From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] EDUCAUSE Comments--NIST SP 800-171, Rev. 3 (Draft)
Date: Friday, July 14, 2023 1:46:55 PM
Attachments: NIST Draft 800-171r3 comments--EDUCAUSE 07-23 f.pdf
sp800-171r3-ipd-comment EDUCAUSE 07-23.xlsx

Please see attached for a cover letter and comments from EDUCAUSE (educause.edu) regarding the initial public draft of NIST SP 800-171, Rev. 3. On behalf of our members, EDUCAUSE thanks NIST for the opportunity to contribute to this important process. – Jarret Cummings

Jarret S. Cummings (he / him / his)
Senior Advisor, Policy and Government Relations

EDUCAUSE
Uncommon Thinking for the Common Good
[redacted] | educause.edu

EDUCAUSE

July 14, 2023

Ron Ross
NIST Fellow, Computer Security
National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930

Victoria Pillitteri
Group Leader (Acting), Security Engineering and
Risk Management Group
National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930

RE: Comments concerning NIST SP 800-171, Revision 3 (Draft)—response submitted to 800-171comments@list.nist.gov

Dear Dr. Ross and Ms. Pillitteri,

On behalf of EDUCAUSE, I would like to thank you for the opportunity to provide input from our cybersecurity community on the draft NIST Special Publication 800-171, Revision 3 (NIST SP 800-171, Rev. 3). The email with which this letter was submitted includes the comments of our community, which are provided via the spreadsheet form made available for that purpose. As the association for advancing higher education through information technology (IT), EDUCAUSE represents over 2,100 colleges, universities, and related organizations. Higher education chief information officers (CIOs), chief information security officers (CISOs), and IT leaders and professionals at all levels of the institution work together through EDUCAUSE to advance the state of cybersecurity in higher education.

I would particularly like to highlight the points raised in our comments regarding organization-defined parameters (ODPs). The introduction of ODPs into 800-171 via the current revision raises the likelihood that the nonfederal organizations subject to 800-171 compliance will face a diverse array of overlapping and potentially conflicting mandates as various federal agencies implement ODPs. Without a common framework to guide the formation and deployment of

[redacted]

ODPs, all of the stakeholders in the 800-171 requirements—agencies and nonfederal entities alike—could soon find themselves back in a world where non-uniform controlled unclassified information (CUI) requirements make tracking and complying with such requirements across agencies a frustratingly difficult and expensive task, which is something that higher education institutions, researchers, and staffs can ill-afford. The potential operational and financial costs stemming from this situation would be further exacerbated if the various agencies do not identify ODPs in requests-for-proposals as a common practice, but rather introduce them during grant award negotiations.

EDUCAUSE believes that NIST can and should take advantage of the opportunity to help federal agencies and their CUI stakeholders by providing a common framework for agencies to consider in developing and applying ODPs, which would align with the Executive Order 13556 requirement for establishing consistent policies and procedures for safeguarding CUI. This would provide all parties with a common frame of reference for how ODPs might be deployed and in what form while preserving agency discretion to craft ODPs that meet the unique provisions of law, regulation, or government policy that give rise to CUI in a particular context. Just the process of engaging agencies and stakeholders in developing such a framework could foster an ongoing dialogue across the 800-171 community about how best to reach and maintain a balance between the uniform approach to CUI security that 800-171 is intended to achieve and the tailoring of requirements that may be necessary in some cases given the specific provisions to which agencies must respond.

We suggest that a NIST Internal/Interagency Report (NISTIR) could serve as an effective vehicle for identifying guiding principles and key considerations that agencies should take into account in assessing and, when necessary, addressing the need for an ODP. In raising this idea, we acknowledge that Federal Information Processing Standards (FIPS) Publication 200 exists with the goal of providing some basis for consistency among federal agencies in relation to measures like ODPs. However, our members do not consider the guidance provided by FIPS 200 to be sufficiently concrete to address the potential problems with ODPs that are likely to arise in nonfederal contexts. Thus, we think a compelling case remains for the production of a NISTIR to provide additional guidance for federal agencies regarding the development and deployment of ODPs in relation to 800-171 implementation. EDUCAUSE and its members would be happy to work with you to explore what might be possible in this space via whatever approach you think would be most appropriate. Please feel free to contact me at your convenience regarding the potential for such an opportunity, or if EDUCAUSE and its members might be otherwise helpful to the 800-171 revision process.

Sincerely,

Jarret S. Cummings

Jarret S. Cummings
Senior Advisor, Policy and
Government Relations
EDUCAUSE
[redacted]

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	EDUCAUSE	Technical	800-171r3 ipd	2	30	The existing scoping language is overly broad, resulting in all requirements applying to any component providing security functionality (such as log servers, configuration management databases, NTP servers) without regard to whether the component could affect the confidentiality of CUI.	Change "The security requirements in this publication are only applicable to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components" to "The security requirements in this publication are only applicable to components of non-federal systems that process, store, or transmit CUI. Components that provide security functionality should be reviewed for their ability to affect the confidentiality of CUI and relevant controls should be applied to those security protection assets."
2	EDUCAUSE	General	800-171r3 ipd	4	79	The organization-defined parameters (ODPs) that federal agencies produce may not be universally or even generally appropriate for non-federal organizations. As a result, a lack of guidelines for federal agencies on the development and application of ODPs, including conditions under which exceptions and alternative controls should generally be allowed, risks imposing on nonfederal entities conflicting terms and requirements from different agencies. The potential for agencies to diverge on whether they identify ODPs in requests-for-proposal or during grant award negotiations, where the latter course presents an array of problems, heightens these concerns. Possible developments such as these hold the potential to greatly complicate security operations, increase associated administrative/operational costs, and produce sub-optimal security outcomes.	NIST should develop an “internal/ interagency report” (NISTIR) that details common principles and guidelines for federal agencies to consider in the development/deployment of ODPs as part of following and extending the requirements of 800-171 to nonfederal entities. SP 800-171 itself should then specifically refer federal agencies to the IR in question as recommended guidance on the development and application of ODPs in relation to securing CUI. This proposal would align with the Executive Order 13556 requirement for establishing consistent policies and procedures for safeguarding CUI.
3	EDUCAUSE	Technical	800-171r3 ipd	5	127	The term "expired accounts" is not defined in 800-171/800-53 or the Computer Security Resource Center (CSRC) Glossary.	Define "expired accounts" in an appropriate location.
4	EDUCAUSE	Editorial	800-171r3 ipd	10	314	The reference to the term “Office of General Counsel” is problematic given that the legal function is not necessarily identified in the same way across all affected organizations. (For example, some higher education institutions may rely solely on outside counsel while still having to follow the 800-171 guidelines per the U.S. Department of Education.) On the other hand, capitalization of the term in the document may lead some institutions to think that it refers to a federal government entity rather than the institution’s legal function (however that may be organized).	Replace the reference to "Office of General Counsel" with text that better aligns with how NIST SP 800-53 addresses the issue "Organizations should consult with their privacy office or officer, if applicable, for input regarding privacy messaging, and with their Office of the General Counsel or organizational equivalent for legal review and approval of warning banner content (as well as for input on privacy messaging if the organization does not have a privacy office or officer)."
5	EDUCAUSE	Technical	800-171r3 ipd	12	419	It is not clear what the definition of "organization-controlled mobile devices" should be. What level of control does an organization have to exert for a device to be considered "organization-controlled?" For example, in higher education research settings, where bring-your-own-device practices for graduate students, research assistants, and even faculty are fairly standard, substituting fully "locked-down" institutionally owned devices for personal devices would be prohibitively expensive and not necessary if the institution deploys reasonable alternative device management measures.	Define "organization-controlled" in an appropriate location, or use the term "organization-managed" instead.
6	EDUCAUSE	Technical	800-171r3 ipd	15	512	If 3.1.10 (Device Lock) and 3.1.11 (Session Termination) are in place, what is the purpose of 3.1.23? If it is to ensure that patches are being applied, then 3.14.1 covers the issue. There is no need to explicitly log users out of a system when sessions are terminated automatically.	Provide additional explanation for the distinction between 3.1.23 and 3.1.10, including examples that illustrate the different issues in question. If a clear, significant distinction cannot be established, consider removing 3.1.23 as unnecessary.
7	EDUCAUSE	Editorial	800-171r3 ipd	15	519	Requirement 3.1.10 does not address automatic enforcement of inactivity logout; it enforces locking a device, which is not the same as logging out (see the discussion for 3.1.10 at line 332, which notes the following "Device locks are not an acceptable substitute for logging out of the system.")	Remove the reference to 3.1.10. The closest control that addresses automatic enforcement of inactivity logout is 3.1.11 (Session Termination).
8	EDUCAUSE	Editorial	800-171r3 ipd	16	563	The term "system developers" is listed twice in the list of example roles.	Remove one reference to "system developers" (line 563 or 564).
9	EDUCAUSE	Technical	800-171r3 ipd	16	577	The rationale for separating 3.2.3 from 3.2.1 or 3.2.2 is not clear. As an enhancement under AT-2 in 800-53, it is more logical to incorporate 3.2.3 into 3.2.1.	Requirement 3.2.3 should be a sub-point under either 3.2.1 or 3.2.2, although we recommend making it a sub-point under 3.2.1.
10	EDUCAUSE	Technical	800-171r3 ipd	19	705	Between 3.3.6, 3.3.3, and 3.3.1, the identified ODPs do not allow organizations to manage their audit record storage space. Requirement 3.3.6 mandates that organizations preserve the original content and time ordering of audit records. One purpose of audit record reduction is to decrease the storage space required for maintaining audit logs. When combined with an ODP such as the one raised in 3.3.3, this preservation requirement could become prohibitively expensive.	Remove one of the ODPs and allow the nonfederal organization the discretion to decide some combination of what to audit (3.3.1), how long to keep those records (3.3.3), or the basis on which to reduce those records (3.3.6) as needed for space.
11	EDUCAUSE	Technical	800-171r3 ipd	24	895	Requirement 3.4.8 explicitly mandates that authorized software be allowed by exception, as opposed to 800-171r2, which gives organizations the option of selecting whether to "Deny-by-Exception (Blacklisting)" or "Permit-by-Exception (Whitelisting)." In some organizations, specifically in higher education research and development but also in software development, known users often need to run "unapproved" software as part of their work. For example, every time a software developer compiles a new version of software, it has a new signature and would need approval in order to run. Without automated approvals, which are expensive, organizations with large numbers of developers or researchers will have many underutilized resources during the approval process. Blocklist methodologies are ideal in these environments in which known bad code (malware) is prohibited from running and heuristic algorithms prevent even the developed code from executing "bad" actions.	Allow the use of either approve-by-exception or blocklist methodologies. Also, consider revising dated terms such as "blacklist," "whitelist," and their derivatives where they appear to alternatives such as "blocklist," "allow list," and "deny list," which woud be consistent with NIST guidance on using inclusive language in its documentation (https //nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8366.pdf) .
12	EDUCAUSE	Editorial	800-171r3 ipd	26	974	Sub-requirement 3.4.12.a uses "significant risk," whereas the title uses "high-risk."	Use either "high-risk" or "significant risk" consistently.
13	EDUCAUSE	Technical	800-171r3 ipd	26	975	The way that 3.4.12.b is worded implies that these controls should be applied when individuals return from all travel, not just from travel to high-risk areas. Sub-requirement 3.4.12.a, on the other hand, explicitly refers to travel "to locations that the organization deems to be of significant risk."	Change the wording to "Apply the following controls to the system when the individual returns from travel to areas of high-risk/significant risk [Assignment organization-defined controls]." See Comment 12 about consistently using either "high-risk" or "significant risk."
14	EDUCAUSE	Technical	800-171r3 ipd	28	1054	The discussion under 3.5.5 (Identifier Mgt.) refers to an individual’s status as a foreign national as the potential basis on which an individual identifier might be established. This example raises particular concerns for higher education institutions, given the number of foreign nationals who participate in our campus communities as faculty and students. Recent experience shows that publicly identifying an individual as a foreign national may have adverse consequences for the individual and the institution while also negatively impacting the ability of the institution to attain and sustain its diversity, equity, and inclusion goals. While it is true that some users may need to know the nationality status of an individual in order to disseminate information appropriately to that person or those similarly situated, access to that attribute—or to other potentially sensitive identifiers—could and should be provided on an as-needed basis.	State clearly in the requirement and/or the discussion that nationality status, or any other potentially sensitive attribute, does not need to be publicly identified, but rather only available to those that have a demonstrated need to know. Also include in the discussion section the recommendation that the appropriate legal authority for the organization (e.g., its Office of General Counsel if applicable) should be consulted for specific guidance on privacy-related policy in relation to this requirement and any related issues.

* indicate required fields

15	EDUCAUSE	General	800-171r3 ipd	29	1080	Requirement 3.5.7.g, "Allow the use of a temporary password for system logons with an immediate change to a permanent password," was dropped from 800-53r5 IA-5(1). Given that the requirement is no longer part of the source framework from which it was derived, its continued relevance to 800-171 should be reconsidered.	Remove 3.5.7.g.
16	EDUCAUSE	Technical	800-171r3 ipd	36	1354	Does 3.13.11 apply if the safeguards for 3.8.5 are primarily physical? It is not clear that the requirement for cryptography as referenced in 3.13.11 in relation to the protection of media during transport applies if there are alternate physical safeguards that are the primary protection for the confidentiality of CUI.	Make reference to 3.13.11 if that is the intent "Implement cryptographic mechanisms as defined in 3.13.11 to prevent the unauthorized disclosure of CUI stored on digital media during transport."
17	EDUCAUSE	Technical	800-171r3 ipd	37	1400	Requirement 3.8.9 states the following "Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI at backup storage locations." The first sentence of the discussion reads as follows "Organizations can employ cryptographic mechanisms or alternative physical controls to protect...." These two statements contradict one another and should be reconciled.	Change the wording in 3.8.9 to reflect that alternate physical controls are acceptable "Implement cryptographic mechanisms or alternate physical controls to prevent the unauthorized disclosure of CUI at backup storage locations."
18	EDUCAUSE	Technical	800-171r3 ipd	39	1473	In multiple controls in the physical protection section (e.g., 3.10.1, 3.10.2), there are references to facilities. In 3.10.7, the entry and exit points are organizationally defined, but not in 3.10.1 and 3.10.2. Higher education institutions often have many facilities and parts of their campuses that are open to the public. Higher education institutions may control physical access within facilities that are otherwise open to the public. For example, a data center may be within an otherwise public building, but the data center itself is controlled and monitored. The wording within 3.10.1 and 3.10.2 do not make it clear that organizations have the discretion to define the areas or facilities needing physical protection.	Change 3.10.1 and 3.10.2 to include the definition that already exists within 3.10.7. An alternative edit could be to place 3.10.7 as the first control in the family, and the facility and boundaries could be defined from there to apply to all controls in the 3.10 (Physical Protection) family.
19	EDUCAUSE	Technical	800-171r3 ipd	49	1867	Requirement 3.13.8 previously permitted physical protections as an alternative to cryptographic mechanisms for both transmission and storage of CUI. SC-8(1) and SC-28(1) do not preclude physical protections as alternative forms of protection. There are many research and high-performance computing components that require the selection of cryptography at installation if cryptography is to be implemented. The costs of encrypting these components at some point after installation is prohibitive for most if not all higher education institutions. Many of these systems are built or bought to support federal research and are paid for through grants and awards. Allowing the use of alternate physical protections (as described in 3.10) still shields CUI in transit and storage within the physical boundaries. When alternate physical protections are not sufficient (as in the case of laptops and portable media, for example), the devices or equipment in question are already required to be encrypted, and a risk analysis would lead any reasonable person to select the cryptographic mechanism instead of the alternate physical controls.	Change 3.13.8 to read as follows "Implement cryptographic mechanisms or alternate physical protections to prevent the unauthorized disclosure of CUI during transmission and while in storage."
20	EDUCAUSE	Technical	800-171r3 ipd	53	1993	Requirement 3.13.18 is merely an enhancement to 3.13.1. Having a separate control is unnecessarily duplicative, and thus we suggest that NIST incorporate 3.13.18 into 3.13.1.	Include "Limit the number of external network connections to the system" as a sub-requirement under 3.13.1.
21	EDUCAUSE	Technical	800-171r3 ipd	56	2114	The relationship between spam protection and the security of CUI is unclear. Anti malware and anti-phishing solutions, for example, would have a much more direct bearing on CUI security as well as the prevention of ransomware, which would also affect CUI availability (even if that isn't a specific requirement of 800-171).	Remove 3.14.8 or make it clear that the requirement only applies to systems in which email is received as part of the system.
22	EDUCAUSE	Technical	800-171r3 ipd	58	2199	It is unclear what "Provide options for alternative sources for continued support for unsupported components" means. Read as it stands, it sounds like merely providing an option to continue local support of unsupported software is sufficient, not that such an option is actually exercised. Unsupported software is extemely common in certain industries, including higher education, on manufacturing and test systems. Sometimes there is an option to purchase a supported version, often at significant cost. When equipment is purchased as part of a contract or grant, there may be no funding to upgrade to the manufacturer's supported version. Likewise, there may be no guarantee that the manufacturer will maintain its support for the software version in question over time. A guideline that directs attention to identifying and implementing alternative measures for ensuring the security of CUI when vendor support of the relevant software has ceased would better serve the underlying objectives of 800-171.	Instead of "Provide options...," the requirement should read as follows "Provide alternative mitigation controls to protect the confidentiality of CUI on unsupported components in line with 3.11.1."
23	EDUCAUSE	Technical	800-171r3 ipd	59	2224	There are some services that are used as public services, meaning anyone can use them at no cost, and there is no agreement between the parties regarding such usage. Someone simply accesses and uses the service/site (e.g., Google search, public databases, public journals). In the course of research that works with or produces CUI, researchers may access those public sites for background or reference material. Requiring that an agreement be in place for the use of such services defeats the open nature of those resources.	Re-word 3.16.3 to allow the organization to define the external system services for which formal agreements, contracts or memorandiums of understanding are necessary, or limit the scope of the external system services covered by 3.16.3 to those that store, process, or transmit CUI.
24	EDUCAUSE	Technical	800-171r3 ipd	74	2811	The definition of FIPS-validated cryptography references "NSA-approved cryptography," but the definition of "NSA-approved cryptography" is not provided in 171r3, which could lead to confusion regarding the relevant definition from the standpoint of 171r3.	Add the relevant definition for "NSA-approved cryptography" (e.g., https //csrc.nist.gov/glossary/term/nsa_approved_cryptography# ~ text Definition(s)%3A,a%20supporting%20key%20management%20infrastructure).
25	EDUCAUSE	Technical	800-171r3 ipd	75	2886	The definition of mobile device can be read to include laptops as well as smartphones, tablets, and e-readers. The definition should make clear that laptop computers are not considered mobile devices in this context.	Add a clarification that laptops are not considered mobile devices in this context.