



July 14, 2023

Dr. Ronald S. Ross
Ms. Victoria Yan Pillitteri
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland 20899

Re: PSC Comments on NIST SP 800-171, Rev. 3 (Draft)

Dear Dr. Ross and Ms. Pillitteri:

On behalf of the Professional Services Council (PSC), I am pleased to submit comments on the **Draft NIST SP 800-171 Rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations***¹, published by the National Institute of Standards and Technology on May 10, 2023. This update reflects significant efforts in data collection, technical analyses, customer interaction, redesign, and development of the security requirements and supporting information for the protection of Controlled Unclassified Information (CUI) and appears to seek improved alignment between widely applicable NIST standard publications (specifically, 800-53 and 800-171). Per statute and regulation, this publication must remain current with “state of the art” safeguards and countermeasures for security standards and guidelines.

As you may know, PSC is an industry association with more than 400 member companies—small, mid-sized, and large—that provide much-needed technology and professional services to all federal agencies. These companies and their workers throughout America and around the world are equally as committed to U.S. Government missions as federal civilian and uniformed personnel. PSC supports our members and their federal customers by promoting effective government practices and policies, improvements in federal contracting, and constructive dialogue between Government and industry. This includes considerable collaboration with, and feedback to, federal agencies that tackle cybersecurity, CUI, and other technology-based issue sets.

PSC appreciates the opportunity to provide comments on NIST SP 800-171 Rev. 3 (Draft), applauds NIST’s rationale underpinning the revision, and agrees that aligning standards and requirements in the complex, dynamic area of cybersecurity are vital for both national security and for consistent adoption and application of such standards and requirements across the industrial base. With that in mind, PSC also notes that NIST can improve several areas of the draft publication by considering, and incorporating as appropriate, industry feedback. Specifically, PSC’s comments address the following issues:

- I. Re-categorized controls (e.g., controls formerly categorized as NFO)**
- II. Inclusion of organization-defined parameters (ODP)**
- III. Prototype CUI overlay**

¹ <https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/draft>

PSC and member companies reviewed the NIST-provided change analysis between Revision 2 and Revision 3, Frequently Asked Questions, and CUI overlay and considered the stated objectives of the changes with a particular focus on these three areas. This letter also includes additional comments, perspective, and recommendations that would support a holistic, effective implementation of the draft Special Publication.

NOTE: As PSC's more than 400 member companies support the depth and breadth of the federal government, PSC's response will not include specific commentary on individual controls, other than as exemplars to represent an overarching concern. Specific controls highlighted are not inclusive of all instances.

I. Re-categorized controls (e.g., controls formerly categorized as NFO)

Discussion: Overall, PSC members see value in SP 800-171's flexibility that allows organizations to tailor requirements to individual networks and the data for which they are responsible. With a flexible and risk-based approach, organizations can consider unique circumstances, including but not limited to operations, customer base, known threats, and risk tolerances. Any changes to SP 800-171 that would limit flexibilities and/or mandate an overly prescriptive approach would likely have negative impacts on costs and competition; increased costs could outpace any short-term benefits and innovators and market disruptors could choose to leave the federal market, while prescriptive requirements would quickly become obsolete.

PSC Recommendations: With the above discussion in mind, NIST could improve elements of the draft Revision 3 to support small businesses, encourage/retain new market entrants, and retain competitive pressures and procurement innovation.

- ***NIST should account for small organizations and those that handle only small amounts of CUI, perhaps even specific to one effort or a small set of efforts.*** Flexibility is particularly important for small businesses because adoption of SP 800-171 requirements more widely than necessary across an organization would increase costs and potentially limit new entrants to the federal marketplace. Costs and administrative burdens, particularly for small businesses, could push them out of the market, which would decrease competition while increasing procurement costs to the government.
- For certain controls, changes in the draft Revision 3 result in more prescriptive requirements by directing ***how*** an organization must implement a requirement. For example, the revised publication would adopt a requirement to implement encryption at rest.² This requirement would remove options for alternative physical safeguards that were included in Revision 2.
- NIST also proposes a control 3.12.5, "Independent Assessment." Through the description, NIST implies employees of the organization would not qualify as impartial or independent assessors. ***NIST should revise the definition of an "independent assessment" such that an organization can define internal controls to support conduct of the assessments by***

² 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 Revision 2, 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.

in-house employees, as appropriate. Additionally, revising the definition in such a manner would improve alignment with the descriptions of an independent assessment included in NIST SP 800-53.

- The related proposed control 3.12.1 simply states the “Independent Assessment” must be “current.” Given the dynamic cybersecurity environment, “current” could be interpreted with varying periodicity based on an individual organization’s knowledge, risk tolerance, and expertise. Such variability could drive significant differences in implementation costs across the industrial base. *PSC recommends providing a frame of reference to the term “current” to level potential interpretation variability.*

II. Inclusion of organization-defined parameters (ODP)

Discussion: Introduction of organization-defined parameters (ODPs) may be a positive step, depending on how—and by whom—ODPs are defined and managed in execution. As currently written, ODPs are first defined by Federal agencies, then by the customer, then by the industry participant. If, in execution, NIST’s intention is for ODPs to be primarily defined and managed by industry participants based on the specific risk situation and business needs, NIST is acknowledging that there is no one-size-fits-all solution to information security. This flexibility is welcome and can help organizations better manage their unique risk.

However, if it is NIST’s intention that ODPs be primarily defined and managed by individual agencies and/or at the Government office/individual contract level, NIST should be careful to ensure that the introduction of ODPs is not used by individual agencies to impose prescriptive requirements or otherwise reduce organizational flexibility. If ODPs are to be defined on an individual agency, or contract by contract basis, an industry participant will be required to maintain and comply with any number of unique ODPs, potentially forcing a company to adopt the most restrictive (and likely most costly) controls, as the common denominator across all active requirements. More specifically, government customers individually defining unique ODPs on each RFI/RFP, contract by contract (or task order by task order) basis, will require unique solutions for each proposal/award (enclave versus enterprise solutions), resulting in an incalculable compliance burden on all industry participants. That level of variability between each solicitation and award will have an outsized—and likely deleterious effect—on small business entities through increased bid, proposal, and compliance costs, introduction of additional barriers to entry which will limit new entrants and has the potential to drive current participants out of the market due to the unpredictable nature of each requirement.

PSC Recommendation:

NIST should clarify the entity responsible for setting ODPs (Industry, Government, or both/situationally dependent).

- For those established by the Government, *NIST should encourage federal agencies to refrain from setting arbitrary or inflexible ODPs.*
- For those that are established at the Agency level, the ODPs should be consistent across activities and/or requirements to limit variability in execution. *NIST should instead primarily allow non-federal organizations to internally define ODPs as needed.*

III. Prototype CUI overlay

Discussion: The prototype CUI overlay helpfully explains how NIST tailored the requirements from the moderate baseline in SP 800-53 Rev. 5 to develop the requirements in the draft. This re-alignment goes a long way towards harmonizing SP 800-171 with other frameworks (e.g., FedRAMP) that map back to SP 800-53 and helps non-federal organizations understand how new security requirements were added, removed, or re-incorporated in the draft Revision 3.

PSC Recommendation: The prototype CUI overlay, which provides a detailed analysis of the tailoring decisions at the control item level between SP 800-53 and SP 800-171, is a new concept that could be beneficial. However, it is unclear how this overlay will be used in practice and how it will interact with the other changes introduced in the draft update. ***PSC recommends that NIST provide detailed guidance on use of the overlay in execution.***

Additional Considerations and Recommendations

While the NIST 800-171 Rev. 3 (Draft) represents progress toward improved protection of CUI, more work is needed to ensure that the guidelines are clear, implementable, and operational. Highlighted below are additional considerations and recommendations to improve the holistic application and implementation of the SP 800-171 Rev. 3:

- **Clear and consistent CUI Guidance**
 - NIST should help users understand the differences between SP 800-171 and other related NIST publications. Within NIST’s CUI series alone, there are substantial differences in applicable controls such as between CUI (outlined in SP 800-171) and CUI associated with a “critical program or high value asset” (outlined in SP 800-172). ***PSC recommends NIST provide additional guidance regarding when and where each publication may apply to help contractors identify and implement applicable requirements/standards.***
 - Recognizing that the National Archives and Records Administration (NARA) is the executive agent of CUI, NIST can still help provide clarity on important threshold issues. ***PSC recommends that NIST work closely with NARA, the Department of Defense (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.
- **Clarify Changes between Rev 2 and Rev 3:**
 - Given the substantial revisions to SP 800-171, including updates to security requirements and families to reflect updates in SP 800-53 Rev. 5, the SP 800-53B moderate control baseline, revised tailoring criteria, and increased specificity for the controls, ***PSC recommends that NIST clearly identify in a red-lined publication (i.e.,***

showing tracked changes) what has changed between Revision 2 and Revision 3. The NIST-provided change document references 27 “withdrawn” requirements; however, only five requirements were removed from the baseline. The other requirements were re-incorporated into existing controls. Supplementing the change analysis/overlay will provide much needed clarity among the changed documents. A red-line version that reflects changes to each control would help parties update their internal control policies and better respond to updates and changes in Revision 3.

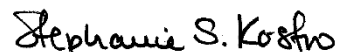
- **Application, alignment, and relation of 800-171 to associated requirements:**
 - *NIST should take additional steps to align SP 800-171 with other procurement-related cybersecurity guidance and, where practicable, release all updated documents as a suite.* A consistent, unified posture will aid NIST in developing clear guidance and expectations that can be consistently implemented by industry. Clear and consistent direction will allow for quicker and more widespread adoption of security practices. Duplicative, confusing, or contradictory recommendations could slow implementation.
 - For example, it is expected that the DoD Cybersecurity Maturity Model Certification (CMMC) 2.0 program will leverage SP 800-171 requirements. It is important for NIST to engage with DoD to promote alignment.
 - SP 800-171 uses the assessment procedures at SP 800-171A. NIST should seek to release an updated SP 800-171A coincident with any related updates for SP 800-171 Rev. 3 to avoid inconsistencies between the requirement and assessment documents. So too, SP 800-172 and 800-172A.
 - *NIST should also coordinate with DoD to provide clear guidance as to whether the new revision will apply to existing contracts and, if so, when the new revision will be implemented.* DFARS 252.204-7012 requires compliance with the version of SP 800-171 “in effect at the time the solicitation is issued or as authorized by the Contracting Officer.” Requiring immediate compliance with Revision 3 on outstanding proposals and/or existing contracts would likely create significant increased costs that were not anticipated when proposals were prepared and submitted.
 - The Federal Acquisition Regulation (FAR) Council is also expected to issue a proposed rule in FAR Case No. 2021-019 in the coming months. According to the FAR Council’s Open Cases Report, 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 engage with the FAR Council to promote alignment, if practical.*
- **Clarify flow-down obligations:**
 - A persistent issue for contractors is determining if information is CUI. Often, federal agencies impose requirements on contractors to safeguard CUI by incorporating SP 800-171 by reference into agreements with contractors and other entities with whom they share CUI. As Government contracting and subcontracting relationships are varied, there is uncertainty about whether and how prime contractors are expected to

ensure subcontractor compliance with SP 800-171. *NIST should provide additional clarity on what requirements apply at the prime and/or subcontractor level.*

As always, PSC and its member companies appreciate the opportunity to engage with NIST and the broader U.S. Government on key issues of great importance to federal agencies, its contracting partners, and the American people. Thank you for soliciting comments on the NIST SP 800-171 Rev. 3 (Draft). Through recommendations for industry engagement and areas for improvement, PSC seeks to continue our long tradition of robust, productive dialogue on issues of importance to technology and professional services contractors and their federal customers.

If you have questions or concerns about PSC comments, please contact Lauren Ayers, PSC Vice President for Defense and Intelligence, at ayers@pscouncil.org or (703) 875-8059.

Yours respectfully,



Stephanie S. Kostro
Executive Vice President for Policy