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

educause.edu
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
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
Senior Advisor, Policy and Government Relations
EDUCAUSE
<table>
<thead>
<tr>
<th>Comment #</th>
<th>Submitted By (Name/Org)</th>
<th>Type (General / Editorial / Technical)</th>
<th>Source (publication, analysis, overhaul)</th>
<th>Starting Page #</th>
<th>Starting Line #</th>
<th>Comment (include rationale)*</th>
<th>Suggested Change*</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EDUCAUSE</td>
<td>Technical</td>
<td>800-171r3 gpdf</td>
<td>2</td>
<td>10</td>
<td>The existing wording is overly broad, in all requirements applying to any component providing security functionality (such as log servers, configuration management databases, NSP servers) without regard to whether the component could affect the confidentiality of CUI.</td>
<td>Change: &quot;The security requirements in this publication are only applicable to components of non-federal systems that process, store, or transmit CUI or that provide protection for such components.&quot;</td>
</tr>
<tr>
<td>2</td>
<td>EDUCAUSE General</td>
<td>General</td>
<td>800-171r3 gpdf</td>
<td>4</td>
<td>70</td>
<td>The organization-defined parameters (ODPs) that federal agencies produce may not be universally or even generally applicable 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 alternate controls should generally be allowed, risks imposing 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.</td>
<td>NIST should develop an &quot;external/inter-agency agency&quot; [NISTR] 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 fill-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.</td>
</tr>
<tr>
<td>3</td>
<td>EDUCAUSE</td>
<td>Technical</td>
<td>800-171r3 gpdf</td>
<td>5</td>
<td>127</td>
<td>The term &quot;expired accounts&quot; is not defined in 800-171/200-53 or the Computer Security Resource Center (CSRC) Glossary. Define &quot;expired accounts&quot; in an appropriate location.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>EDUCAUSE Editorial</td>
<td>Editorial</td>
<td>800-171r3 gpdf</td>
<td>10</td>
<td>134</td>
<td>The reference to the term &quot;Office of General Counsel&quot; 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 &quot;Office of General Counsel&quot; with text that better aligns with how NIST SP 800-53 addresses the issue &quot;Organizations should consult with their privacy office or officer, if applicable, for input regarding privacy messaging, and with their Office of General Counsel or organizational equivalent for legal review and approval of warning banner content&quot; (as well as for input on privacy messaging since the organization does not have a privacy office or officer).</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>EDUCAUSE</td>
<td>Technical</td>
<td>800-171r3 gpdf</td>
<td>12</td>
<td>418</td>
<td>It is not clear what the definition of &quot;organization-controlled mobile devices&quot; should be. What level of control does an organization have to exert for a device to be considered &quot;organization-controlled&quot;? 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 &quot;locked-down&quot; institutionally owned devices for personal devices would be prohibitively expensive and not necessary if the institution deploys reasonable alternative device management measures. Define &quot;organization-controlled&quot; in an appropriate location, or use the term &quot;organization-managed&quot; instead.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>EDUCAUSE</td>
<td>Technical</td>
<td>800-171r3 gpdf</td>
<td>15</td>
<td>512</td>
<td>F 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 3.4.1 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 clear, significant distinction cannot be established, consider removing 3.1.23 as unnecessary.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>EDUCAUSE Editorial</td>
<td>Editorial</td>
<td>800-171r3 gpdf</td>
<td>15</td>
<td>519</td>
<td>Requirement 3.1.10 does not address automatic enforcement of inactivity (logoff); 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: &quot;Device locks are not an acceptable substitute for logging out of the system.&quot;) Remove the reference to 3.1.10. The closest control that addresses automatic enforcement of inactivity (logoff) is 3.1.11 (Session Termination).</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>EDUCAUSE Editorial</td>
<td>Editorial</td>
<td>800-171r3 gpdf</td>
<td>16</td>
<td>563</td>
<td>The term &quot;system developers&quot; is listed twice in the list of example roles. Remove one reference to &quot;system developers&quot; (line 563 or 564).</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>EDUCAUSE</td>
<td>Technical</td>
<td>800-171r3 gpdf</td>
<td>16</td>
<td>577</td>
<td>The rationale for separating 3.2 from 3.2.1 or 3.2.2 is not clear. As an enhancement under AT-2 in 800-53, it is no longer logical to incorporate 3.2 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.</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>EDUCAUSE</td>
<td>Technical</td>
<td>800-171r3 gpdf</td>
<td>19</td>
<td>705</td>
<td>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 3.4.4 mandates that organizations preserve the original content and time order 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.</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>EDUCAUSE</td>
<td>Technical</td>
<td>800-171r3 gpdf</td>
<td>24</td>
<td>895</td>
<td>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 &quot;Deny-by-Exception (Blacklisting)&quot; or &quot;Permit-by-Exception (Whitelisting).&quot; In some organizations, specifically in higher education research and development but also in software development, known users often need to run &quot;unapproved&quot; software as part of their work. For example, every time a software developer compiles a new version of software, it has a new signature (malware), is prohibited from running and heuristic algorithms prevent even the most experienced developer from accidentally gathering new evidence. Allow the use of either approve-by-exception or blacklist methodologies. Also, consider revising dated terms such as &quot;blacklist,&quot; &quot;whitelist,&quot; and their derivatives where they appear to alternatives such as &quot;blacklist,&quot; &quot;allow list,&quot; and &quot;deny list,&quot; which would be consistent with NIST guidance on using inclusive language in its documentation (<a href="https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.8386.pdf">https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.8386.pdf</a>).</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>EDUCAUSE Editorial</td>
<td>Editorial</td>
<td>800-171r3 gpdf</td>
<td>29</td>
<td>914</td>
<td>Sub-requirement 3.4.12.a uses &quot;significant risk,&quot; whereas the title uses &quot;high risk.&quot; Live either &quot;high risk&quot; or &quot;significant risk&quot; consistently.</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>EDUCAUSE</td>
<td>Technical</td>
<td>800-171r3 gpdf</td>
<td>29</td>
<td>979</td>
<td>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 &quot;travel to locations that the organization deems to be of significant risk.&quot; Change the wording to &quot;Apply the following controls to the system when the individual returns from travel to areas of high-risk/significant risk.&quot;</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>EDUCAUSE</td>
<td>Technical</td>
<td>800-171r3 gpdf</td>
<td>28</td>
<td>1054</td>
<td>The discussion under 3.5.5 (Identify App) 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.</td>
<td></td>
</tr>
</tbody>
</table>
Remove 3.5.7.g.

Make reference to 3.11.11 if that is the intent "Implement cryptographic mechanisms as defined in 3.11.11 to prevent the unauthorized disclosure of CUI stored on digital media during transport."

Change the wording to 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."

Change 3.10.1 and 3.10.2 to include the definition that already exists within 3.10.7. An alternate edit could be to place 3.10.7 as the first of the 3.10 (Physical Protection) family, and the facility and boundaries could be defined from there to apply to all controls in the 3.10 (Physical Protection) family.

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."

Include ‘Limit the number of external network connections to the system’ as a sub-requement under 3.11.1.

Remove 3.14.8 and make it clear that the requirement only applies to systems in which email is received as part of the system.

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.’

Re-word 3.16.3 to allow the organization to define the external system services for which formal agreements, contracts or memorandums 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.

Add the relevant definition for “NIST-approved cryptography” (e.g., https://csrc.nist.gov/publications/detail/sp/800-195/rev-3).