From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] Comments on CUI Series Publications: CTIA Comments on NIST SP 800-171
Date: Friday, September 16, 2022 4:10:46 PM
Attachments: CTIA Comments re NIST SP 800-171 Pre Draft Call for Comments.pdf

Good afternoon,

Please find attached CTIA's comments on NIST SP 800-171. Let us know if you have any questions.

Thank you!

Justin Perkins

Justin Perkins
Manager, Cybersecurity & Policy
1400 16th Street, NW
Washington, DC 20036
[redacted]

September 16, 2022

Via 800-171comments@list.nist.gov
Dr. Laurie Locascio
Under Secretary of Commerce for Standards and Technology and Director, National Institute of Standards and Technology
United States Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20889

Re: Pre-Draft Call for Comments: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Dear Dr. Locascio,

CTIA[1] appreciates the opportunity to engage with the National Institute of Standards and Technology ("NIST") as it updates its Controlled Unclassified Information ("CUI") publications ("800-171 Series"), starting with SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* ("SP 800-171").[2] CTIA has collaborated with NIST on numerous cybersecurity issues and proceedings, including by providing feedback on the 800-171 Series, SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* ("SP 800-53"), the *Framework for Improving Critical Infrastructure Cybersecurity*, and other important cybersecurity guidance documents.

CTIA members include many of the world's largest carriers that provide voice, data, and cloud-based services to the federal government under contracts and subcontracts, including with the Department of Defense ("DoD"). CTIA supports NIST's interest in promoting the cybersecurity of non-federal systems handling CUI and to protect key systems and networks in a sophisticated and dynamic threat environment.

CTIA supports the comments of the Information Technology Industry Council ("ITI") in this proceeding, and offers these comments to provide further perspective from the wireless industry. Specifically, as NIST considered updates to the 800-171 Series, CTIA encourages NIST to: (1) incorporate the flexibility needed to allow organizations to tailor 800-171 Series controls in a risk-based manner; (2) align the 800-171 Series with other federal cybersecurity efforts, including the Department of Defense's ("DoD") Cybersecurity Maturity Model Certification ("CMMC") 2.0 program; and (3) consider targeted changes to SP 800-171's treatment of encryption to account for the current threat environment.

[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] NIST, *Pre-Draft Call for Comments: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/draft (last visited Sept. 9, 2022) ("Pre-Draft Call for Comments").

<u>NIST Should Ensure That Any Updates to the 800-171 Series Promote Flexibility and Allow Organizations to Tailor Controls in a Risk-Based Manner.</u>

As CTIA has consistently advocated to NIST and other federal agencies, it is important that cybersecurity guidance be flexible and risk-based. This approach allows organizations to properly balance risk, resource, and threat assessment considerations as they devise optimal cybersecurity solutions. To that end, NIST has previously endorsed this approach and explicitly incorporated flexibility into the 800-171 Series. For example:

- In SP 800-172A, *Assessing Enhanced Security Requirements for Controlled Unclassified Information*, NIST states that "[o]rganizations are not expected to use all of the assessment methods and objects contained within the assessment procedures identified in this publication. Rather, organizations have the flexibility to establish the level of effort needed and the assurance required for an assessment (e.g., which assessment methods and objects are deemed to be the most useful in obtaining the desired results). The decision on level of effort is made based on how the organization can accomplish the assessment objectives in the most cost-effective and efficient manner and with sufficient confidence to support the determination that the CUI enhanced security requirements have been satisfied."[3]

- In a draft version of SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171* ("SP 800-172"), NIST wrote that "[b]ased on feedback received during the public comment period, the final draft of this publication includes . . . a more flexible requirements selection approach to allow implementing organizations to customize their security solutions. Assignment and selection statements have also been added to certain requirements to give organizations the flexibility to establish specific parameter values, where appropriate."[4]

As NIST considers updates to the 800-171 Series, CTIA encourages NIST to maintain this important flexibility and facilitate a risk-based approach to the implementation of 800-171 Series controls.

Moreover, NIST should build on this risk-based foundation by adding to the 800-171 Series clear, flexible guidance that is specific to procurement professionals. One important procurement-specific consideration that NIST should explicitly address is contractors' ability to select 800-171 Series controls under a risk management framework. By acknowledging that the selection of security controls necessitates a risk-based analysis, NIST will provide tangible value to contractors seeking to comply with the 800-171 Series in a manner appropriate for their own individual company.

Similarly, NIST should provide guidance for federal procurement officials on the need to carefully consider whether 800-171 Series controls should be required for contracts that handle very little CUI, as

[3] NIST, SP 800-172A, Assessing Enhanced Security Requirements for Controlled Unclassified Information, at 5 (Mar. 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172A.pdf.

[4] NIST, Draft SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171, at iv (July 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172-draft.pdf.

the burdens of compliance are likely to outweigh the benefits for such contracts. Further, NIST should develop guidance that addresses if and when it is appropriate for prime contractors to flow down 800-171 Series requirements when CUI is stored in subcontractor systems. NIST has previously addressed the issue of flow-down requirements in the "C-SCRM in Acquisition" section of SP 800-161 Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, and it should use that section as a guide for addressing this issue in the 800-171 Series.[5]

<u>NIST Should Align 800-171 Series Guidance With Other Federal Cybersecurity Efforts, Including DoD's CMMC 2.0 Program.</u>

In the Pre-Draft Call for Comments, NIST asks stakeholders for suggestions on "[h]ow to improve the alignment between the [800-171 Series] and other frameworks."[6] CTIA recommends that NIST ensure that any updates to the 800-171 Series align with the standards required of the government under SP 800-53.

NIST has long valued consistency across federal and non-federal systems in protecting CUI. Indeed, SP 800-171 is based on the following "fundamental assumptions": (1) "[s]tatutory and regulatory requirements for the protection of CUI are *consistent*, whether such information resides in federal systems or nonfederal systems including the environments in which those systems operate;" (2) "[s]afeguards implemented to protect CUI are *consistent* in both federal and nonfederal systems and organizations;" and (3) "[t]he confidentiality impact value for CUI is no less than [Federal Information Processing Standards ("FIPS") 199] *moderate*."[7] Consistent with these assumptions, NIST should ensure that any changes to SP 800-171 do not provide more onerous requirements than are applied to the federal government under SP 800-53. Further, to promote consistency and harmonization, NIST should map the overlapping controls between SP 800-171 and SP 800-53.

In addition to maintaining consistency with SP 800-53, it is crucial that NIST coordinate and work closely with DoD as it develops CMMC 2.0. DoD is currently revamping the CMMC program under CMMC 2.0, with an interim rule expected to be published next year.[8] CMMC 2.0 will leverage the 800-171 Series controls; specifically, CMMC Level 2 will require compliance with all 110 SP 800-171 controls and either a self-assessment or a CMMC Third Party Assessment Organization assessment to confirm compliance.[9] Additionally, CMMC Level 3 will require compliance with at least a subset of the SP 800-172 controls and a government assessment to confirm compliance.[10]

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

[6] Pre-Draft Call for Comments.

[7] NIST, SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, at 5 (Feb. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf ("SP 800-171 Rev. 2").

[8] *See* DoD, *CMMC FAQs*, https://www.acq.osd.mil/cmmc/faq.html (last visited Sept. 9, 2022); Mark Pomerleau, *Pentagon updates timeline for CMMC cybersecurity initiative*, FedScoop (May 18, 2022), https://www.fedscoop.com/pentagon-updates-timeline-for-cmmc-cybersecurity-initiative/.

[9] DoD, Cybersecurity Maturity Model Certification Version 2.0: Overview Briefing (Dec. 3, 2021), https://www.acq.osd.mil/cmmc/docs/CMMC-2.0-Overview-2021-12-03.pdf.

[10] *Id.*

It is critical that NIST appreciate the substantial resources that contractors expend to comply with the 800-171 Series. As a result, there would be significant compliance costs if the 800-171 Series is inconsistent with guidance that DoD issues under CMMC 2.0. To that end, as NIST coordinates with CMMC on aligning the 800-171 Series with CMMC 2.0, it is important that, at a minimum: (1) DoD contractors who receive a CMMC Level 2 certification from an independent assessment organization while the 800-171 Series is being updated will maintain their certification; and (2) CMMC's three-year certification period will apply during this period. Additionally, in coordinating with DoD, NIST should address not just the content of and guidance about specific security controls, but also more global considerations such as when and to what extent these controls are required. This coordination will facilitate risk-based implementations of the important guidance provided in the 800-171 Series.

NIST Should Consider Targeted Changes to SP 800-171's Treatment of Encryption to Account for the Current Threat Environment.

SP 800-171 currently requires organizations to encrypt all CUI using cryptography validated according to FIPS 140-series requirements.[11] In light of issues with the Cryptographic Module Validation Program's ability to quickly validate new cryptographic modules, NIST should re-consider this control and ensure that any encryption requirements account for these challenges. Moreover, as the federal government prepares for a transition to post-quantum cryptography, 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.

* * *

CTIA is pleased to provide feedback to NIST as it updates the 800-171 Series. As NIST proceeds with this update, CTIA recommends that NIST: (1) incorporate sufficient flexibility to allow organizations to tailor 800-171 Series controls according to a risk assessment; (2) align the 800-171 Series with other federal cybersecurity efforts, including DoD's CMMC 2.0; and (3) consider targeted changes to SP 800-171's treatment of encryption.

Respectfully submitted,

/s/ Thomas K. Sawanobori

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
1400 16th Street, NW, Suite 600

[11] SP 800-171 Rev. 2, at 81 (describing Control 3.13.11 as: "[e]mploy FIPS-validated cryptography when used to protect the confidentiality of CUI").

Washington, DC 20036
[redacted]
www.ctia.org