

**From:** [800-171comments@list.nist.gov](mailto:800-171comments@list.nist.gov) on behalf of [REDACTED]  
**To:** [800-171comments@list.nist.gov](mailto:800-171comments@list.nist.gov)  
**Subject:** [800-171 Comments] Comments on NIST SP 800-171r3 initial public draft  
**Date:** Friday, July 7, 2023 6:21:25 PM  
**Attachments:** [image001.png](#)  
[image002.png](#)  
[image003.png](#)  
[image004.png](#)  
[image005.png](#)  
[HITRUST Comments on NIST SP 800-171\\_r3 IPD Final.pdf](#)

---

Please see the attached comments for NIST SP 800-171r3

Thank you for the opportunity to submit.



**Tyler Henson**

Manager, Government Affairs

P: [REDACTED]

[REDACTED]



**CONFIDENTIALITY NOTICE:** The contents of this email message and any attachments are intended solely for the addressee(s) and may contain confidential and/or privileged information and/or may be subject to copyright or other intellectual property protection and be legally protected from disclosure. If you are not the intended recipient of this message or their agent, or if this message has been addressed to you in error, please immediately alert the sender by reply email and then delete this message and any attachments. If you are not the intended recipient, you are hereby notified that any use, dissemination, copying, or storage of this message or its attachments is strictly prohibited.

July 6, 2023

National Institute of Standards and Technology  
ATTN: Mr. Ron Ross  
Computer Security Division  
Information Technology Laboratory  
100 Bureau Drive, Mail Stop 2000  
Gaithersburg, MD 20899-2000

**RE: Call for Comments on Initial Public Draft: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations**

Dear Mr. Ross:

Thank you for the opportunity to review and comment on the Initial Public Draft (IPD) of NIST SP 800-53 revision 3 (r3),<sup>1</sup> *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

The following comments are submitted on behalf of HITRUST<sup>2</sup>, a globally recognized leader in information risk management and assurance reporting. Since it was founded in 2007, HITRUST has championed programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security, and risk management leaders from the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management frameworks as well as related assessment and assurance methodologies.

We first focus our comments on how NIST dealt with HITRUST's pre-draft comments<sup>3</sup> submitted in late 2022 and then provide very limited comments on the three topics of interest specified in the IPD. We subsequently forego use of the suggested comment template as our review does not extend to the level of detail it requires.

---

<sup>1</sup> Ross, R., and Pillitteri, V. (2023, May). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (NIST SP 800-171r3 ipd). Gaithersburg, MD: NIST. Available from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.ipd.pdf>.

<sup>2</sup> HITRUST (2023). *About HITRUST*. Available from <https://hitrustalliance.net/about-hitrust/>.

<sup>3</sup> Cline, B. (2022, Sep 13). [Letter from HITRUST to NIST re: Pre-Draft Call for Comments: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.] Available from [https://csrc.nist.gov/csrc/media/Projects/protecting-controlled-unclassified-information/Pre-Call-For-Comment-Sept-2022/CUIPreCall\\_HITRUSTAlliance\\_Sep13\\_2022.pdf](https://csrc.nist.gov/csrc/media/Projects/protecting-controlled-unclassified-information/Pre-Call-For-Comment-Sept-2022/CUIPreCall_HITRUSTAlliance_Sep13_2022.pdf).

## General Comments

HITRUST is pleased to see the previous structure and content of the requirements in NIST SP 800-171 r2 replaced with more streamlined guidance incorporating an enhanced overlay<sup>4</sup> of the NIST moderate impact baseline consistent with the tailoring guidance contained in NIST SP 800-53B.<sup>5</sup> By doing so, NIST addressed many of our previous concerns with the existing guidance, which included but is not necessarily limited to:

- Lack of consistency with NIST SP 800-53 resulting in many-to-many relationships between NIST SP 800-53 and NIST SP 800-171 controls
- Lack of a detailed mapping of these many-to-many relationships

As a result, the new guidance along with the new CUI overlay make the protection requirements easier to understand and more readily integrable by (1) organizations that use a NIST SP 800-53B control baseline or one of its existing overlays<sup>6</sup> in their existing cybersecurity programs and by (2) Standards Developing Organizations (SDOs) like HITRUST<sup>7</sup> that incorporate NIST SP 800-53 controls into their cybersecurity standards or otherwise map to them.

However, based on our reading of the IPD and related Frequently Asked Questions (FAQs),<sup>8</sup> it appears that NIST intends to:

- Maintain the NFO designation which tailors out requirements expected to be implemented by nonfederal organizations without specification
- Retain requirements intended to mitigate advanced persistent threats (APTs) in a separate document, NIST SP 800-172, rather than incorporate them into the CUI overlay.

HITRUST believes continued use of the NFO designation—even though the number of such controls have been reduced significantly due to their redesignation as NCO, FED, or CUI—will result in a continued lack of transparency with relying parties around the status of these controls.

Further, retaining specification of APT requirements in a separate document and ostensibly a separate overlay continues to add unnecessary complexity in the promulgation and implementation of CUI-related protection requirements. It would be better in HITRUST's opinion for APT-related requirements to be integrated into NIST SP 800-171 along with an additional tailoring criterion of APT. However, if NIST does issue separate APT guidance and (potentially) an associated overlay, an integrated overlay of the CUI and APT requirements could help mitigate the problem.

---

<sup>4</sup> NIST (2023). Enhanced Overlay. In NIST Glossary of Key Information Security Terms. Available from [https://csrc.nist.gov/glossary/term/enhanced\\_overlay](https://csrc.nist.gov/glossary/term/enhanced_overlay).

<sup>5</sup> Joint Task Force (2020, Oct). Control Baselines for Information Systems and Organizations (NIST SP 800-53B). Gaithersburg, MD: NIST. Available from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf>.

<sup>6</sup> For example, see FedRAMP (2023). FedRAMP Security Controls Baseline. Available from [https://www.fedramp.gov/assets/resources/documents/FedRAMP\\_Security\\_Controls\\_Baseline.xlsx](https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Controls_Baseline.xlsx).

<sup>7</sup> Cline, B. (2018). HITRUST as an Industry Standards Organization. Available from <https://hitrustalliance.net/documents/content/The-HITRUST-Industry-Standards-Organization.pdf>.

<sup>8</sup> NIST (2023, May 10). Initial Public Draft (IPD) NIST SP 800-171, Revision 3: Frequently Asked Questions. Available from <https://csrc.nist.gov/csrc/media/Publications/sp/800-171/rev-3/draft/documents/sp800-171r3-ipd-faq.pdf>.

## Specific Comments (Topics of Interest)

### 1. *Re-categorized controls (e.g., controls formerly categorized as NFO)*

HITRUST has no issue with the re-categorization of the controls other than retaining the NFO designation as previously discussed.

### 2. *Inclusion of organization-defined parameters (ODP)*

HITRUST has no issue with the addition of organization-defined parameters as this is consistent with the approach taken in NIST SP 800-53.

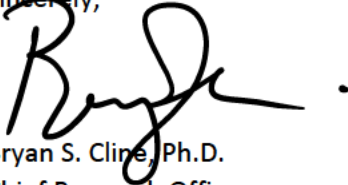
### 3. *Prototype CUI Overlay*

We applaud the addition of a CUI overlay of the NIST SP 800-53B moderate impact baseline as it solves several of the issues identified in our response to the pre-draft call for comments. We hope NIST will also consider our input above and include an APT overlay as a tailoring criterion should the NIST SP 800-172 controls be integrated into NIST SP 800-171 r3. As discussed earlier, an integrated CUI/APT overlay would also be helpful.

Despite these caveats, HITRUST would like to reiterate our belief that the new simplified IPD—especially considering the addition of a prototype CUI overlay of the NIST SP 800-53B moderate impact baseline—is vastly superior to current guidance as it greatly facilitates the integration of CUI protection requirements into organizational cybersecurity programs and external cybersecurity standards.

Thank you again for the opportunity to comment on the proposed changes to NIST guidance on the protection of CUI in the new IPD. We hope you find these comments useful. Please feel free to contact me at [REDACTED] should you have any questions or desire additional information related to our response.

Sincerely,



Bryan S. Cline, Ph.D.  
Chief Research Officer  
Office of Research & Analysis