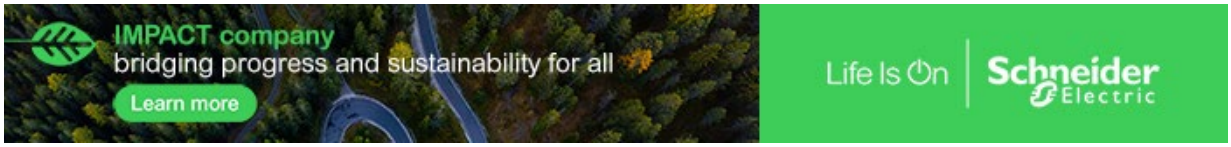
From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Schneider Electric - SP 800-171 Comments
Date: Friday, September 16, 2022 2:18:30 PM
Attachments: image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png
image009.png
Schneider Electric_SP 800-171 Comments.pdf

On behalf of Schneider Electric, I am pleased to share the attached comments in response to the pre-draft call for comments for NIST's planned update of the Controlled Unclassified Information (CUI) series of publications.

Best regards,

Sheila Casserly

Sheila Casserly
Director of Digital Policy, North America
Governance
Schneider Electric
M [redacted]
E [redacted]
Washington, D.C.
United States



[redacted]
24/7 support. Mobile catalog. Access to expert help.

Dr. Laurie Locascio
Under Secretary of Commerce for Standards and Technology and Director
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

September 16, 2022

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

Dear Dr. Locascio:

Schneider Electric strongly supports the National Institute of Standards and Technology (NIST) update of its resources on cybersecurity. As a partner to the US Federal Government, we actively leverage the NIST Controlled Unclassified Information (CUI) series of publications to assess controls for the protection of CUI and verify that our systems follow Federal data handling requirements.

At Schneider Electric, we drive digital transformation by integrating world-leading process and energy technologies, endpoint to cloud connecting products, controls, software, and services, across the entire lifecycle, enabling integrated company management. Our integrated solutions enable homes, commercial buildings, data centers, and critical infrastructure to operate more efficiently and securely.

The cybersecurity of our products and services is of vital importance to us and our customers. Our products and services are used in over one million buildings worldwide—including 40,000 water & wastewater treatment installations, 40% of the world's hospitals, over 10 of the world's top electric utilities, over 10 of the world's largest airports, and more.

Moreover, Schneider Electric actively partners with the US Federal Government in various cybersecurity initiatives, including as the first equipment manufacturer to participate in the US Department of Energy (DOE) Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program as well as through testing support for the US Department of Defense (DOD) More Situational Awareness for Industrial Control Systems (MOSAICS) program with the US Navy.

Below are selected examples of our engagement in the cybersecurity community:

- World Economic Forum Centre for Cybersecurity Partner
- Paris Call for Trust and Security in Cyberspace Supporter
- Cyber Tech Accord Signatory
- Cybersecurity Coalition Member
- ISA Global Cybersecurity Alliance Founding Member
- Electricity Information Sharing and Analysis Participating Vendor
- DOE CyTRICS program – first participating manufacturer to test products used in the US grid.
- Cybersecurity and Infrastructure Security Agency (CISA) Industrial Control Systems Joint Working Group (ICSJWG) – we hold multiple leadership positions in relevant working groups.

- Participate in numerous standards development organizations from the International Electrotechnical Commission (IEC) to the International Organization for Standardization (ISO) to craft relevant cybersecurity standards for our products and solutions.
- Schneider Electric, together with the ISA GCA, is working hand in hand with CISA and companies globally to utilize the proven Federal Emergency Management Agency (FEMA) Incident Command System for use in coordinating cyber incident responses. This effort is called the Incident Command System for Industrial Control Systems (ICS4ICS). This innovative framework helps cyber responders globally to identify, respond, and recover from cyber incidents using the same framework emergency responders in all other sectors use every day.

Our comments regarding Schneider Electric's current use of the CUI series and our suggestions for improvement are listed below:

- At Schneider Electric, we are active implementers of the NIST CUI series of publications.
- Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, is the foundational framework we use to verify our network systems and processes are aligned with Federal and DoD data handling requirements and to work towards achieving at least Level 2 compliance with the DoD Cybersecurity Maturity Model Certification (CMMC).
- We find SP 800-171 an excellent resource with controls that comprehensively cover CUI. In order to gather quantitative and qualitative data from within Schneider Electric on the use, effectiveness, challenges, and benefits of SP 800-171 and its compatibility with other frameworks and standards, we issued a survey to CUI series implementers within our company working most closely with SP 800-171.[1] Based on a rating on a 1-5 scale from four respondents, SP 800-171 scores 4.5 out of 5 on effectiveness and adequacy of the breadth of requirements to achieve the goal of safely handled CUI. These implementers note the success of SP 800-171 in establishing a standardized baseline of cyber protection for organizations processing important government information and providing specific controls and guidelines to ensure secure data systems.
- Moreover, CUI series implementers within Schneider Electric rate SP 800-171's alignment with NIST Risk Management Framework (SP 800-53) and CMMC highly—4.5 and 5 of out 5, respectively—noting how SP 800-171 effectively pulls controls from SP 800-53 and forms the basis for CMMC.
- However, challenges and shortcomings remain in SP 800-171 and its supporting publications that we hope will be addressed in the upcoming revision. Specifically, Schneider Electric recommends making the following improvements to the Series:

- ***Expand SP 800-171 to include OT.*** 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.
    - **Map ISA/IEC 62443 to SP 800-171** as a normative reference for cybersecurity for OT in automation and control systems. The ISA/IEC 62443 international series of standards is widely known and used within industry; NIST could alleviate compliance challenges while

[1] See Appendix for methodology of internal survey.

maintaining the highest standards of cybersecurity by mapping SP 800-171 to ISA/IEC 62443 and allowing Federal Government partners to provide ISA/IEC 62443- or NIST-aligned compliance attestations.

- ***Improve ease of implementation through tiered compliance and clear examples.*** CUI series implementers within Schneider Electric rate SP 800-171's ease of use 3.5 out of 5. While SP 800-171 provides a standardized and comprehensive way to protect CUI, the controls are difficult to implement on an enterprise-wide basis and in some cases would benefit from more narrow scope.
    - **Acknowledge partial compliance.** Achieving full compliance across organizations requires expensive, resource-intensive technical upgrades—regardless of the size of the organization and whether it is cloud-based SaaS (Software as a Service) or not. Currently, even if an organization implements the majority of sub-controls in a control family, the organization receives no credit for compliance with this control family as it pertains to the CMMC certification. We propose that NIST recommend to the DoD that short-term plans of actions and milestones (POAMs) continue to be allowed as a means of demonstrating compliance.
    - **Provide more guidance and examples on how to become 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 the appropriate scope. For example, is a broad, top-level SSP sufficient or do companies need to create an SSP for each individual system (e.g., laptops, servers, etc.)? In this case, strong examples of SSPs and instructional videos on how to draft an SSP would help organizations of all sizes set expectations and allocate resources efficiently.
- ***Facilitate understanding for a broader audience.*** Currently, SP 800-171 lacks alignment with the NIST Cybersecurity Framework, a widely known and adopted resource across a broad range of cybersecurity stakeholders. Although SP 800-171 has grown clearer with each revision, the fourteen control families encompassing hundreds of highly technical controls is still complicated to understand, especially for non-technical audiences.
    - **Drive alignment between SP 800-171 and the NIST Cybersecurity Framework**. CUI series implementers within Schneider Electric rate SP 800-171's alignment with the Cybersecurity Framework 1.5 out of 5 and indicate that there is little to no inherent alignment between these two resources. 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.
    - **Target different audiences with different publications.** 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.

Schneider Electric appreciates this opportunity to submit comments. If you have any questions or need additional information, please contact me at [redacted]

Sincerely,

Patrick M. Ford

Patrick M. Ford
Chief Information Security Officer, Americas Region
Schneider Electric

Appendix: Internal Survey Methodology

To gather quantitative and qualitative data from within Schneider Electric on the use, effectiveness, challenges, and benefits of SP 800-171, and its compatibility with other frameworks and standards, we issued a survey to CUI series implementers within our company working most closely with SP 800-171. The results of this survey are discussed throughout this document.

NIST SP 800-171 Internal Survey Questions

1. In key words or phrases, how do you use SP 800-171?

2. How easy to use is SP 800-171?

   Not easy to use (1) (2) (3) (4) (5) Very easy to use

3. How effective are SP 800-171 requirements at achieving the goal of safely handled CUI?

   Not effective (1) (2) (3) (4) (5) Very effective

4. How adequate is the breadth of requirements in SP 800-171 to achieve the goal of safely handled CUI?

   Inadequate (1) (2) (3) (4) (5) Adequate

5. In key words or phrases, what are the benefits of using SP 800-171?

6. In key words or phrases, what are the challenges of using SP 800-171?

7. How well does SP 800-171 align with the following frameworks and standards?

   Poorly aligned (1) (2) (3) (4) (5) Very well aligned

   a. NIST Risk Management Framework (SP 800-53)
   b. NIST Cybersecurity Framework
   c. General Services Administration (GSA) Federal Risk and Authorization Management Program (FedRAMP)
   d. DOD Cybersecurity Maturity Model Certification (CMMC)

8. Do you have any other comments, critiques, or observations to share on SP 800-171?