in the DIB that has not been addressed by the Department of Defense (DoD) or NIST.

We believe it is essential that the cybersecurity standards be clarified to permit contractors at all tiers to understand what is required of them for purposes of meeting their baseline contractual obligations. By the same token, NIST should not be unduly prescriptive in developing new controls to allow companies the flexibility needed depending on the size of their businesses. Finally, in going through the NIST checklists and guidance, NDIA is particularly concerned the guidance skews toward more sophisticated systems and larger businesses with greater resources. The significant impacts of increasing regulation are magnified for small business, and the

government must ensure regulations do not inadvertently become a barrier to small business participation in the defense industrial base.

However, a flat, check-the-box standard does not meaningfully address the emerging types of threats that the DIB must protect against. There is a need for flexibility and risk assessment in determining what is needed for adequate security for different contractors, in different sectors, falling under different tiers in the DIB, to address their different risks. A standard that lacks flexibility to adapt security requirements, which may be adequate for unique information systems, is also likely to be ineffective and too rigid for the DIB.

I. Manufacturer Concerns

One area in particular that does not seem to be adequately addressed in the NIST SP 800-171 relates to manufacturing companies' need to protect CUI in both their information technology (IT) systems and their manufacturing systems, hereinafter referred to as Operational Technology (OT):

a. NIST SP 800-171 and supporting documents may not currently address this need.

b. As the trend in Industry 4.0 is toward IT/OT convergence, "air gapping" the manufacturing system OT is both technically and competitively unwise. The lack of clarity regarding which controls need an alternative treatment in OT causes difficulty in compliance, especially for small manufacturers.

c. Many of the IT security requirements referenced in NIST SP 800-171 are difficult, if not impossible, to implement in OT systems. For example, requiring dual authentication during the operation of the OT systems may pose safety risks in manufacturing – requiring input of passwords and authentication before accessing a manufacturing system may impose delays in stopping or starting a system during the manufacturing process.

d. Further, dismantling or reengineering OT systems to meet the NIST SP 800-171 requirements at a time that CMMC 2.0 is being developed and rolled out may result in actions that may satisfy one, but not the other standard. CMMC 2.0 is an obligation on all DoD contractors to implement cybersecurity functions that are intended to be accomplished in the long term. But in order to make NIST SP 800-171 more relevant, the revision should address the potential path of transition to

CMMC 2.0 as it provides a level of protection for threats that are not represented in NIST SP 800-171, such as advanced persistent threats (APTs), ransomware attacks and the like.

e. NDIA recommends that NIST SP 800-171 be revised to clarify which security

controls are not well suited to OT, and to provide references to other NIST publications (e.g., NIST SP 800-182) that may be used to provide compensating controls for addressing CUI protection in OT.

f. There also needs to be clarification of when and how to document "enduring exceptions." Organizations can have legacy systems that cannot be replaced or remediated right away. In such situations, an enduring exception is needed until the organization can replace the legacy system, which may be many years depending on the manufacturing system involved. If the system cannot be replaced, then there needs to be clarity on how the exception might be used more narrowly and the considerations for crafting *ad hoc* requirements for unique systems. Where change to an OT legacy system can take millions of dollars and years, further clarification of the path forward is needed. In this regard, NDIA submits that DoD's assessment methodology has more detail than NIST on the enduring exception. It would be appropriate to address this in the new version. It also should be remembered that DoD and its contractors will continue to need to work with small manufacturers to develop and deliver production systems.

g. With regard to "enduring exceptions," better guidance should be available to identify the process under which enduring exceptions can be available for non-IT systems. Industry could be better served using a risk-based management process.

h. The revised requirements, if they properly consider legacy OT, will also protect OT against loss of confidentiality which may result when an OT is not compatible with current rigid requirements.

II. Cloud Architectures and Zero Trust Architecture

The revised NIST SP 800-171 requirements also need to be more cognizant of cloud architectures and cloud-delivered security, which are promising solutions, particularly for small businesses. Therefore, the revised requirements should further instruct how the requirements can be met in conjunction with cloud solutions, particularly within the context of federal and industry trends to adopt a cloud-first, zero trust strategy.

NIST SP 800-171 v. 2 at 3.13.7 calls for "[p]revent[ing] remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling)." We suggest that NIST further clarify the reference to split tunneling particularly to distinguish from acceptable cloud

implementations. The description in the publication could be seen to prohibit use of cloud implementations especially from remote locations if an employee doesn't have to go through VPN to enterprise network to get to cloud but can connect directly due to other secure technologies.

NIST SP 800-171 v. 2 at 3.1.14 calls for "[r]out[ing] remote access via managed access control points." We suggest that NIST further clarify the definition of "remote access" in the context of cloud-native architectures which may be accessed from distributed, non-local user endpoints.

Similarly, NIST SP 800-171 v. 2 at 3.1.15 calls for "[a]uthoriz[ing] remote execution of privileged commands and remote access to security-relevant information." Again, we suggest that NIST further clarify what constitutes "remote" in the context of cloud-native architectures. We note that the assessment objectives for 3.1.15 as described in NIST SP 800-171A (June 2018) call for the identification of "privileged commands authorized for remote execution" and "security-relevant information authorized to be accessed remotely", as well as the authorization of "the execution of the identified privileged commands via remote access" and "access to the identified security-relevant information via remote access." In a cloud-first architecture, much or all of an organization's security-relevant information may be hosted in the cloud; if the definition of "remote" does not appropriately consider cloud architectures, it could be seen to apply to all interactions between an end user or administrator and cloud resources.

III. Security Protections and External Service Providers

NDIA notes that there is industry confusion around what constitutes "security protections" in the scope and applicability of NIST SP 800-171 v.2 (Section 1.1), specifically as it pertains to requirements for external service providers such as managed service providers (MSPs) and managed security service providers (MSSPs).

We recommend that NIST provide a commercially relevant definition of "managed service provider" that differentiates MSPs and MSSPs from cloud service providers (CSPs), each of whom play functionally distinct roles as external service providers. In the absence of a clear definition of "managed service provider", other organizations may seek to unilaterally enforce conflicting interpretations, as evidenced by the pre-decisional draft CMMC Assessment Process v. 1.0 published by the Cyber AB, which conflates MSPs and CSPs and prescribes either FedRAMP Moderate equivalency or CMMC Level 2 certification, using interpretations of NIST SP 500-292 and other disparate sources to justify their position.

Additionally, we strongly recommend that NIST create an overlay to NIST SP 800-171 for external service providers such as MSPs and MSSPs who do not process, store, or transmit CUI themselves, but who provide IT and security services to organizations that process, store, or transmit CUI. Such an overlay should focus on controlling and protecting access to environments that contain CUI.

IV. Compliance & Assessments

In terms of assessing compliance with the security requirements in the standard, there needs to be consistency, but also an ability to accept risk-based, flexible solutions.

a. NDIA submits that the DIBCAC's approach to the review of a contractor's systems for compliance is not the same as the approach being used by Cyber AB C3PAOs. Specifically, DIBCAC assessors are in a position to address exceptions or workarounds for certification. C3PAOs are not. Thus, contractors' risk inconsistent treatment, and in fact disadvantageous treatment, if they are certified by C3PAOs and not DIBCAC reviewers.

b. NDIA submits that to avoid such inconsistent treatment, NIST should "bake in" the assessment methodology in the revised version of NIST SP 800-171.

c. However, the state of threats to different companies, as well as their contractual commitments and needs, can differ and change quickly. Different contractors will have different needs and constraints in implementing cybersecurity controls. The assessment methodology should be able to take into account and afford the contractors latitude to approach problems and look at other authorities to address these risks. An assessment that allows contractors to assess their needs and take a flexible, comprehensive and articulated risk-based approach, based on their industry, should be acceptable. Contractors might be asked to explain their approach, why they couldn't comply with one control, and what they considered in planning the approach they are taking.

V. Safe Harbor and Advance Notice of Proposed Rules

NIST may take more than one year to review and incorporate comments into a revised version of NIST SP 800-171. Some form of safe harbor should be afforded contractors that proceed to certify their compliance for current contracts. Further, revision of the NIST SP 800-171 should be undertaken in conjunction with revision of the rules to incorporate the new version into the

procurement process. Advanced publication of the revised rules before they are formally adopted, so that regulators have ample time to alert stakeholders and address their comments and concerns, is encouraged. Additionally, tabletops with industry to determine where the issues reside and what workarounds might be appropriate also might assist in the development of a risk-based, flexible standard and set of rules that will better enable the DIB's diverse membership to achieve compliance and an appropriate level of security.

VI. Scoping Guidance

The current version of NIST SP 800-171 lacks clear scoping guidance. CMMC 2.0 has attempted to fill this void, yet the guidance still lacks clarity. Providing scoping guidance in NIST SP 800-171 would allow for better industry inclusion in the definition of the guidance.

a. The CMMC scoping guidance definition of OT provides coverage for different types of systems, but note "OT includes hardware and software that use direct monitoring and control of industrial equipment to detect or cause a change" is too specific in many instances. It is not atypical for an external system to have a need to interface with an OT asset. These systems can be used to gather data which would be considered CUI from the OT asset, and by the provided definition would be classified as CUI assets. However, due to the limited capabilities of the OT system, implementation of all required NIST SP 800-171 controls would cause the asset connected to the OT system to not be able to provide the correct capabilities and to fail to meet the required functions it was designed to meet.

b. Inclusion of scoping guidance in NIST SP 800-171 would allow for the creation of a control applicability matrix to differing asset types. Scoping guidance should include information on which controls could align with each asset type. CUI assets and Security Protection Assets will not always be able to implement the same controls, nor should they. A Security Protection Asset that doesn't process CUI should have a very different control set applied.

VII. Additional suggested updates to improve usability or provide further clarity

The following comments are offered to improve the usability of the standard or to further clarify specific language:

a. NIST SP 800-171 v.2 states that certain controls or control enhancements, indicated as Nonfederal Organization (NFO) controls, are "expected to be routinely satisfied by nonfederal organizations without specification." NDIA

suggests that NFO tailoring assumptions may be out of step with industry realities, particularly for small businesses. We assert that if NIST intends for industry to implement controls or control enhancements, they should be included explicitly as requirements in NIST SP 800-171; however, we do not believe that the NFO controls related to documented policies and procedures should be included as explicit requirements. As noted in the NIST Cybersecurity Framework, among other sources, organizations will have varying degrees of maturity with regard to internal documentation, and that ad hoc process may be acceptable or expected at certain maturity levels. We believe that rigorous documentation requirements, particularly for small businesses, can lead to "pencil whipping" exercises with little benefit to security outcomes.

b. NIST SP 800-171 v.2, Appendix B, defines "FIPS-validated cryptography" to include "A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended). …" We recommend adjusting the NIST FIPS 140-2 requirement to adapt more flexibility to "utilize and document strong encryption techniques when cryptography is used and/or requested."

c. We suggest changing or modifying the reference to "CMMC AB" to "Cyber AB (previously called the "CMMC AB") as that is their new name.

d. Suggest clarification of the non-federal organization (NFO) security controls in Appendix E, which are additional requirements.

e. Additional clarity needed for Cloud providers as FedRAMP Moderate Equivalent is hard to assess. It is important for NIST to align with other regulating agencies to ensure NIST SP 800-171 (current version v.2 and future v.3) will align with other regulatory releases.

f. DoD and a few other agencies may be further down the implementation road for CUI, but it appears that there's still a lack of consistency in treatment of CUI and a big gap in implementation at other agencies. Addressing CUI in a consistent and coherent scheme needs to be undertaken. Industry cannot protect the data that has not been properly identified. In most cases that needs to start with the government's identification and implementation of a CUI program.

g. Suggest adding at least two sets of visualizations to help understand the overall workflow process. The visualizations should include 1) a workflow of the overall process, 2) swim lane maps of each of the different aspects of the workflow to allow for additional breakouts (i.e., pre-assessment, assessment, post assessment) to include, but not be limited to: start, stop, decision triangles, activities, comments, and 3) key decision makers and ownership should be included in the visuals. The visual elements should also include simplified decision trees to help provide users with an understanding of each section and process. There also should be a summary document explaining map structure and providing a legend for identifying swim lane/workflow icons.

h. Suggest removing elements and discussions that are duplicative of the other CMMC documentation and to just refer to the authoritative source for additional information and discussion. A quick sentence is appropriate but there are instances where too detailed of a discussion occurs in the CAP. This will help minimize any discrepancies between documents.

i. Suggest consistency in definitions and removal of detailed descriptions. Instead of detailed descriptions, suggest that the DoD and NIST establish and refer to the authoritative source to minimize inconsistencies between various standards and documents. For example, one section discusses and defines cloud using DFARS 252.239-7010 and another section refers to NIST.

j. CUI identification triggers compliance requirements. The National Archives and Records Administration Information Security Oversight Officer 2021 Annual Report to the President recognized that despite presidential requirements for agencies to fully implement their CUI programs, this still has not been accomplished:

> All executive branch agencies must fully implement the CUI program. If this program is not fully implemented, we believe the executive branch and its private industry partners will revert to a pre-9/11 agency-centric ad hoc "Wild West" that the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) warned was a risk to national security.[1] The program's demise would also adversely impact other existing programs such as

[1] Information Security Oversight Office (ISOO) 2021 Annual Report to the President (archives.gov). https://www.archives.gov/files/isoo/reports/isoo-2021-annual-report-to-the-president-final.pdf

the National Operations Security Program under National Security Presidential Memorandum (NSPM)-28, efforts to standardize the requirements and protections for this information in government contracts and information sharing agreements that will save the government and private industry money, and undermine DoD initiatives to protect information concerning a variety of advanced technologies. Implementation efforts still require strong White House support, guidance, and direction to make sure the program is fully implemented and adequately funded.

In conclusion, we appreciate your consideration of our comments. We are available to provide additional explanation or information as requested. If you have any questions, please contact Nick Jones, Director of Strategy, at [redacted] or Jeff Goldberg, Director of Regulatory Policy at [redacted].

Sincerely,

National Defense Industrial Association