From:	800-171comments@list.nist.gov on behalf of [redacted]
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] Draft NIST Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (Draft SP 800-171 Rev.3)
Date:	Friday, July 14, 2023 3:00:51 PM
Attachments:	image001.png KP Comments NIST SP 800-171 R3 FINAL.pdf

---

RE: *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (Draft SP 800-171 Rev.3)*

Kaiser Permanente appreciates the opportunity to offer comments on the above-captioned request for comment. Our comment letter is attached, if you have questions please contact us at [redacted]

Thank you,

Megan Lane
Counsel, Government Relations
She/her/hers
[redacted]

Assistant:
[redacted]

KAISER PERMANENTE®

Kaiser Foundation Health Plan
Program Offices

July 14, 2023

RE: *NIST Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (Draft SP 800-171 Rev.3)*

Submitted via email to: 800-171comments@list.nist.gov

Kaiser Permanente (KP) appreciates the opportunity to offer feedback on the above-captioned request for comments (RFC).[1] The Kaiser Permanente Medical Care Program is the largest private integrated health care delivery system in the U.S., delivering health care to over 12 million members in eight states and the District of Columbia[2] and is committed to providing the highest quality health care.

The protection of Controlled Unclassified Information (CUI) in nonfederal systems and organizations is critical to the ability of the federal government to successfully conduct its essential functions. As a health care organization that partners with the federal government to serve Medicaid and Medicare patients and enrollees, Kaiser Permanente has a responsibility to protect data from security threats and breaches. We appreciate NIST's efforts to update SP 800-171 to help organizations better understand how to implement specific cybersecurity safeguards in SP 800-53 Rev. 5[3] and offer the following comments.

SP 800-171 Revision 3 ("Revision 3") is a significant improvement and welcome update from SP 800-171 Revision 2. It is technically oriented towards assisting organizations adopt specific security controls aligned with other NIST Special Publications (e.g., SP 800-53, SP 800-63) in order to comply with CUI protection requirements. Revision 3 eliminates confusion caused by the basic and derived security requirement labels and is written in a way that is simpler and easier to understand. Revision 3 improves and simplifies the requirements for multi-factor authentication (MFA) in requirement 3.5.3. We caution that these simplified requirements should be appropriately aligned with the corresponding assessment objectives in SP 800-171A[4] to ensure that the requirements, including any prerequisites, are fully captured. For example, we recommend retaining the current assessment objective 3.5.3(a) in the next revision to SP 800-171A because it is important to leverage a comprehensive and current list of all privileged accounts for all components to meet this requirement even though privileged accounts are not mentioned in requirement 3.5.3 in SP 800-171 Revision 3.

We support the new re-categorized controls and organization-defined parameters (ODPs). We recommend NIST provide further guidance, where feasible, on ODP usage to assist organizations in implementing SP 800-171. For example, we recommend that the guidance specify the expected minimum and maximum values for ODPs that define the expected frequency of certain activities such as vulnerability scans every year or revisions to procedures every two years. We also recommend that the guidance specify the criteria for when ODP would apply and the process for developing and agreeing to the various ODP.

---

[1] SP 800-171 Rev. 3 (Draft), Protecting CUI in Nonfederal Systems and Organizations | CSRC (nist.gov)

[2] Kaiser Permanente comprises Kaiser Foundation Health Plan, Inc. and its health plan subsidiaries outside California and Hawaii; the not-for-profit Kaiser Foundation Hospitals, which operates 39 hospitals and over 720 other clinical facilities; and the Permanente Medical Groups, self-governed physician group practices that exclusively contract with Kaiser Foundation Health Plan and its health plan subsidiaries to meet the health needs of Kaiser Permanente's members.

[3] https://csrc nist.gov/publications/detail/sp/800-53/rev-5/final

[4] https://csrc nist.gov/publications/detail/sp/800-171a/final

We also recommend that the discussion on the prototype CUI overlay be extended to address common CUI use causes that address Health and Privacy information.

Lastly, we recommend that NIST revise section 3 to explicitly address all three important aspects of confidentiality, integrity and availability (CIA), for both systems and data. However, if NIST chooses to focus on protecting the confidentiality of CUI in accordance with the directives issue in E.O. 13526 and 32 C.F.R 2002, we recommend that footnote 7 be moved into the text of the document to explain how the security of objectives of confidentiality and integrity are closely related because this important explanation could be missed in a footnote.

* * *

We applaud NIST for this valuable and thoughtful work. Please feel free to contact Jamie Ferguson [redacted] or Megan Lane [redacted] with any questions or concerns.

Sincerely,

Jamie Ferguson
Vice President, Health IT Strategy and Policy
Kaiser Foundation Health Plan, Inc.