From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] CTIA Comments re: NIST SP 800-171
Date: Monday, July 17, 2023 6:45:06 AM
Attachments: 20230714 CTIA comments NIST SP 800-171 Rev 3.pdf

---

Happy Friday, July 14, 2023

Please see attached CTIA's comments in response to NIST SP 800-171. Could you please confirm receipt?

Thank you,

Justin

ctia™
Justin Perkins
Manager, Cybersecurity & Policy
[redacted]

Before the Department of Commerce
National Institute of Standards and Technology
Washington, D.C.

In the Matter of

NIST SP 800-171 Rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*	)))	Initial Public Draft

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Justin C. Perkins
Manager, Cybersecurity and Policy

CTIA
[redacted]
www.ctia.org

July 14, 2023

Table of Contents

I. INTRODUCTION AND SUMMARY

CTIA[1] is pleased to submit comments on the National Institute of Standards and Technology's ("NIST") draft Revision to *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, SP 800-171* ("800-171") *Rev. 3* ("Draft" or "Revision 3").[2]

CTIA is proud to partner with NIST on a range of cybersecurity issues and efforts. Given that CTIA's members include many of the world's largest telecommunications providers that provide voice, data, and cloud-based services to the federal government under contracts and subcontracts, including with the Department of Defense ("DoD"), CTIA has engaged with NIST on multiple workstreams focused on promoting cybersecurity for nonfederal systems handling controlled unclassified information ("CUI"), including providing feedback on the 800-171 Series,[3] including NIST's most recent Pre-Draft Call for Comments.[4] More generally, CTIA has collaborated with NIST on numerous cybersecurity issues and proceedings.[5] In addition, CTIA

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *See* NIST SP 800-171 Rev. 3 (Initial Public Draft), Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST (May 10, 2023), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.ipd.pdf ("Draft SP 800-171 Rev. 3").

[3] Comments of CTIA on Draft NIST SP 800-171B, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets (filed Aug. 2, 2019).

[4] Comments of CTIA on Pre-Draft Call for Comments: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (filed Sept. 16, 2022), https://csrc.nist.gov/csrc/media/Projects/protecting-controlled-unclassified-information/Pre-Call-For-Comment-Sept-2022/CUIPreCall_CTIA_Sep16_2022.pdf.

[5] This includes commenting on *Security and Privacy Controls for Information Systems and Organizations, SP* 800-53 ("800-53") *Rev. 5*, Comments of CTIA on Final Public Draft SP 800-53, Security and Privacy Controls for Information Systems and Organizations (filed May 29, 2020), the *Framework for Improving Critical Infrastructure Cybersecurity*, *e.g.*, Comments of CTIA on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management, Dkt. No. 220210-0045 (filed April

and its members are engaged in public-private partnerships to improve the cybersecurity of government and the private sector, working with the Department of Homeland Security's ICT Supply Chain Risk Management ("SCRM") Task Force,[6] the Communications Sector Coordinating Council ("CSCC"),[7] and the Federal Communications Commission ("FCC")'s Communications Security, Reliability and Interoperability Council ("CSRIC")[8] to bring industry expertise and experience to protect networks and ensure reliable service.

800-171—whose current Revision 2[9] was finalized in January 2021—is a foundational document that plays a key role in establishing cybersecurity expectations for government contractors with respect to handling CUI. In practice, it serves to establish cybersecurity expectations for government contractors handling CUI, so changes to 800-171 will have downstream effects on government contractor obligations. In particular, some agencies incorporate 800-171 by reference into their agreements with contractors and other entities with whom they share CUI.[10] Accordingly, changes to 800-171 will directly impact government contractors by way of their contracts that deal with CUI. Revisions to 800-171 will also impact contractors through the forthcoming Cybersecurity Maturity Model Certification ("CMMC")

25, 2022), and other important cybersecurity guidance documents.

[6] *ICT Supply Chain Risk Management Task Force*, CISA, https://www.cisa.gov/resources-tools/groups/ict-supply-chain-risk-management-task-force (last visited July 6, 2023).

[7] *Communications Sector Coordinating Council*, CSCC, https://www.comms-scc.org/ (last visited July 6, 2023).

[8] *Communications Security, Reliability, and Interoperability Council*, FCC, https://www fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited July 6, 2023).

[9] *See* NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST (Feb. 2020), https://doi.org/10.6028/NIST.SP.800-171r2 (includes updates as of Jan. 28, 2021) ("SP 800-171 Rev. 2").

[10] For example, the standard DoD clause at DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires all contractors and their subcontractors to implement the security controls in 800-171 on any nonfederal information system that will store, process, or transmit CUI, among other things, as a condition of receiving the contract. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, https://www.acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses#DFARS_252.204-7012 ("DFARS 252.204-7012").

program, through which DoD plans to assess contractors' compliance with the standards in 800-171.[11] DoD has announced that it intends to base the requirements for the most prevalent level (Level 2) of its forthcoming CMMC program on 800-171.[12] DoD currently provides additional guidance on each of the Revision 2 security controls in its CMMC Level 2 Assessment Guide.[13] Given the significant changes in the Draft, the current guidance in DoD's Assessment Guide will likely need to be updated.

Accordingly, as NIST moves forward with the Draft to update this central document, it should acknowledge the significant impact its updates and changes will have on government contractors, and it should prioritize clarity, flexibility, and harmonization—to minimize confusion and ease implementation hurdles. With these comments, CTIA encourages NIST to:

- Work with its federal partners to clarify the scope of 800-171 by updating definitions and providing more resources to help organizations identify CUI;
- Provide guidance for flowing down requirements to subcontractors;
- Expand on explanatory guidance to help contractors understand what is new and unique in the Draft Revision;
- Maintain and bolster the voluntary, flexible, and risk-based nature of the Draft, recognizing that inflexible and overly prescriptive requirements impose costs out of proportion to their benefits, limit innovation, and can quickly become obsolete;
- Ensure that Organization-Defined Parameters ("ODPs") are tools to promote flexibility and that they do not define overly prescriptive or discordant requirements from one agency to the next;
- Maintain and bolster harmonization with other federal procurement guidance, particularly with 800-53 Rev. 5, while still recognizing the important role 800-171 plays for federal contractors; and
- Coordinate with other agencies to ensure that 800-171 is implemented with the guiding principles of risk-management and harmonization.

[11] *See About CMMC*, DoD, https://dodcio.defense.gov/CMMC/About/ (last visited July 6, 2023); *CMMC Model*, DoD, https://dodcio.defense.gov/CMMC/Model/ (last visited July 6, 2023).

[12] *See* CMMC Assessment Scope: Level 2 (Version 2.0), DoD (Dec. 2021), https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level2_V2.0_FINAL_20211202_508.pdf

[13] *Id*.

CTIA looks forward to continued engagement with NIST to ensure that Revision 3 will remain a helpful resource for organizations to use to support their government contracts.

II. GIVEN THAT SP 800-171 PLAYS A CENTRAL ROLE IN ESTABLISHING CYBERSECURITY EXPECTATIONS FOR CUI, NIST SHOULD ENHANCE THE CLARITY OF THE DOCUMENT.

A. NIST Should Provide Clear Guidance for Organizations To Identify CUI and Address Ambiguities Regarding the Applicability of 800-171.

800-171 provides recommended requirements for protecting the confidentiality of CUI,[14] which is "information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended."[15] The security requirements in 800-171 "are only applicable to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components,"[16] and are "intended for use by federal agencies in contractual vehicles or other agreements between those agencies and nonfederal organizations."[17] As described above, for government contractors, the obligation to protect CUI is created by federal contract.[18]

A significant and persistent issue for contractors is determining whether information is CUI. There are many families of CUI defined by multiple laws and regulations,[19] so interpreting

---

[14] *What Is the NIST SP 800-171 and Who Needs to Follow It?*, NIST (Oct. 8, 2019), https://www.nist.gov/blogs/manufacturing-innovation-blog/what-nist-sp-800-171-and-who-needs-follow-it-0.

[15] Exec. Order No. 13556, 75 Fed. Reg. 68675, 68675 (Nov. 9, 2010), https://www.govinfo.gov/content/pkg/FR-2010-11-09/pdf/2010-28360.pdf.

[16] *See* Draft SP 800-171 Rev. 3 at 2 (emphasis removed).

[17] *Id.* at i.

[18] *See, e.g.*, *supra* note 10 and accompanying text.

[19] *See*, *About Controlled Unclassified Information (CUI)*, National Archives and Records Administration, https://www.archives.gov/cui/about (last visited July 6, 2023); *see also CUI Categories*, National Archives and Records Administration, https://www.archives.gov/cui/registry/category-list (last visited July 6, 2023).

these rules is challenging, as they overlap and are sometimes ambiguous. Determining which systems store, process, or transmit CUI presents an additional challenge. For example, one type of CUI is Controlled Defense Information, defined in part as information "[c]ollected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract."[20] This potentially ambiguous definition presents particular challenges for telecommunications carriers.[21]

While CTIA recognizes that the National Archives and Records Administration ("NARA") is the executive agent of the CUI regime,[22] NIST can still help provide clarity on these important threshold issues. NIST should encourage NARA, DoD, and other agencies to clarify and provide additional guidance for contractors. To the extent possible, NARA should seek to limit what is defined as CUI. Doing so would enable prioritization of protections for truly sensitive information and reduce unnecessary compliance costs for federal contractors that in turn raise prices for goods and services that the government needs.

With respect to Revision 3, NIST should also help users understand the differences between 800-171 and other related publications. Within NIST's CUI series alone, there are substantial differences in applicable controls as between CUI (outlined in 800-171) and CUI associated with a "critical program or high value asset" (outlined in 800-172).[23] Providing clear

[20] *See* DFARS 252.204-7012(a)(2).

[21] As CTIA has explained in past advocacy, there is ambiguity that NIST should work with DoD to clarify about the compliance obligations of telecommunications providers in circumstances where data is transiting a commercial telecommunications network pursuant to a communications services contract. *See* Comments of CTIA on Draft NIST SP 800-171B, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets, at 15-16 (filed Aug. 2, 2019).

[22] *See* 32 C.F.R. § 2002.4(m).

[23] *See* NIST SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171, NIST, at ii (Feb. 2021), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf.

guidance as to when each document may apply would help to reduce confusion.

B. NIST Should Coordinate with DoD to Clarify Any Possible Flow-Down Obligations Related to 800-171.

NIST should directly address any possible flow-down expectations between prime- and sub-contractors in the next iteration of Revision 3, as doing so will address known ambiguities and promote a more consistent approach. Given the diversity of government contracting and subcontracting relationships and the different levels of access that prime contractors and/or subcontractors may have to government systems and data, including CUI, there is some uncertainty about whether and how prime contractors are expected to ensure subcontractor compliance with 800-171. While the Draft generally discusses requirements for acquisition strategies, tools, and methods, as well as supply chain controls and processes, it does not directly address the issue of whether and how prime contractors should flow-down to subcontractors any contractual requirements to implement 800-171.

To address this issue, NIST should consider coordinating with agencies such as DoD to develop supplemental resources—including tools, trainings, and best practices—to guide compliance with 800-171, including how prime contractors may best manage subcontractor compliance and how to assess which controls may be appropriate to flow-down. NIST is well positioned to work collaboratively with industry and other key stakeholders to ensure these resources are well-informed, consensus-driven, and flexible and risk-based. NIST can leverage the guidance provided in the "C-SCRM in Acquisition" section of 800-161 Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*.[24]

[24] *See* NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST, at 37-42 (May 2022), https://nvlpubs nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf.

C. NIST Should Continue to Provide Change Management Tools and Resources to Help Government Contractors Monitor and Understand Updates to 800-171.

Given the substantial revisions proposed in the Draft to 800-171—which include updates to security requirements and families to reflect updates in 800-53 Rev. 5, the 800-53B moderate control baseline, revised tailoring criteria, and increased specificity for the controls—it is vital that NIST clearly identify what has changed between Revision 2 and Revision 3. In conjunction with the Draft, NIST has already provided helpful change management tools, such as the Change Analysis and Prototype CUI Overlay spreadsheets.[25] NIST should continue to bolster these efforts.

First, NIST should consider clarifying and supplementing its Change Analysis.[26] The Change Analysis references 27 "withdrawn" requirements; however, only five requirements were actually removed from the baseline. The other requirements were re-incorporated into existing controls.[27] NIST should provide a redline comparison of each revised control. Though the Change Analysis in the form of a spreadsheet is helpful, a redline of changes to each control would help parties update their internal control policies and better respond to updates and changes in Revision 3. *Second*, NIST should continue robust public outreach, including hosting public presentations and webinars to communicate and clarify changes to interested parties. Among other venues, sector-specific public-private partnerships such as the Sector Coordinating

[25] *SP 800-171 Rev. 3 (Draft): Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST, https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/draft (last visited July 6, 2023).

[26] Change Analysis (Rev. 2 to IPD Rev. 3), NIST (May 10, 2023), https://csrc nist.gov/csrc/media/Publications/sp/800-171/rev-3/draft/documents/sp800-171r2-to-r3-ipd-analysis.xlsx ("Change Analysis").

[27] *See* Draft SP 800-171 Rev. 3, Protype CUI Overlay: Overview and Request for Feedback, NIST (May 10, 2023), https://csrc nist.gov/csrc/media/Publications/sp/800-171/rev-3/draft/documents/sp800-171r3-ipd-cui-overlay.xlsx ("Prototype CUI Overlay"); Change Analysis.

Councils would offer meaningful engagements.[28]

III. NIST SHOULD ENSURE THAT ORGANIZATIONS SUBJECT TO SP 800-171 HAVE THE FLEXIBILITY TO TAILOR CONTROLS IN A RISK-BASED MANNER TO ACCOUNT FOR DIVERSE NETWORKS AND OPERATING ENVIRONMENTS.

A. NIST Should Ensure that Revision 3 Embodies Its Longstanding Commitment to Risk-Based and Flexible Cybersecurity Guidance by Further Bolstering Flexibility and Amending Overly Prescriptive Elements of the Draft.

Government contractors in the wireless industry, like other government contractors, use varied techniques and technologies to manage cybersecurity risks and protect CUI. Federal contractors have tremendous diversity in their size, complexity, and mission, and as such, they can have very different system architectures. This diversity requires flexible, risk-based approaches. As CTIA has outlined in previous comments, this type of flexible and risk-based approach allows organizations to account for their unique circumstances, including different operations, threats, and risk tolerances.[29]

Similarly, cybersecurity controls should be tailored based on the context and risk profile of any given CUI use case. CUI may require protection and control for a variety of reasons, including security, privacy, law enforcement, and protection of confidential business or financial information.[30] Flexibility is also critical for contractors to establish a fair and workable approach to implementing requirements for safeguarding CUI, considering that contractors may be subject to legal liability related to implementation of 800-171 requirements. Liability can arise under

---

[28] *See Sector Coordinating Councils*, CISA, https://www.cisa.gov/resources-tools/groups/sector-coordinating-councils (last visited July 6, 2023).

[29] *See* Comments of CTIA on Pre-Draft Call for Comments: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (filed Sept. 16, 2022), https://csrc.nist.gov/csrc/media/Projects/protecting-controlled-unclassified-information/Pre-Call-For-Comment-Sept-2022/CUIPreCall_CTIA_Sep16_2022.pdf.

[30] *See CUI Categories*, NARA, https://www.archives.gov/cui/registry/category-list (last visited July 6, 2023).

contracts or subcontracts that incorporate 800-171 as the standard for protecting controlled unclassified information.[31] Controls and protections must therefore be flexible to balance the mission needs of the agencies and their contractors' ability to access and process the information, while accounting for differences in organizations' contexts and risk profiles.

In the Draft, NIST takes important steps in the right direction of promoting a flexible and risk-based approach by highlighting the importance of risk assessments and tailoring controls. In particular, consistent with past CTIA advocacy, the Draft reflects updates that are clearly intended to bolster the flexible and risk-based nature of 800-171. For example, NIST notes that among the changes made, NIST "[i]ntroduced organization-defined parameters (ODPs) in selected security requirements to increase flexibility and help organizations better manage risk."[32] The Draft also contains multiple references to risk-based assessments of the applicability of controls or families of controls. For example, in discussing supply chain security, NIST notes that "a supply chain risk assessment can inform the strategies, tools, and methods that are most applicable to the situation."[33] Similarly, NIST instructs that organizations rely on the results of a risk assessment in considering whether a "secondary system use notification" is needed. The Draft also adds a new tailoring criterion of "Not Applicable" ("NA") and assigns NA to the Project Management and Personally Identifiable Information ("PII") controls.[34] This

[31] Notably, the False Claims Act has been used as an enforcement vehicle to prosecute contractor misrepresentations associated with cybersecurity compliance, and the Department of Justice ("DOJ") has identified contractor cybersecurity as an area of enforcement focus for its Civil Cyber-Fraud Initiative. Press Release, DOJ, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[32] *See* Draft SP 800-171 Rev. 3 at iii.

[33] Draft SP 800-171 Rev. 3 at 60.

[34] *See* Initial Public Draft (IPD) NIST SP 800-171, Revision: Frequently Asked Questions, NIST, at 3 (May 10, 2023), https://csrc.nist.gov/csrc/media/Publications/sp/800-171/rev-3/draft/documents/sp800-171r3-ipd-faq.pdf ("FAQs").

clarification will promote the flexibility of nonfederal organizations to manage internal controls of CUI on the basis of risk and adapted to the privacy laws and regulations applicable to that organization, consistent with past CTIA advocacy related to 800-53 Rev. 5.[35]

But there is more for NIST to do to bolster its risk-based and flexible approach and further account for the type, volume, or location of CUI. Indeed, several aspects of the Draft risk being inflexible, including changes to encryption expectations and other overly prescriptive updates:

- ***Overall Approach:*** The Draft appears to not adequately address the diversity in CUI use cases. For example, the Draft does not include guidance for organizations that handle very little CUI and does not account for the size of the organization in providing its guidance. This type of "one-size-fits-all" approach risks promoting a compliance mindset and unnecessarily increasing compliance costs; providing a roadmap for bad actors; and ossifying contractors' cybersecurity approach—instead of promoting a dynamic and nimble approach that allows contractors to keep pace with evolving threats and complex operating environments.
- ***Prescriptive Controls:*** For several controls, the addition of details in the Draft appears to increase the prescriptiveness of the controls, moving the document away from an outcome-based set of requirements. In 800-171 Rev. 2, each of the 110 requirements is typically explained in a single, broad sentence, giving companies flexibility in how they choose to meet those requirements. However, the Draft updates several of these requirements to add instructive detail or combine multiple requirements under one control; and in a few instances, the addition of detail is overly prescriptive. For example, in the Identification and Authentication control IA-5(1) (Password Management), found at security requirement 3.5.7, the Draft adds new elements that were not specified in the 800-171 Rev. 2 language.[36] 800-171 Rev. 2 stated the requirement for 3.5.7 as follows: "Enforce a minimum password complexity and change of characters when new passwords are created."[37] Rev. 2's language left flexibility for the organization to determine what constitutes a "minimum password complexity" and what constitutes a "change of characters" for new passwords. In contrast, the new 3.5.7 adds prescriptive language from 800-53 Rev. 5 control IA-5, instructing that organizations enforce specific password composition and complexity rules (to be defined as an ODP), and requiring organizations to allow users to select spaces and "all printable characters" in a

[35] *See* Comments of CTIA on Final Public Draft SP 800-53, Security and Privacy Controls for Information Systems and Organizations (filed May 29, 2020).

[36] Draft SP 800-171 Rev. 3 at 29.

[37] SP 800-171 Rev. 2 at 71.

password.

- ***Encryption:*** In the Draft, NIST took a positive step towards a more flexible and risk-based approach by removing prescriptive language around the use of FIPS-validated cryptography in favor of a broader discussion.[38] However, a significant change from Revision 2 to the Draft is the proposed adoption of a requirement for contractors to implement encryption at rest.[39] This requirement removes options for alternative physical safeguards that were available in Revision 2, and as such, should be reconsidered.[40] Rather than a blanket requirement for encryption at rest, NIST should account for implementation of cryptographic protections based on risk and impact. Some types of CUI, such as an organization's internal, non-customer financial or business strategy data may be proprietary and commercially sensitive but may not require encryption at rest or when being used within the organization. There may also be situations in which alternative compensating controls, including the physical safeguards discussed in 800-171 Rev. 2, are appropriate. And, as the federal government prepares for a transition to quantum-resistant cryptography,[41] NIST should ensure that SP 800-171 provides guidance that allows organizations to prioritize the types of CUI that need to be protected as part of this transition.
- ***Independent Assessment:*** The Draft also proposes a requirement for independent assessments of controls, with its description of the requirement implying that employees of the organization may not be impartial or independent.[42] Instead of the Draft's current description, NIST should clarify that the independent assessment control is flexible and can allow for impartial employees to conduct assessments, as appropriate. Indeed, this approach is consistent with 800-53, Rev. 5, which recognizes that "[i]ndependent assessments can be obtained from elements within organizations."[43] Requiring third-party assessors, on the other hand, creates additional risk and burden for organizations to manage and is inappropriate and overly prescriptive for the wide range of private companies that may be subject to SP

[38] Draft SP 800-171 Rev. 3 at 49 ("Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage"). In SP 800-171, the corresponding Control 3.13.11 was: "[e]mploy FIPS-validated cryptography when used to protect the confidentiality of CUI." SP 800-171 Rev. 2 at 81.

[39] Draft SP 800-171 Rev. 3 at 50.

[40] SP 800-171 Rev. 2 at 38 ("Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission *unless otherwise protected by alternative physical safeguards*") (emphasis added).

[41] NIST's National Cybersecurity Center of Excellence ("NCCoE") has a Migration to Post-Quantum cryptography project that works to raise awareness of issues related to the migration. *See Migration to Post-Quantum Cryptography*, NIST, https://www nccoe nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms (last visited July 6, 2023). CTIA is engaged with NCCoE on the project. *See* Comments of CTIA on Draft NIST SP 1800-38A, Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography, Volume A: Executive Summary (filed June 8, 2023).

[42] Draft SP 800-171 Rev. 3 at 46 ("To achieve impartiality, assessors do not … act as management or employees of the organizations they are serving").

[43] NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, NIST, at 85 (Sept. 2020), https://nvlpubs nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ("SP 800-53 Rev. 5"). Even DoD, in its CMMC 2.0 proposal, allows for a self-assessment for a subset of covered contractors. *About CMMC*, DoD, https://dodcio.defense.gov/CMMC/about/ (last visited July 6, 2023).

> 800-171 via contracts. Companies use many methods to conduct assessments and audits, including outside assessors, internal auditors, or third-party certifications. Many companies have robust internal audit functions with considerable expertise in the organization's systems and capabilities, which make outside assessors' contributions less valuable. NIST should recognize the diversity of approaches in the private sector and use a more flexible description of the requirement, consistent with 800-53 Rev. 5, that would allow the requirement for independent assessors to be completed by employees of an organization.

Moving forward, NIST should address these overly prescriptive and inflexible aspects of the Draft and should bolster Revision 3's flexible and risk-based approach. To do this, NIST should (1) add additional language to stress how the publication promotes a flexible and risk-based approach, similar to language in 800-53 Rev. 5, which states, "The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk;"[44] (2) amend prescriptive language and approaches—noted above—that stray from a risk-based, flexible approach; and (3) consider clarifying in the discussion section for each requirement that a requirement can be implemented in different ways in different contexts, which NIST can do by including use case examples or adding language that reserves flexibility for how an organization chooses to implement the control. Taking these steps—which are consistent with NIST's approach in other foundational guidance documents such as the Discussion Draft of the Cybersecurity Framework 2.0 Core[45]—will better align 800-171 with longstanding risk management principles and will help address uncertainty about ODPs, discussed below.

B. If NIST Incorporates the Concept of Organizational-Defined Parameters into 800-171, Flexibility and Voluntariness Should Remain Cornerstones of Implementation.

While ODPs were "[i]ntroduced . . . in selected security requirements to increase

[44] SP 800-53 Rev. 5 at ii.

[45] Discussion Draft of the NIST Cybersecurity Framework 2.0 Core, NIST, at 4-5 (Apr. 24, 2023), https ://www nist.gov/system/files/documents/2023/04/24/NIST Cybersecurity Framework 2.0 Core Discussion Draft 4-2023 final.pdf (including notional "implementation examples" while clarifying that they are neither comprehensive nor a baseline of required actions).

flexibility,"[46] as noted above, NIST should be careful to protect against these tools being used by agencies in practice to impose prescriptive requirements or otherwise reducing organizational flexibility in protecting the confidentiality of CUI.

In the Draft, NIST introduces "fill in the blank" ODPs to 800-171. This concept is drawn from 800-53 Rev. 5,[47] which utilizes ODPs to give the government flexibility to tailor controls to support specific organizational missions or business functions, or to manage risk. In practice in the 800-53 context, federal agencies subject to 800-53 Rev. 5 may develop their own policies and procedures for the system controls that protect the information security needs of their computing systems, following the control structure outlined in 800-53.[48] For the purposes of 800-171, NIST explains that an agency may choose to specify an ODP or provide guidance on how nonfederal organizations may define ODPs.[49] Once ODPs are defined by an agency, they will become part of the security parameters prescribed by that agency.[50]

CTIA appreciates that the introduction of ODPs is intended to maintain flexibility. However, NIST should proceed with caution in this space and protect against the risk that ODPs could lead to federal agencies implementing 800-171 guidelines in an inconsistent or overly prescriptive manner. Determinations by federal agencies to create ODPs could be overly prescriptive or limit the ability of nonfederal organizations to innovate or use a risk-based

---

[46] *See* Draft SP 800-171 Rev. 3 at iii.

[47] SP 800-53A explains further that ODPs allow "the attribute values of depth and coverage [to be] assigned by the organization and specified within the assessment plan (e.g., the level of rigor for documentation review, the number of similar assessment objects to test)." *See* NIST SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations Revision 5, NIST, at 18 (Jan. 25, 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf.

[48] For example, 800-53 Rev. 5 requirements may defer to organization-defined parameters to allow the organization to provide implementation detail, such as frequency of testing. *See* SP 800-53 Rev. 5 at 11. Where that is the case, agency-specific guidance will then define these parameters for any given requirement.

[49] *See* Draft SP 800-171 Rev. 3 at 4.

[50] *Id.*

approach to address the controls. Furthermore, if federal agencies set different ODPs, nonfederal organizations may be required to impose different criteria, approaches, or solutions simultaneously. Some of these requirements may not be compatible, posing problems particularly for government contractors working with different agencies. Contractors might then assess the ODPs their customer agencies promulgate and choose to require implementation of the most stringent ODP across the contractor organization out of an abundance of caution, and at significant cost. In this way, overly specific and unharmonized ODPs will likely impose significant hardship on small and medium-sized businesses.

To protect against these unintended outcomes, where practical, NIST should encourage federal agencies to refrain from setting arbitrary or inflexible ODPs, and instead allow nonfederal organizations to internally define risk-based ODPs, as needed. And while NIST has noted that it will not produce default or baseline ODPs,[51] NIST should work with the appropriate federal partners to help promote a government-wide approach to ensure ODPs are flexible and risk-based and to determine which ODPs should be defined consistently across agencies, and which may require more tailored, agency-specific parameters. These recommended steps for NIST to promote flexibility and harmonization with respect to ODPs will help ensure that Revision 3 is not overly prescriptive, help reduce confusion arising from possible inconsistencies between ODPs, and help procurement stakeholders adopt the updated guidance faster and more efficiently.

[51] NIST, *Protecting Controlled Unclassified Information: What's New in Draft SP 800-171 Rev. 3*, at 58:20 (June 6, 2023), *available at* https://csrc.nist.gov/Events/2023/protecting-cui-draft-sp800171-rev3 ("June 6, 2023 NIST CUI Webinar").

IV. NIST SHOULD CONTINUE TO PROMOTE HARMONIZATION OF PROCUREMENT-RELATED CYBERSECURITY EXPECTATIONS, WHILE PRIORITIZING A FLEXIBLE AND RISK-BASED APPROACH.

A. NIST Has Already Taken Steps to Harmonize Various Lines of Effort with Respect to CUI and Other Procurement-Related Guidance, Which Is Important To Promote Clarity and Consistency.

Harmonization of various procurement-related cybersecurity efforts is critical in developing clear guidance that can be consistently implemented by industry. CTIA has previously advocated for NIST to align the 800-171 series with other federal cybersecurity efforts, including the 800-53 controls and CMMC 2.0 program. This is consistent with the emphasis in the National Cybersecurity Strategy on the need to harmonize and streamline cybersecurity efforts more generally.[52] Indeed, clear and consistent direction will allow for quicker and more widespread adoption of security practices, while duplicative, confusing, or contradictory recommendations could slow implementation.

To this end, NIST has already taken important steps towards harmonization. For example, NIST's decision to release the next draft of *Assessing Security Requirements for Controlled Unclassified Information*, SP 800-171A ("800-171A"), in tandem with the next revision to the Draft, helpfully promotes harmonization.[53] An outdated version of 800-171A could not be used to assess an organization's adoption of 800-171 Rev. 3. Therefore, coupling the 800-171 and -171A revisions will significantly reduce the burden on the community of having to adapt internal or externally required assessments of 800-171 implementation without the associated assessment guidance.

---

[52] National Cybersecurity Strategy, The White House, at 9 (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[53] Protecting Controlled Unclassified Information: What's New in Draft SP 800-171, Revision 3, NIST, at 15 (June 6, 2023), https://csrc.nist.gov/csrc/media/Presentations/2023/new-in-draft-sp-800-171-rev-3/images-media/NIST-SP-800-171-WEBINAR-6June2023.pdf.

The Draft also makes useful changes that aim to focus 800-171 on controls directly related to protecting the confidentiality of CUI, so as not to create unnecessary overlap or confusion with other guidance. In the Draft, NIST acknowledges certain nonfederal organization ("NFO") controls—meaning controls designated as "[e]xpected to be implemented by nonfederal organizations without specification"[54]—were not being implemented or assessed, so the Draft reassigns several of these NFO controls, which will give nonfederal organizations more clarity as to whether the control may be evaluated for compliance with SP 800-171.[55]

NIST has also rightly worked to promote harmonization with respect to aligning 800-171 with 800-53 Rev. 5. *First*, the Draft further aligns 800-171 with 800-53 Rev. 5: specifically, the Draft provides an overlay that explains how NIST has tailored the requirements from the moderate baseline in 800-53 Rev. 5 to develop the requirements in the Draft.[56] This re-alignment goes a long way towards harmonizing 800-171 with the other frameworks that can be mapped back to 800-53, such as FedRAMP. *Second*, the Draft removes the distinction between "basic" controls, meaning controls based on FIPS-200, and "derived" controls, meaning the controls derived from 800-53 and considered relevant to protecting confidentiality of CUI.[57] As background for this change, NIST explains that while the security requirements for safeguarding CUI in nonfederal systems and organizations are derived from FIPS 199, FIPS 200, and 800-53, it determined that the description of requirements in FIPS 200 lacked specificity.[58] Revision 3

[54] *See* Draft SP 800-171 Rev. 3 at 79. The Draft reclassifies these controls as NCO (an NCO designation means that the controls are "[n]ot directly related to protecting the confidentiality of CUI"); FED (a FED designation means that the controls are "[p]rimarily the responsibility of the Federal Government"); or CUI (A CUI designation means that the controls are "[d]irectly related to protecting the confidentiality of CUI."). *Id.*

[55] *See* FAQ at 2-3.

[56] *See* Prototype CUI Overlay.

[57] *See* FAQs at 1.

[58] *Id*. at 1-2.

therefore aims to increase specificity and clarity of the requirements by refocusing the security requirements to align more closely to language used in 800-53, rather than FIPS publications.[59] *Third*, the Draft provides a Prototype CUI Overlay[60] that shows how the requirements in the Draft align with the controls in 800-53 Rev. 5, with an explanation of the tailoring decisions that NIST made in developing the Draft.[61] These explanations help nonfederal organizations understand how 800-171 security requirements were added, removed, or re-incorporated in the Draft Revision to more closely align 800-171 with 800-53.

While harmonization is an important goal and NIST's effort to further align 800-171 with 800-53 is in many respects helpful, CTIA encourages NIST to proceed with caution with respect to its broad application of 800-53, Rev.5 and its future plans for both documents in light of the fact that NIST has explained that its long-term goal is to move away from having specific 800-171 requirements and instead use only 800-53 controls.[62] *First,* as CTIA has consistently advocated, 800-53 is a document that was intended to provide a catalog of controls for federal systems.[63] Accordingly, its controls are not tailored for contractors handling CUI. 800-171 provides an important foundation for tailoring government agency-specific 800-53 controls for non-government systems that have diverse and unique architectures, and NIST should encourage

[59] *Id.*

[60] *See* Prototype CUI Overlay.

[61] For example, the Prototype CUI overlay shows how NIST tailored control SC-28, Protection of Information at Rest in 800-53 Rev. 5, to security requirement 3.13.8 in 800-171 by combining multiple requirements and updating the title to reflect the merged requirements.

[62] June 6, 2023 NIST CUI Webinar at 19:15 (noting a long-term goal to move away from specific requirements in 800-171 and instead use only 800-53 language). Controls applicable to CUI would then be identified only through an "Overlay." *Id.* at 20:00 (describing a future in which there are no separate 800-171 requirements, but instead 800-171 becomes a CUI overlay in the 800-53 control catalog.)

[63] Comments of CTIA on Draft NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, at 2 (filed Sept. 12, 2017) ("If NIST insists on integrating privacy and security controls, it should clearly state that 800-53 is for federal systems and is likely to be of limited utility to the private sector").

further tailoring, guided by longstanding risk management principles, as 800-171 is implemented and applied in various operating environments. This tailoring step is critical, and NIST should protect against the misconception that 800-53 Rev. 5 controls can simply be picked up and transferred into 800-171 without flexibility and risk-informed considerations. *Second*, while CTIA recognizes the potential benefits of having a single set of source controls derived from 800-53, those benefits do not outweigh the potential harms of doing away with 800-171 as a standalone document, which would be in tension with the important tailoring function that 800-171 serves. Since its inception, 800-171 has added value because it enables nonfederal entities who are subject to CUI protection requirements to adapt their security controls to their unique system architectures and operating environments. Maintaining a separate set of requirements for nonfederal organizations allows those entities to adapt their security to account for the size, complexity, and mission of each organization, and the types of CUI the organization handles. Removing 800-171 as a standalone document would undermine the flexible approach that recognizes that nonfederal systems are substantially different than federal systems.

B. NIST Should Take Additional Steps To Align 800-171 with Cybersecurity Guidance that May Be Relevant to Contractors.

Overall, providing tools to show the interconnections between relevant procurement guidance will be helpful for organizations implementing 800-171, especially small and mid-sized government contractors. While the Draft provides a good start towards this goal, NIST should consider further alignment with key cyber guidance relevant to contractors. With respect to further alignment with 800-53 Rev. 5 and other relevant cyber guidance, NIST has noted that it does not intend to provide a mapping between Revision 3 and other sets of security controls,

other than updating the mapping between 800-53 Rev. 5 and ISO/IEC 27001:2022.[64] NIST should reconsider this position and create updated mappings or overlays between 800-171 and other sets of security control frameworks that can be mapped back to 800-53, such as FedRAMP. The Draft includes several significant changes to security requirements, so prior mappings of Revision 2 will be outdated. Further, revised mappings will help nonfederal organizations, including government contractors who will be directly impacted by changes in Revision 3, get up to speed on new requirements and better prepare to implement those requirements promptly. With respect to further alignment with CMMC, DoD is currently revamping the CMMC program under CMMC 2.0, with an interim rule expected to be published next year.[65] As noted above, CMMC 2.0 will leverage the 800-171 Series requirements; specifically, CMMC Level 2 will require compliance with all SP 800-171 requirements and either a self-assessment or a CMMC Third Party Assessment Organization assessment to confirm compliance.[66] Additionally, CMMC Level 3 will require compliance with at least a subset of the 800-172 requirements and a government assessment to confirm compliance.[67] It is therefore particularly important for NIST to engage with DoD to ensure alignment.

Further, NIST should coordinate closely with agencies regarding how 800-171 Rev. 3 is implemented in government contracts. As changes to 800-171 will necessarily impact federal agencies—particularly DoD because of the CMMC 2.0 program, as noted above—NIST should consult with those federal entities and consider how 800-171 will interact with ongoing efforts,

---

[64] *See* FAQs at 4.

[65] *See CMMC FAQs*, DoD, https://dodcio.defense.gov/CMMC/FAQ/ (last visited July 7, 2023); Mark Pomerleau, *Pentagon updates timeline for CMMC cybersecurity initiative*, FedScoop (May 18, 2022), https://www.fedscoop.com/pentagon-updates-timeline-for-cmmc-cybersecurity-initiative/.

[66] Cybersecurity Maturity Model Certification Version 2.0: Overview Briefing, DoD (Dec. 3, 2021), https://dodcio.defense.gov/Portals/0/Documents/CMMC/CMMC-2.0-Overview-2021-12-03.pdf.

[67] *Id.*

and should encourage DoD and relevant federal agencies whose programs rely on 800-171 to promote a harmonized approach to implementation. Additionally, NIST should coordinate directly with agencies who incorporate 800-171 or plan to issue related rulemakings regarding whether and how Revision 3 requirements should be flowed down to subcontractors. Of note, the Federal Acquisition Regulation ("FAR") Council is expected to issue a proposed rule in FAR Case No. 2021-019 in the coming months;[68] this proposed rule is expected to standardize common cybersecurity contractual requirements, as mandated by Executive Order 14028. NIST should consider how this rulemaking will interact with SP 800-171. And, as referenced in the ODP discussion above, NIST should encourage federal agencies to make sure that their CUI guidance is consistent with 800-171, or that it does not unduly diverge from the 800-171 baselines or adopt an overly prescriptive or inflexible approach.

V. CONCLUSION

CTIA is pleased to continue to work with NIST on 800-171 and the CUI series. As NIST finalizes Revision 3, NIST should (1) work to clarify issues around identifying CUI, potential subcontractor flow-downs, and change management between 800-171 Revisions 2 and 3; (2) ensure that 800-171 continues to provide flexible, risk-based guidance, and especially protect against mechanisms intended for flexibility being used in an unintended prescriptive manner; and (3) promote harmonization with other procurement-related guidance, including 800-53 Rev. 5.

[68] Open FAR Cases as of 6/30/2023, DoD, at 6 (June, 30, 2023), https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf.

/s/ Thomas K. Sawanobori
Thomas K. Sawanobori
Senior Vice President, Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Justin C. Perkins
Manager, Cybersecurity and Policy

CTIA
[redacted]

July 14, 2023