[redacted]

From: Bryan Cline [redacted]
Date: Tuesday, September 13, 2022 at 1:11:01 PM UTC-4
Subject: HITRUST Response to the NIST SP 800-171 / CUI Series RFC
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>
Cc: Donna Steward [redacted]

Dear Mr. Ross,

Thank you for the opportunity to provide pre-draft comments on NIST's anticipated revision of the CUI series of documents. We hope you find them useful, and please feel free to contact me should you have any questions or desire additional information related to our response.

R,

Bryan

Bryan S. Cline, Ph.D.
Chief Research Officer (CRO)
P: [redacted]
E: [redacted]

HITRUST

6175 Main Street
Suite 400
Frisco, TX 75034

[redacted]
www.HITRUSTAlliance.net

September 13, 2022

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

Dear Mr. Ross:

Thank you for the opportunity to provide comments on/responses to your pre-draft call for comments on protecting Controlled Unclassified Information (CUI) in nonfederal systems and organizations with regard to the following set of four documents (herein after referred to as 'the CUI series') from NIST: SP 800-171 r2[1] and SP 800-172,[2] which contain security requirements that nonfederal systems or organizations that handle CUI are expected to implement, and SP 800-171a[3] and SP 800-172a,[4] which contain procedures for such systems and organizations to assess the performance of their implementation of the security requirements.

The following comments/responses are submitted on behalf of HITRUST,[5] 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.

---

[1] Ross, R., Pillitteri, V., Dempsey, K. (2020, February). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (NIST SP 800-171 Rev. 2). Gaithersburg, MD: NIST. Available from https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

[2] Ross, R., Pillitteri, V., Guissanie, G., Wagner, R., Graubart, R., Bodeau, D. (2020, February). *Enhanced Security Requirements for Protecting Controlled Unclassified Information*. (NIST SP 800-172). Gaithersburg, MD: NIST. Available from https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

[3] Ross, R., Pillitteri, V., Dempsey, K. (2020, February). *Assessing Security Requirements for Controlled Unclassified Information* (NIST SP 800-171a). Gaithersburg, MD: NIST. Available from https://csrc.nist.gov/publications/detail/sp/800-171a/final.

4 Ross, R., Pillitteri, V., Dempsey, K. (2020, March 15). *Assessing Enhanced Security Requirements for Controlled Unclassified Information* (NIST SP 800-172a). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172A.pdf.

[5] HITRUST (2022a). *About HITRUST*. Available from https://hitrustalliance.net/about-hitrust/.

HITRUST

6175 Main Street
Suite 400
Frisco, TX 75034

[redacted]
www.HITRUSTAlliance.net

Use of the CUI Series

1. How organizations are currently using the CUI series (SP 800-171, SP 800-171A, SP 800-172, and SP 800-172A).

While HITRUST cannot speak to how other organizations use the CUI series outside of the HITRUST community, we use NIST SP 800-171 as one of the authoritative sources in the HITRUST CSF™[6] to help HITRUST Organizations[7] that leverage the HITRUST Approach[8] assess the maturity of their information security and privacy protection programs and demonstrate compliance with security and privacy laws and regulations relevant to the sensitive information in their care. We also leverage NIST SP 800-171 and NIST SP 800-172 along with other relevant resources to help inform the selection of good security hygiene and best/leading practices in the HITRUST bC[9] and i1[10] Assessments, respectively.

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.).

As mentioned in the previous question, HITRUST uses the CUI series together with other standards and best practice frameworks to inform its selection of good hygiene and best/leading practices. We also integrated the CUI series into the HITRUST CSF when the first iteration of the DoD CMCC program was proposed and will update its requirements and related mappings to the HITRUST CSF as needed to support the program's final implementation. Our intent is to allow HITRUST External Assessor Organizations[11] that also become a CMMC Third Party Assessment Organization[12] for CMMC to assess and report on CMMC compliance based on a HITRUST CSF Assessment.[13]

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

It is clear from the tables in Appendix D[14] of NIST SP 800-171 and Appendix C[15] of NIST SP 800-172 that the CUI series' controls can be mapped to the controls in both NIST SP 800-53 and the International Standards Organization (ISO) and International Electrotechnical Commission (IEC) Standard 27001.[16] However, while the alignment of controls in NIST SP 800-171 and -172 to ISO/IEC 27001 is as one might expect when viewed through the lens of its many-to-many mappings, the same cannot be said for their

---

[6] HITRUST (2022b). *HITRUST CSF Framework*. Available from https://hitrustalliance.net/product-tool/hitrust-csf/.

[7] HITRUST (2021, Dec). *HITRUST Glossary of Terms and Acronyms*, Version 5.2. Frisco, TX: Author, p. 17. Available from https://hitrustalliance.net/content/uploads/Glossary-of-Terms-and-Acronyms_Ver-6.0.pdf.

[8] HITRUST (2020). *Key Considerations of a Data Protection, Information Risk Management, and Compliance Program*. Frisco, TX: Author.

[9] HITRUST (2022c). *HITRUST Basic, Current-state (bC) Assessment*. Available from https://hitrustalliance.net/hitrust-basic-current-state-bc-assessment/.

[10] HITRUST (2022d). *HITRUST Implemented, 1-Year (i1) Validated Assessment*. Available from https://hitrustalliance.net/certification/hitrust-implemented-1-year-i1-validated-assessment/.

[11] Office of the Under Secretary of Defense for Acquisition & Sustainment (2022). *CMMC: Assessments*. Available from https://www.acq.osd.mil/cmmc/faq.html.

[12] Joint Task Force, JTF (2020, Sep). *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53, Rev 5). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[13] HITRUST (2020, May). *How the HITRUST Approach can help organizations demonstrate compliance with and obtain certification under the DoD CMMC program*. Frisco, TX: Author.

[14] Ross, R., Pillitteri, V., Dempsey, K. (2020, February), pp. 61 - 83.

[15] Ross, R., Pillitteri, V., Guissanie, G., Wagner, R., Graubart, R., Bodeau, D. (2020, February), pp. 50 – 67.

[16] ISO (2013, Oct). *Information technology – Security techniques – Information security management systems – Requirements* (ISO/IEC 27001:2013). Geneva: Author. Available from https://www.iso.org/standard/54534.html.

relationship to NIST SP 800-53. Given NIST SP 800-171 and -172 are technically overlays[17] of the NIST SP 800-53B[18] moderate security control baseline, the mappings should be one-to-one or, at worst, many-to-one rather than many-to-many. For example, NIST SP 800-171 3.1.1 and 3.1.2 are both mapped to NIST SP 800-53 AC-2, AC-3 and AC-17.

We suggest NIST address this issue by reworking the tables in both documents to indicate which aspect of a CUI series control is addressed by the security controls in NIST SP 800-53 and ISO/IEC 27001 that are mapped to it. Alternatively, NIST could simplify the overlay(s) contained in NIST SP 800-171 and -172 as discussed in our response to Questions 5, 6 and 7.

4. Benefits of using the CUI series

In addition to the obvious benefit from using the CUI series, which is the understanding by organizations of the U.S. government's expectations for the protection of CUI and the subsequent ability to do business with government agencies, HITRUST is able to leverage the CUI series to help inform its selection of good security hygiene and best/leading practice controls and support third-party certification of an organization's implementation of the CUI series controls or a framework like CMMC that uses the CUI series controls as described previously in our response to Questions 1 and 2.

5. Challenges in using the CUI series

We see two major challenges in using the CUI series as it exists today:

- The difficulty in understanding how the security requirements in the CUI series are addressed by the security controls in either NIST SP 800-53 or ISO/IEC 27001, which may form the basis of an organization's overall security program or for the provision of assurances about the state of their program to other stakeholders and which may subsequently require more detailed, i.e., precise, mappings to NIST SP 800-171 and -172.

- The difficulty associated with the interpretation and consumption of two separate but related overlays of NIST SP 800-53 in the CUI series. NIST SP 800-171 focuses on confidentiality requirements (which often address integrity as well)[19] while NIST SP 800-172 addresses integrity and availability requirements but also includes advanced persistent threat (APT) requirements with all three security properties.

Updates for consistency with SP 800-53 Revision 5 and SP 800-53B

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

We believe the benefits of updating the CUI series for consistency with NIST SP 800-53 r5 and NIST SP 800-53B far outweigh any challenges to 'backward compatibility' if the update occurs before full implementation of the DoD CMMC program. However, even if such an update occurs after CMMC is implemented, any risk associated with an organization's transition to such a revised CUI series can be

---

[17] NIST (2022a). Overlay. In *NIST Glossary of Key Information Security Terms*. Available from https://csrc.nist.gov/glossary/term/overlay.

[18] Joint Task Force, JTF (2020, Oct). *Control Baselines for Information Systems and Organizations* (NIST SP 800-53B). Gaithersburg, MD: NIST, p. 67. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf.

[19] Ross, R., Pillitteri, V., Dempsey, K. (2020, February), p. vi.

mitigated by including a very detailed/precise mapping between the 'legacy' NIST SP 800-171 and -172 controls and the moderate security baseline in NIST SP 800-53B as recommended in our response to Question 3. Such a mapping would also support external mappings to other commonly used information protection frameworks such as the Center for Internet Security (CIS) Critical Security Controls[20] and regulatory requirements such as the HIPAA Security Rule.[21]

Updates to improve usability and implementation

7. Features of the CUI series should be changed, added, or removed. Changes, additions, and removals can cover a broad range of topics, from consistency with other frameworks and standards to rescoping criteria for inclusion of requirements. For example:

a. 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 security requirements.

Consistent with our response to Question 6, we also recommend updating the CUI-series with a single overlay of the NIST SP 800-53B moderate security baseline rather than the two ostensibly provided in NIST SP 800-171 and -172 today. A single overlay would be much less confusing for the user and more consistent with how other overlays have been developed using the tailoring guidance in NIST SP 800-53B. Examples of such overlays include the Federal Risk and Authorization Management Program (FedRAMP),[22] Internal Revenue Service (IRS) Publication (Pub) 1075,[23] Centers for Medicare and Medicaid Services (CMS) Acceptable Risk Safeguards[24] and Minimum Acceptable Risk Standards for Exchanges,[25] and the HITRUST CSF.

The specific security properties (confidentiality, integrity, and/or availability) addressed by a control could be indicated in tables similar to those provided in Appendix D of NIST SP 800-171 and Appendix C of NIST SP 800-172 along with other relevant information such as a mapping to other frameworks including ISO 27001 and the NIST Cybersecurity Framework, designation as an advance persistent threat (APT) control, and potential support for a penetration-resistant architecture (PRA), damage-limiting operations (DLO), and/or designing for cyber resiliency and survivability (CRS).

---

[20] CIS (2022). *CIS Critical Security Controls Version 8*. Available from https://www.cisecurity.org/controls/v8.

[21] Office of Civil Rights, OCR (2013, Mar 26). *HIPAA Administrative Simplification Regulation Text: 45 CFR Parts 160, 162, and 164*. Washington, DC: HHS. Available from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.

[22] FedRAMP (2022). *Baselines*. Available from https://www.fedramp.gov/baselines/.

[23] IRS (2021, Nov). *Tax Information Security Guidelines for Federal, State and Local Agencies* (IRS Publication 1075). Washington, DC: Author. Available from https://www.irs.gov/pub/irs-pdf/p1075.pdf.

[24] CMS (2017, Nov 21). *CMS Acceptable Risk Safeguards (ARS)*, Version 3.1. Washington, DC: Author. Available from https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/117_Systems_Security_MAC_ARS.pdf.

[25] CMS (2015, Nov 10). *MARS-E Document Suite 2.0 Volume II: Minimum Acceptable Risk Standards for Exchanges*, Version 2.0. Washington, DC: Author. Available from https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/2-MARS-E-v2-0-Minimum-Acceptable-Risk-Standards-for-Exchanges-11102015.pdf.

b. Change to the security requirement tailoring criteria: Impact of modifying the criteria used to tailor [2] 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).

Overlays developed from tailoring a control baseline should provide "a fully specified set of controls, control enhancements, and other supporting information,"[26] and the overlays provided by FedRAMP, CMS, the IRS, and others do so. However, NIST does not follow this practice with its CUI controls by tailoring out some controls and enhancements as NFO and FED, i.e., as being routinely satisfied without specification by nonfederal and federal organizations, respectively. We subsequently recommend NIST discontinue this practice in the next revision of the CUI series, as our experience with the assessment and certification of organizational information security and privacy programs over more than a decade has shown us there is no guarantee that organizations will implement a control without specification.

8. Any additional ways in which NIST could improve the CUI series

HITRUST has no further recommendations at this time.

Thank you again for the opportunity to provide pre-draft comments on NIST's planned revision to the CUI series of documents. We hope you find these comments useful—especially with respect to integrating NIST SP 800-171 and -172 into a single enhanced overlay.[27] 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

[26] JTF (2020, Oct), p. 67.

[27] NIST (2022b). *Enhanced Overlay*. In NIST Glossary of Key Information Security Terms. Available from https://csrc.nist.gov/glossary/term/enhanced_overlay.