[redacted]

From: Thomas Dover [redacted]
Date: Wednesday, July 20, 2022 at 12:02:36 PM UTC-4
Subject: Comments on CUI Series Publications
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>

Sir/Madam,

Reference is made to your email, dated 7/19/22, with subject heading *Protecting Controlled Unclassified Information: Pre-Draft Call for Comments on the CUI Series*.

Further reference is made to your request for information regarding the use of SP.800-171, 800-171A, 800-172 and 800-172A.

My comments will focus on the following areas:

- Use of the CUI Series

- Updates to improve usability and implementation

By way of background I presently work in the Healthcare sector in Information Technology (since 2014) where I serve as Sr. Information Security Specialist for a Healthcare Delivery Organization (HDO). Previously, I worked in the federal government (1988-2012) first in the Treasury Department and post-9/11 in the Department of Homeland Security. I served as both Special Agent and Supervisory Special Agent with the United States Secret Service. The majority of my assignments, duties and responsibilities dealt with technology ranging from investigations (digital forensics) to infrastructure protection (Critical Systems). I served as a 'Resident Affiliate' at Carnegie-Mellon University (from 2005 until retirement in 2012) and have taught Cybersecurity, Network Security, Physical Security and Business Continuity courses as an Adjunct at several community colleges (in western PA) since 2012. I have followed NIST guidance regarding Computer and Information Security for decades and have noted its explosive growth in this area post 9/11. I have found NIST guidance to be practical, applicable, vendor-neutral and capable of standing up to regulatory and legal scrutiny.

Now, on to my comments.

Use of the CUI Series

I have been using SP's 800-171r2, 172 & 172A since June, 2019. I did not include 800-171A because it is not referenced in 171r2. Specifically, 171A employs the assessment methods *Examine*, *Interview* & *Test*, however, these methods are not stated, cited or present in 171r2. Moreover, 171A was published in June, 2018 so I could only assume it was intended for 171r1 and/or 171 (see timeline below). *Examine*, *Interview* & *Test* are present in 172A—along with attributes *Depth* and *Coverage*—so my use of these assessment metrics began with 172 in April, 2021.

06/2015: 800-171 - Protecting CUI in Nonfederal Systems and Organizations
12/2016: 800-171r1 - Protecting CUI in Nonfederal Systems and Organizations
06/2018: 800-171A - Assessing Security Requirements for CUI
06/2019: 800-171r2 - Protecting CUI in Nonfederal Systems and Organizations
06/2019: 800-171B - Enhanced Security Requirements for Protecting CUI
02/2020: 800-171r2(rev) - Protecting CUI in Nonfederal Systems and Organizations
07/2020: 800-172 – Enhanced Security Requirements for Protecting CUI
04/2021: 800-172A – Assessing Enhanced Security Requirements for CUI

There are two central reasons why I use the CUI series:

1. Controlled Unclassified Information, by definition, could be equally applied to Protected Health Information (PHI) which by law and regulation (HIPAA\HITECH) requires both security and privacy protections relative to the Confidentiality, Integrity and Availability (CIA) of information.

2. SP.800-171r2 represented the first time that I read a NIST publication wherein requirements specific to the federal government were omitted--realizing, of course, that NIST, being a federal agency, directs its resources (correctly) to federal assets and systems. This exception, however, made it much easier (and extensively so) to parse and filter requirements applicable to the non-government sector (i.e., Healthcare).

Other reasons include:

1. The lack of discoverable methodology by third-party vendors contracted to perform security or risk assessments (as required by HIPAA).

2. The lack of quantifiable results of such assessments.

3. Referencing of NIST publications (most notably CSF and SP.800-53r5) by third-party vendors as part of their proprietary assessment methodology but without explanation of how or where NIST guidance was applied (or even used).

4. Lack of clear, concise results (excessive obfuscation and complexity)

5. Regulatory or legal review integrity

In effect, I wanted a relatively straightforward, consistent and repeatable security/risk assessment which met HIPAA requirements and whose methodology and results could be easily understood and explained; quantified and summarized; and completed easily. Quantifying results allow me to track and evaluate, over time, the level-of-compliance with NIST standards. Interestingly, at least in my case, such statistical evaluation has never been part of any commercial assessment process or methodology.

Using the Requirements outlined in 171r2 & 172, along with the assessment metrics in 172A, I created a simple Excel workbook suitable for Security\Risk assessment. I enhanced NIST guidance by adding several pieces of information either required by HIPAA or for internal (administrative) tracking. Among the variables added were a Compliance Value, Satisfying Statement, Validation Point\Tool and Security Control-Type. These variables allow me to assess the compliance of my company's security posture\footprint against NIST guidance and recommendations either specifically or comprehensively. In addition, quantifying the

assessment has allowed me to track compliance at both individual (control family) and aggregate levels. I perform an assessment every six months.

As mentioned earlier, I have taught Cybersecurity at the college level since 2012. NIST is one of the first resources I present to students and Security\Risk Assessment among the first topics. Since most academic texts are lacking in how to actually perform such assessments I utilize multiple NIST publications for this purpose.

In May, 2021, I was awarded a grant to create an Open Educational Resource (OER) specifically for Security/Risk Assessment using NIST publications. The book was published in December, 2021 and I used it in my Spring Semester, 2022 Cybersecurity class. It provides complete details as to my use of the CUI series and its attendant workbook assessment tool can downloaded as well. **Note:** in addition to the CUI series I incorporated SP.800-213 (*IoT Device Security for the Federal Government*) and SP.800-213A (*IoT Device Security for the Federal Government: IoT Device Cybersecurity Requirement Catalog*) in the book as these publications can be applied to Medical IoT (MIoT) in a way similar to the CUI series. Whereas the CUI series focuses on Information Technology (IT), SP.800-213 and 213A deal with Operation(al) Technology (OT) which is growing in use in the healthcare sector.

If interested, the book, titled *Using NIST for Security and Risk Assessment* can be found at the following URLs:

1. https://bc3.pressbooks.pub/tpd1811/ (Pressbooks format. Pressbooks in an online authoring and publishing tool. This was the OER grant award)

2. https://eng.libretexts.org/Courses/Butler_County_Community_College/Using_NIST_for_Security_and_Risk_Assessment (LibreText format. LibreText is a Department of Education\NSF grant project administered by UC Davis for OER development and resources).

In sum, I use the CUI series both professionally\operationally and as an educational tool.

Updates to Improve Usability and Implementation

I offer the following suggestions:

1. Merge SP.800-171r2 and SP.800-172 into a single publication but distinguish between 171r2's 110 base-security requirements and 172's 34 enhanced-security requirements.

2. Integrate SP.800-171A assessment methods into 171r2 for continuity.

3. Either integrate 172's Adversary Effects section into its control requirements (applicable as well to 171r2) or remove it. I was unable to determine its relationship to, or with, other aspects of 172. See Appendix B of the OER book for details.

Finally, I want to thank both you (NIST) and your partners\contributors for the dedication and effort you make in producing these publications. It is both recognized and appreciated.

Respectfully,

Thomas P. Dover
Practical Administrative Solutions/Grane Healthcare
Pittsburgh, PA