From: [redacted] 800-171comments
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] ITI Comments for NIST SP 800-171 Pre-Draft Call for Comments
Date: Thursday, September 15, 2022 12:47:45 PM
Attachments: ITI Comments on NIST SP 800-171 Pre-Draft Call for Comments.pdf

---

Dear NIST Colleagues,

The Information Technology Industry Council (ITI) appreciates the opportunity to provide pre-draft comments on the revision of SP 800-171. ITI has long considered SP 800-171 and the overall CUI protection series to be an invaluable resource to organizations looking for guidance on storing sensitive government information in their systems. In this context, we believe the SP 800-171 revision presents a key opportunity for NIST to make helpful updates to the document.

We thank you for your consideration of our comments and remain available to answer any follow up questions.

Best regards,

Leopold Wildenauer
Policy Manager, Public Sector
Information Technology Industry Council
700 K Street NW, Suite 600
Washington, DC 20005
[redacted]

ITI Promoting Innovation Worldwide

9/15/2022

Dr. Laurie Locascio
Under Secretary of Commerce for Standards and Technology and Director, National Institute of Standards and Technology (NIST)
United States Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20889

Dear Dr. Locascio,

The Information Technology Industry Council (ITI) appreciates the opportunity to submit our thoughts on the upcoming revision of NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.* ITI is the premier advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers with the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

ITI's members, who are uniquely attuned to the challenging and evolving cyber threats facing the U.S. and the world, deeply understand the importance of network security and protecting sensitive federal data. Many of our members are key partners with the U.S. government, providing innovative IT equipment and services needed to optimize government operations. ITI has long considered SP 800-171 and the overall CUI protection series to be an invaluable resource to organizations looking for guidance on storing sensitive government information in their systems. In this context, we believe the SP 800-171 revision presents a key opportunity for NIST to make helpful updates to the document.

We urge NIST to:

- Prioritize reciprocity between various cybersecurity schemes
- Integrate key policy developments, including the rollout of the U.S. Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) and the May 2022 National Security Memo (NSM)-10
- Create user-friendly tailoring guidance for the document's security controls
- Include guidance for acquisition professionals

General Comments

<u>Reciprocity</u>

The importance of reciprocity when developing guidance for federal contractors' storage of critical U.S. government information cannot be overstated. Alignment between U.S. and international cybersecurity schemes and frameworks is crucial to ensuring that U.S. government agencies have

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
[redacted]

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
[redacted]

[redacted]
www.itic.org
@iti_techtweets

access to a diverse supplier base that can expedite the rate of compliance with the new SP 800-171 requirements. Thus, NIST should prioritize reciprocity in revising the SP 800-171 guidance.

NIST should collaborate with appropriate government stakeholders to perform a comprehensive crosswalk for various contractor cybersecurity schemes that leverage the controls contained in SP 800-171. ITI recommends that NIST work with DoD and GSA to standardize how contractors report the body of evidence used in various assessments. If a contractor has already provided sufficient proof of control implementation in a previous assessment, they should be allowed to reuse the standardized body of evidence for other compliance schemes that leverage the same underlying controls from SP 800-171. Such a standardized reporting format will give contractors a clear sense of what additional requirements are needed to demonstrate their compliance with another cybersecurity scheme. This will improve the process for assessments leveraging the same standard and increase the availability of shared services to the federal government. For example, contractors may leverage the same standardized body of evidence to demonstrate successful implementation of controls for FedRAMP Moderate and CMMC Level 2. To that end, we urge NIST to work with GSA and DoD to provide standardized crosswalk between NIST SP 800-171, FedRAMP, CMMC, and DoD's Cloud Computing Secure Requirements Guide.

Internationally, NIST should explore how it might align a revision of SP 800-171 with the United Kingdom government's cloud security guidance as well as international consensus standards like ISO/IEC 20243-1:2018 (O-TTPS), regarding maliciously tainted and counterfeit products. We also recommend that NIST map ISA/IEC 62443 to SP 800-171 as a normative reference for cybersecurity for operational technology in automation and control systems. The 62443 international series of standards is widely known and used within industry; NIST could alleviate compliance challenges while maintaining the highest standards of cybersecurity by mapping SP 800-171 to 62443 and allowing Federal Government partners to provide 62443- or NIST-aligned compliance attestations.

Coordinated Rollout of NIST SP 800-171 Revision and DoD CMMC 2.0

DoD is currently in the process of implementing CMMC 2.0, which leverages SP 800-171 as its core requirements for CMMC Level 2 and SP 800-172 for CMMC Level 3. NIST should coordinate with stakeholders in DoD and elsewhere in the executive branch to reduce instances of confusion while both cybersecurity initiatives are implemented concurrently. At a minimum, the U.S. government should clarify that DoD contractors who receive a CMMC Level 2 certification from an independent assessment organization while the SP 800-171 revision is ongoing should not have to start from scratch when NIST publishes a newer version of this guidance, and that the CMMC's three-year certification period should still apply during this transition.

Our responses to the topic areas related to 800-171 and the CUI series are as follows:

1. *How organizations are currently using the CUI series (SP 800-171A, SP 800-172 and SP 800-172A)*
2. *How organizations are currently using the CUI series with other frameworks and standards (e.g., NIST Risk Management Framework, NIST Cybersecurity Framework, GSA Federal Risk*

and Authorization Management Program [FedRAMP], DOD Cybersecurity Maturity Model Certification [CMMC], etc.)

3. *How to improve the alignment between the CUI series and other frameworks*

In addition to the above, ITI recommends that NIST drive alignment between SP 800-171 and the NIST Cybersecurity Framework. NIST's current efforts to update the CUI Series and the Cybersecurity Framework concurrently present an opportunity for NIST to align both revisions and continue streamlining language and standards around cybersecurity.

4. *Benefits of using the CUI series*
5. *Challenges in using the CUI series*

Our member organizations consider SP 800-171 to be a valuable resource for understanding the cybersecurity requirements for protecting sensitive government information on their systems. We also believe that there is room for NIST to make it more accessible to technical and non-technical audiences alike. We recommend that NIST release as part of its revision a succinct compliance guide for a variety of audiences, with useability as the ultimate goal. NIST should also include comprehensive FAQs early in the document to improve useability.

NIST should also provide more guidance and examples on how to become SP 800-171 compliant. This could include high-level architecture examples, processes, technology stack examples, policy samples and templates, and/or a list of companies and consultants that can help with compliance efforts. For example, there is currently no guidance on what is expected in an organization's system security plan (SSP). Companies must create an SSP from scratch without knowing what the appropriate scope is. Is a broad, top-level SSP sufficient or do companies need to create an SSP for each individual system (laptops, servers, etc.)? In this case, strong examples of SSPs and explainer videos about how to draft an SSP would help organizations of all sizes set expectations and allocate resources efficiently.

We recommend that NIST publish less technical volumes for executive audiences in the same way NIST has created such volumes in the preliminary draft of NIST SP 1800-35A *Implementing a Zero Trust Architecture,* targeting business decision makers (SP 1800-35A), technology, privacy, security program managers (SP 1800-35B) and IT professionals (SP 1800-35C). SP 800-171 is by nature very technical, which is suitable for technical professionals within an organization; however, organization-wide understanding and buy-in for compliance requires that SP 800-171 be more friendly for a non-technical audience as well.

Additionally, we believe NIST should update certain SP 800-171 controls regarding access control, identification, and authentication to reflect that when Virtual Desktop Infrastructure (VDI) is used to control access, device identification is not necessary, since with VDI access there is no data stored on devices. NIST should amend controls 3.1.1 (limit information system access to authorized users, processes acting on behalf of authorized users, or devices), 3.5.1 (identify information system users, processes acting on behalf of users, or devices), and 3.5.2 (authenticate or verify the

identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems) to account for the usage of VDI.

6. *Impact on the usability and existing organizational implementation (i.e., backward compatibility) of the CUI series if it were updated for consistency with SP 800-53 Revision 5 and the moderate security control baseline in SP 800-53B*

NIST's SP 800-53 Rev. 5 fixes certain interpretations in controls from which SP 800-171 has been derived (e.g., split tunnelling), and has added a new family of controls for supply chain risk management (SCRM). Because of their close relation to the underlying standard, SP 800-171 and -172 should be thought of as overlays to SP 800-53. As NIST SP 800-171 and -172 are updated, there needs to be clear instruction on backward compatibility and mapping to newer controls. NIST already adopted a similar approach to handling SCRM controls in the recent revision of SP 800-161 which mirror those contained in SP 800-53. This approach could serve as a model for the revision of SP 800-171 and future updates to the SP 800-series.

One SP 800-53 control assumes that the dash-1 policy and procedure controls are needed to ensure a particular family of controls are based in defined organizational policy and procedure. CMMC 1.0 had a maturity framework that mapped to the Non-Federal Controls defined in SP 800-171 but has been removed in CMMC 2.0. In future revisions of SP 800-171, clear guidelines should be provided in maturing the control framework and how the dash- controls are inherited or incorporated explicitly.

7. *Features of the CUI series that should be changed, added, or removed.*

<u>Clarify 20 Additional Controls from CMMC 1.0</u>
CMMC 1.0 included a delta of 20 additional controls for companies seeking CMMC Level 3 (now CMMC Level 2) certification. These controls were designed to serve as stepping stones to some of the controls in the higher CMMC levels. We ask that NIST provide clear guidelines as to whether some or all of these additional controls will be included in the next SP 800-171 revision.

<u>Expand Scope of SP 800-171 to Include Operational Technology (OT)</u>
When SP 800-171 was originally published in 2015 and updated in 2016 and 2020, much of the cybersecurity community was focused on securing information technology (IT) systems and assets. However, given the rapid increase in attacks on operational technology (OT), which is used to control physical functions within critical environments, any future updates to the CUI Series should consider how CUI flows within and between OT as well as IT systems and provide detailed guidance to practitioners on how to address these challenges. Mapping the SP 800-171 controls to ISA/IEC 62443 will assist in these challenges.

<u>Include Guidance for Tailoring Controls</u>
Tailoring the various controls from a NIST framework to apply scoping considerations, select compensating controls, assign values to agency-defined control parameters, and supplement baselines with control enhancements or additional controls is a common practice within the U.S.

government. NIST should consider providing tailoring guidance to contractors holding CUI on non-federal systems, working with the National Cybersecurity Center of Excellence (NCCoE) in the process.

Take Steps to Improve Cryptography Validation Process and Implement Directives from National Security Memo (NSM)-10 on Cryptography

SP 800-171 control 3.13.11 requires organizations to encrypt all CUI using cryptography validated according to the Federal Information Processing Standards (FIPS) 140-series requirements. As ITI outlined to NIST in multiple letters throughout 2021 and 2022, there have been substantial difficulties related to the Cryptographic Module Validation Program (CMVP)'s ability to quickly validate new and innovative cryptographic modules. The backlog of cryptographic modules waiting in queue remains stubbornly high; this challenge runs the risk of limiting the availability of critical cryptographic products for government use and halting missions altogether. ITI strongly recommends that NIST continue its work to find ways to streamline and automate the CMVP validation process and resolve the backlog associated with the program.

Additionally, we believe it is critical for NIST to clarify use cases in which FIPS 140-2 or FIPS 140-3 compliant settings are to be used, including in firewalls or in the use of cloud services.

Furthermore, NSM-10 outlined a plan for the U.S. government to develop and fully transition to quantum-resistant cryptographic algorithms by 2035. We suggest that, in preparation for this goal, the SP 800-171 revision include guidance on how organizations can inventory their systems to determine what data should be a priority to protect as the U.S. moves to quantum-resistant cryptography.

Add Dedicated Section Tailored to Government Acquisition Professionals

Though NIST notes early in the current guidance that the federal acquisition workforce is a key audience for SP 800-171, ITI believes the document would be strengthened with specific guidance for acquisition professionals as they conduct procurements that involve the storage of CUI in contractor systems. NIST should use the "C-SCRM in Acquisition" section in SP 800-161 Rev. 1, *Cyber Supply Chain Risk Management for Systems and Organizations* as a model. We recommend that this section include the following:

1. Language discouraging federal acquisition personnel from using lowest price technically acceptable (LPTA) source selection for IT and cybersecurity procurements, in line with a January 2021 Federal Acquisition Regulation (FAR) final rule. While LPTA is one of the most common source selection procedures used by federal contracting personnel, there has been a growing understanding that LPTA cannot assess the potential risk posed by a source, does not account for other risk mitigating actions or hidden costs outside the scope of the procurement (like ransomware payments), and cannot reliably ensure the selection of the highest-performing IT product. NIST should also consider recommending that price only be considered by contracting officers after the technical evaluation process, when the pool has been narrowed to bidders who have "cleared the bar" in terms of maturity.

2. A discussion of when it is appropriate for prime contractors to flow down the SP 800-171 requirements when CUI will be stored in a subcontractor's systems. NIST should clarify that while protecting sensitive federal information is critical, prime contractors should avoid overapplying flow down requirements to prevent artificially limiting their supplier base.
3. A reminder that contracting officers and program managers should be mindful in requiring SP 800-171 in contracts in acknowledgement that it can be cost-prohibitive for companies handling very little CUI to implement the guidance. The more expensive the controls are to implement, the more likely it is that the U.S. government will lose diversification in its supply chain as a result of companies choosing to exit the federal marketplace.

7a. Addition of new resources to support implementation: The benefits and challenges of including an SP 800-53 Control Overlay and/or a Cybersecurity Framework Profile Appendix as an alternative way to express the CUI requirements

ITI believes NIST should amend control 3.13.1 (monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the information systems) to clarify that when boundary monitoring is by passive sensing only and when no mission data is stored or transmitted to Security teams, those Security teams and their systems can be considered out-of-scope for CUI.

Concerning controls 3.14.4 (update malicious code protection mechanisms when new releases are available) and 3.14.5 (perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed), NIST should state that when using Next-Generation Antivirus (NGAV) and where the assessment of malware is context, behavior, or usage-based determination, periodic scan profile updating is not a functional requirement.

7b. Change to the security requirement tailoring criteria: Impact of modifying the criteria used to tailor the moderate SP 800-53B security control baseline (e.g., the potential inclusion of controls that are currently categorized as NFO – Expected to be routinely satisfied by nonfederal organizations without specification)

Concerning control 3.8.3 (sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse), NIST should clarify that this requirement can be security tailored as not applicable for organizations that do not use removeable system media.

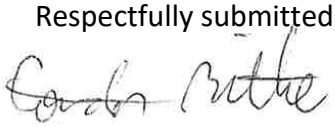
8. Any additional ways NIST could improve the CUI series
We recommend that NIST provide guidance tailored to managers and users of shared services that will have to implement the SP 800-171 requirements. We believe this will benefit small businesses that currently lack sufficient resources to make technical decisions on control implementation, and this guidance would tell them what controls they must implement themselves versus which ones

can and should be provided by a managed service provider (MSP) or a cloud service provider (CSP).

This guidance should also provide clarity on the role of a CSP versus an MSP regarding who "owns" which aspects of the network security process. While a CSP provides infrastructure and/or platform services, the MSP is responsible for the correct configuration of those services to the SP 800-171 requirements, connection to those services, and ongoing continuous monitoring. NIST should use the SP 800-171 revision process as an opportunity to streamline the confusing and competing patchwork of third-party cybersecurity guidance that currently exists.

Thank you for your consideration of our comments. We hope that ITI can serve as a resource to NIST as it undergoes the process to revise SP 800-171. If you have any questions or would like to discuss our comments in greater depth, please don't hesitate to reach out to Kelsey Kober, Senior Manager of Policy, Public Sector, at [redacted] or [redacted].

Respectfully submitted,



Gordon Bitko
Senior Vice President of Policy, Public Sector
Information Technology Industry Council (ITI)