**From:** 800-171comments@list.nist.gov on behalf of [redacted]
**To:** 800-171comments@list.nist.gov
**Cc:** [redacted]
**Subject:** [800-171 Comments] Comments from University of Illinois re: NIST SP 800-171
**Date:** Friday, July 14, 2023 3:17:57 PM
**Attachments:** image001.png
NIST sp800-171r3-comment-UIUC-template (1).xlsx

---

Colleagues,

Thank you for the opportunity to provide our input and comments to the NIST SP 800-171 security requirements, control sets, ODPs and CUI overlay. The work of NIST in these revisions along with the opportunity to receive comments is greatly appreciated by our community.

Generally, we see the creation of organization defined policy (ODP) as an opportunity to also consider the unique culture, organizational structure, and federation of complex enterprises such as higher education. We look forward to expansion of these types of ODPs, as well as possibly overlays that could be used by higher education to balance and meet strong cybersecurity and data protection objectives while having flexibility that acknowledges the unique nature of higher education.

We additionally offer some specific considerations to incorporate or expand the systems focus of 800-171 to incorporate a data and privacy focus approach.

Thank you for the opportunity to comment. Again, we recognize and are grateful for your and the entire community's work on these revisions, and the opportunity to provide input.

If you have any questions at any time, please do not hesitate to contact us.

Phil

Phil Reiter, MS MIS
Associate Director, Privacy
Office of the CIO Technology Services Privacy and Security
Adjunct Lecturer, iSchool
University of Illinois at Urbana-Champaign
[redacted]
[redacted]

ILLINOIS

| Comment # | Submitted By (Name/Org):* | Type (General / Editorial / Technical) | Source (publication, analysis, overlay) | Starting Page # * | Starting Line #* | Comment (include rationale)* | Suggested Change* |
|---|---|---|---|---|---|---|---|
| | University of Illinois | General | NIST SP800-171r3 ipd | ii | 2 | Consider including principle investigators and/or researchers as an audience for higher education contracts/partnerships. PIs traditional are part of the shared responsibility model and the document should reflect their role. | After the second bullet, add Higher Education "Principle Investigators" and/or subcontractors with research responsibilities for security, confidentiality and data protection. |
| | University of Illinois | General | NIST SP800-171r3 ipd | 1 | | Include a section indicating that CUI/ sensitive data may not be use to train public artificial intelligence or generative AI models, language learning models, et al. | "CUI/ sensitive data may not be use to train public artificial intelligence or generative AI models, language learning models" |
| | University of Illinois | General | NIST SP800-171r3 ipd | 1 | | Define parameters for the use of AI in securely, privately, and appropriately processing data collected, stored, or used in the course of a CUI-involved program. | Define the borders, boundaries, limits on unanticipated sharing of data, contractual and third party aspects of limiting access to CUI. |
| | University of Illinois | General | NIST SP800-171r3 ipd | 1 | | Consider a privacy control overlay to the template with a data-centric focus on the CUI data lifecycle | |
| | University of Illinois | General | NIST SP800-171r3 ipd | 1 | 524 | Require generalized and CUI specific privacy training as part of 800-171 | Extend/Include controls to require generalized privacy training on an annual or periodic basis as an ODP for access to CUI information, aligned with existing security training |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 5 | 116 | Specify account and data access management related to the authorization to access the level/type of data, e.g. CUI | "d... and authorized access to data hosted on system" |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 6 | 184 | Define the use of data management technologies/tools to appropriately tag, control data flows | "Organizations may use data management technologies to align CUI content to NIST controls and frameworks, policy, and to control the flow of information to only authorized personnel." |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 9 | 292 | Consider a soft lockdown option after unsuccessful attempts of allowing access to some resources but restricting access to data and/or CUI/ protected data | "Organizations should consider temporary restrictions to CUI data when a threshold of unsuccessful logon attempts is reached until reviewed by authorized personnel and validated." |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 9 | 274 | Incorporate controls that consider least privilege within virtualized environments that have administrative access on the host. This may be an issue for enterprises, including higher education, where this practice may still exist. Block access to data and lateral movement when unexpected privileged functions are executed in an environment containing sensitive/CUI data. | |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 12 | 443 | Include disabling of unnecessary software | "... and disabling unnecessary hardware and/or software, especially FARS prohibited software or malicious software." |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 12 | 447; 432 - 434 | In addition to these technical access controls, a link to training and awareness of how individual third party software can place security at risk may be appropriate. Noting that digital access/action is needed (usability) in addition to physical action to protect and control devices/ | "Controls supporting clear taining and awareness on the use of secure devices and understanding of the risks third-party applications may pose to CUI security is required" |
| | University of Illinois | General | NIST SP800-171r3 ipd | 15 | 524 | Specify training for data privacy and confidentiality | The training and awareness content has a strong systems security vs. data focus. Increase the focus on data protection in the construction and requirements. |

| Comment # | Submitted By (Name/Org):* | Type (General / Editorial / Technical) | Source (publication, analysis, overlay) | Starting Page # * | Starting Line #* | Comment (include rationale)* | Suggested Change* |
|---|---|---|---|---|---|---|---|
| | University of Illinois | General | NIST SP800-171r3 ipd | 16 | 577 | Include threats related to travel, especially internationally | Many researchers and administrators have both CUI and nonCUI related responsibilities that can require travel and interational travel. Advanced training and awareness in this area is important. |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 26 | 958 | Information location and data flows may be complex and not often fully understood, even to the advanced admin, in modern systems | Consider controls that employ data management capabilities to automate and manage. |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 37 | 1399 | Cryptographic protections have shelf lives and may not be sufficient alone in protecting backups as a control | Include / tie to full destruction of backups/physical media as appropriate and periodically audit/assess if backups that are retained for longer time/cold storage are protected with current encryption standards or require updates. |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 38 | 1425 | Access to only systems is defined, while access to data is as critical and may be distributed | Include explicit language about the removal of individuals access to **data** in addition to systems. Even in controlled environments, in today's ecosystem, access to data may be disparate and not fully controlled by role or Identity governance |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 42 | 1576 | Risk assessment needs to explicitly define third party / cloud hosted providers and privacy impact assessments as examples | Include / explicitly define controls or provide examples related to cloud hosted vendors, third party risk management (in alignment with supply chain risk) and contractual and other data and privacy impact assessments as inputs to risk assessment for unauthorized disclosure ... for CUI. |
| | University of Illinois | General | NIST SP800-171r3 ipd | 45 | 1681 | POAMs may vary widely and update frequency and action may create vulnerability or unmitigated risk. Models and approaches vary by organization; organization defined plan is positive addition. | Consider defining standards or having scope/institution based models for POAM lifecycle |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 46 | 1716 | Controls may not reflect maturity of CMMC/CUI rollouts | Define controls that provide independent assessment reporting lines and obligations for assessors regardless of internal or third party assessment, similar to data protection officers or auditors. |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 49 | 1867 | Controls do not consider mechanisms such as homomorphic encryption | Include controls that consider parallel processing and distributed processing (in the context of transmission and storage for this control) using homomorphic encryption |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 50 | 1902 | Current controls do not include quantum resistant controls | Consider the Kyber or other implementable controls for key generation, et al, with current availability on market. |
| | University of Illinois | Technical | NIST SP800-171r3 ipd | 51 | 1915 | Consider including quantum-resistant cryptography controls for CUI-specific sensitive information | Refer to recent NIST quantum-resistant cryptographic systems for such controls |
| | University of Illinois | General | NIST SP800-171r3 ipd | 52 | 1972 | Explicitly address newer software defined networks and control channels, as well as third party software to manage networks | Incorporate controls detailing limiting and protecting network comms and control traffic, metadata and profiles with third parties. Consider impacts of new AI/ML tools and / or third party monitoring. |

| Comment # | Submitted By (Name/Org):* | Type (General / Editorial / Technical) | Source (publication, analysis, overlay) | Starting Page # * | Starting Line #* | Comment (include rationale)* | Suggested Change* |
|---|---|---|---|---|---|---|---|
| | University of Illinois | General | NIST SP800-171r3 ipd | 54 | 2028 | Emphasize establishing baseline code revisions explicitly | In addition to describing malicious code prevention capabilities, emphasize the importance of code baseline/reference models to compare against for malicious code. |
| | University of Illinois | Editorial | NIST SP800-171r3 ipd | 56 | 2127 | Move Policy & Procedures section earlier in document | Consider a technical - administrative model and align Policy & Procedure and Training and awareness controls and editing the document for clarity, and including earlier. Consider "Blockchain" and modern approaches to authenticate and validate. |
| | University of Illinois | General | NIST SP800-171r3 ipd | 57 | 2177 | Include and/or overlay Privacy Engineering principles | While noting that the privacy risk framework and other NIST controls related to privacy are not part of this control set, there is an opportunity here to incorporate foundational privacy engineering controls (anonymization, privacy enhancing technologies, data managment and lifecycle, data loss prevention, and other controls, or link to such. |
| | University of Illinois | General | NIST SP800-171r3 ipd | 59 | 2252 | Supply chain & procurement visibility requirements (sunshine laws, State procurement rules) may conflict with CUI and confidentiality requirements, particularly for sensitive research | Include controls that require appropriate confidentiality for such research |