

**From:** [800-171comments@list.nist.gov](mailto:800-171comments@list.nist.gov) on behalf of [REDACTED]  
**To:** [800-171comments@list.nist.gov](mailto:800-171comments@list.nist.gov)  
**Subject:** [800-171 Comments] 800-171, Rev. 3 (FPD) / 800-171A, Rev. 3 (IPD) -- EDUCAUSE Comments  
**Date:** Friday, January 26, 2024 10:18:13 AM  
**Attachments:** [EDUCAUSE Comments 171r3 171Ar3 01-26-24 f.pdf](#)  
[EDUCAUSE sp800-171r3-fpd-comments 01-26-24.xlsx](#)  
[EDUCAUSE sp800-171Ar3-ipd-comments 01-26-24.xlsx](#)

---

Please see attached for the comments of EDUCAUSE (educause.edu) regarding the final public draft of NIST SP 800-171, Revision 3, and the initial public draft of SP 800-171A, Revision 3. The higher education IT community appreciates the opportunity to provide feedback on these important resources. If further clarification or discussion of any of our comments would be helpful, please let me know. – Jarret Cummings

---

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

**EDUCAUSE**  
*Uncommon Thinking for the Common Good*  
[REDACTED] | [educause.edu](https://educause.edu)

January 26, 2024

Ron Ross  
NIST Fellow, Computer Security  
National Institute of Standards and Technology (NIST)  
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 (NIST)  
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 (Final Public Draft), and NIST SP 800-171A, Revision 3 (Initial Public Draft)—responses submitted to [800-171comments@list.nist.gov](mailto:800-171comments@list.nist.gov)

Dear Dr. Ross and Ms. Pillitteri:

Writing for the EDUCAUSE cybersecurity community, I would like to thank you for the opportunities that NIST has made available for stakeholders to help inform the third revision of the NIST Special Publication (SP) 800-171 controlled unclassified information (CUI) cybersecurity guidelines (i.e., NIST SP 800-171, Rev. 3, or 800-171r3), as well as the companion assessment guide, NIST SP 800-171A, Rev. 3 (800-171Ar3). As the association for advancing higher education through information technology (IT), EDUCAUSE represents nearly 2,200 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. While our community's comments on the final public draft of 800-171r3 and the initial public draft of 171Ar3 have been provided in the specified comment templates (please see the attachments to the email with which this letter was submitted), I would like to address a few key points.

Our members consider 171r3 and 171Ar3 to be two sides of the same coin. From the perspective of higher education cybersecurity leaders and professionals, it is difficult to provide comprehensive input on 171r3 without the model for applying it that 171Ar3 reflects, and 171Ar3, of course, will necessarily shift as changes are made in 171r3 based on feedback regarding the final public draft. As you will see in our comments on each resource, they refer to each other out of necessity, given that information in 171Ar3 is central to interpreting 171r3 and identifying gaps or problems in it, and vice versa. Based on the essential relationship between these interrelated guides, EDUCAUSE would recommend that NIST delay the release of the final version of 171r3 to allow time for the further development and completion of 171Ar3. We are confident that the current and future comment processes for 171Ar3 will have significant implications for 171r3, making additional changes in the standards guide itself likely. Stakeholders will need to use the two resources together from the start to maximize the efficacy of their implementation and compliance efforts, and NIST can best serve the many sectors and organizations that will need to use these resources, as well as the federal agencies whose CUI is involved, by releasing them together in final form.

Regarding organization-defined parameters (ODPs), the EDUCAUSE community appreciates the efforts that NIST made between the initial and final public drafts of 171r3 to narrow the field for ODPs. An expansive, unguided use of ODPs would concern our members greatly due to the potential it introduces for widely disparate interpretations of requirements between agencies. However, EDUCAUSE member feedback indicates that the final public draft of 171r3 diverges significantly from NIST SP 800-53 in relation to the specification of ODPs, which runs against the stated goal for 171r3 to better align with 800-53. Higher education cybersecurity leaders and professionals recognize that the two guides are not intended to be identical, so some differences in terms of where and how ODPs might be deployed under each are to be expected. The rationale for where and how ODPs appear in 171r3 as compared to 800-53, though, is not clearly stated, and it is otherwise difficult to discern. EDUCAUSE asks that NIST delineate in the final version of 171r3 the governing principle or principles for the deployment of ODPs across both 800-53 and 171r3. We also request that NIST include an explanation of where and why the two do not align in relation to ODPs so that the path that NIST intends to follow in terms of maintaining the overall alignment between 171r3 and 800-53 in this respect is clear.

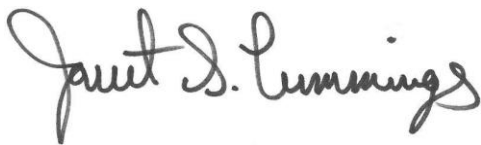
We would also like to note that, from an assessor's perspective, the initial public draft of 171Ar3 leaves a number of terms vague or undefined in ways that would make assessment of the requirements in question difficult and likely produce substantial variability in their assessment from assessor to assessor. We highlight these concerns in relation to specific assessment objectives in our comments, but the repeated use of "periodically" across various objectives serves as one example. Under the current version of 171A, the organization under

assessment has the discretion to determine what the timeframes are for the activities designated in the relevant requirements, but it is required to specify timeframes. The draft 171Ar3, however, does not specify those timeframes, nor does it refer to a requirement or requirements for the entity under assessment to do so. As a result, an assessor using 171Ar3 would have to rely solely on his/her/their judgment to determine whether the entity performed a required activity “periodically” as compared to “seldomly” or “intermittently,” which would likely lead to highly variable results across assessments.

Finally, our members appreciate the formation by NIST of its Generative AI Public Working Group ([https://airc.nist.gov/generative\\_ai\\_wg](https://airc.nist.gov/generative_ai_wg)). They believe that it serves as an effective model for engaging knowledgeable stakeholders from across relevant communities in developing NIST guidance. Given the diverse sectors and organizations impacted by NIST SP 800-171, and thus the varied contexts in which this wide range of stakeholders must apply 800-171, EDUCAUSE suggests that both NIST and the 800-171 stakeholder communities would be well-served by the formation of a public working group for 800-171. Such a group would allow for the more efficient development of requirements that reflect the broad array of circumstances in which 800-171 must be implemented and maintained, and thus the requirements would be easier to understand, implement, and maintain in those circumstances as a result.

EDUCAUSE and its member representatives stand ready to work with NIST on these issues and others that might advance the clarity and effectiveness of 171r3 and 171Ar3. If such opportunities arise, EDUCAUSE looks forward to learning where and how our community might best help NIST engage in those efforts.

Sincerely,



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

[NIST SP 800-171, Rev. 3 \(Final Public Draft\) \(https://csrc.nist.gov/pubs/sp/800/171/r3/FPD\)](https://csrc.nist.gov/pubs/sp/800/171/r3/FPD)

| Comment # | Submitted By (Name/Org):* | Type (General / Editorial / Technical) | Source (publication, analysis, overlay) | Starting Page # * | Starting Line #* | Comment (include rationale)*   | Suggested Change*   |
|-----------|---------------------------|--|---|-------------------|------------------|--|---|
| 1         | EDUCAUSE                  | Editorial                              | FPD                                     | 6                 | 147              | The term "intended system usage" is not defined anywhere and is not included in 171A.  | Rephrase "intended system usage" as "approved system usage" and include an assessment objective for "approved system usage" in 800-171A.  |
| 2         | EDUCAUSE                  | Technical                              | FPD                                     | 11                | 347              | Requiring a "publicly viewable image" precludes turning off the display (assuming a and b are also met). The discussion also references the older language of "pattern-hiding displays" rather than publicly viewable image. | Reword Requirement "c" to read as follows: "Conceal, via the device lock, information previously visible on the display with a publicly viewable image or a pattern-hiding display."                              |
| 3         | EDUCAUSE                  | Editorial                              | FPD                                     | 15                | 489              | The use of "organizational entity" is confusing in Requirement "c.2." This can be read to exclude individuals.   | Reword Requirement "c.2" to read as follows: "Retention of approved system connection or processing agreements with the organizational entity or individual hosting or managing the external system."             |
| 4         | EDUCAUSE                  | Editorial                              | FPD                                     | 16                | 533              | There is no definition of "social mining" in the glossary or NIST's glossary. The discussion presents the general outlines of a definition, but a normative reference is needed.   | NIST should assess whether it can refer to the existing definition of "data mining" in its overall glossary as the basis for a definition of "social mining," which is needed to give clarity to the requirement. |

\* indicate required fields

|   |          |                     |     |    |     |   |  |
|---|----------|---------------------|-----|----|-----|---|--|
| 5 | EDUCAUSE | Editorial/Technical | FPD | 18 | 603 | <p>If the organization-defined parameter (ODP) specifies the event types to be logged, why is the requirement asking to "specify?" If the ODP is defined by an external entity, then there is no need to review the event types selected for logging periodically as the ODP will dictate that.</p> | <p>Reword Requirement "a" to read as follows: "The following event types are selected for logging within the system [Assignment: organization-defined event types]."</p> |
| 6 | EDUCAUSE | Technical           | FPD | 19 | 627 | <p>The relevant requirement should incorporate specific wording on how to manage devices/systems that cannot include the listed content in the audit logs. There is a preamble statement about systems that cannot meet the requirements (see lines 133-138); however, that is not auditable.</p>   | <p>Reword Requirement "a" to start with "Where the system supports it, include the following content in audit logs:..."</p>  |

|   |          |           |     |    |     |   |   |
|---|----------|-----------|-----|----|-----|---|---|
| 7 | EDUCAUSE | Editorial | FPD | 19 | 651 | <p>The requirement specifically refers to a "records retention policy," implying that an organization must have an artifact named "records retention policy" rather than audit record retention information in another policy, standard, or document. Additionally, records retention policies are generally for business purposes and do not usually include audit log retention requirements.</p> | <p>Reword Requirement "b" as follows: "Retain audit records for a time period consistent with records retention requirements."</p>  |
| 8 | EDUCAUSE | Technical | FPD | 21 | 713 | <p>There is no guidance or determination regarding how long to keep original audit content. Is it for a specified time? Is it until a specific event?</p>   | <p>Reword Requirement "b" to read as follows: "Preserve the original content and time ordering of records for [Assignment: organization-defined time period]." Also adjust 171A to include an assessment objective for that ODP or an implicit organizationally defined value to be stated.</p> |

|    |          |           |     |    |     |   |   |
|----|----------|-----------|-----|----|-----|---|---|
| 9  | EDUCAUSE | Technical | FPD | 21 | 728 | The requirement to synchronize clocks with a reference clock is implied by defining granularity. It is not explicit, however, and simply defining granularity allows an organization to not use a reference clock as long as the granularity is met within the system. This would make correlation of actions across different systems (different organizations) difficult. | Re-introduce the requirement that internal system clocks must meet the defined granularity from a reference clock.  |
| 10 | EDUCAUSE | Technical | FPD | 22 | 770 | Requirement 3.4.1 no longer gives guidance on what should be included in a baseline configuration (software, hardware, etc). There is not any additional guidance in the discussion on what to include.   | The requirement or discussion should include what is expected to be in a baseline configuration.  |
| 11 | EDUCAUSE | Editorial | FPD | 24 | 824 | There is no definition of "activities associated with configuration-controlled changes" nor is there additional information in the discussion.  | Clarify specifically what "activities associated with configuration-controlled changes" are. Are those tracking, reviewing, approving or disapproving, and logging? |
| 12 | EDUCAUSE | Technical | FPD | 24 | 838 | This requirement is redundant with 3.4.3.b, which explicitly requires that security impacts are considered in the required review.  | Remove Requirement 3.4.4 as ORC (adequately covered by other related controls).   |



|    |          |           |     |    |      |  |   |
|----|----------|-----------|-----|----|------|--|---|
| 13 | EDUCAUSE | Editorial | FPD | 26 | 905  | The discussion for Requirement 3.4.8 still implies that defining prohibited software is acceptable.  | Remove the sentence, "Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious," from the discussion. |
| 14 | EDUCAUSE | Editorial | FPD | 26 | 915  | The discussion for Requirement 3.4.8 refers to verifying the integrity of software, which is not a requirement.  | Remove the last two sentences of the discussion of Requirement 3.4.8 (starting at "Organizations consider verifying the integrity of ...").   |
| 15 | EDUCAUSE | Technical | FPD | 27 | 948  | Requirement 3.4.11.b is identical to 3.1.1.c, which requires a list of authorized users, their roles, and their privileges.  | Remove Requirement 3.4.11.b as ORC (adequately covered by other related controls).  |
| 16 | EDUCAUSE | Technical | FPD | 30 | 1070 | The way this requirement is worded implies that a password must be changed on first use <i>*after*</i> account recovery. Many account recovery processes include changing a default, initial, or expired password as part of the process. Asking users to change their password <i>*again*</i> when they first use it is redundant and can result in users selecting poor passwords. | Reword Requirement "e" as follows: "Select a new password upon first use after account recovery or as part of the account recovery process."  |

|    |          |           |     |    |      |   |  |
|----|----------|-----------|-----|----|------|---|--|
| 17 | EDUCAUSE | Technical | FPD | 34 | 1205 | This requirement for incident response training is for end users of a system, not specifically for incident response handlers.  | Integrate this requirement into Requirement 3.2.2 as part of the training that incident response handlers should receive in order to fulfill the responsibilities of their position. |
| 18 | EDUCAUSE | Technical | FPD | 35 | 1240 | While the goal of Requirement 3.7.4.b is admirable, the act of inspection isn't clear. How are employees supposed to inspect the maintenance tool(s)? By physical inspection only? Malware inspection (Requirement "c")?  | Ensure that the discussion and the assessment guide are clear on what "inspect" means in this scenario. Is it a physical inspection or a logical inspection?                         |
| 19 | EDUCAUSE | Technical | FPD | 36 | 1307 | Requirement 3.8.1 is not clear regarding where in the media lifecycle this should apply. Is this only after the media is used and ready for disposal or reuse? Is it while the media is in active use as well? One of "physically control" or "securely store" will be sufficient to protect CUI. | Reword Requirement 3.8.1 to "Physically control <i>or</i> securely store system media containing CUI..."   |
| 20 | EDUCAUSE | Technical | FPD | 37 | 1325 | With the removal of "authorized users," what does it mean to restrict access?   | Re-word the requirement to include "authorized users" (i.e., "Restrict access to CUI on system media to authorized users").  |

|    |          |           |     |    |      |  |  |
|----|----------|-----------|-----|----|------|--|--|
| 21 | EDUCAUSE | Editorial | FPD | 38 | 1369 | The discussion references 03.13.11, but there is no requirement to encrypt the media (in this requirement, 03.08.05).  | Remove the reference to cryptography and 03.13.11. Requirement 3.13.8 requires encryption of CUI during transmission or in storage.  |
| 22 | EDUCAUSE | Editorial | FPD | 40 | 1448 | The term "security-related system property" is not defined in the glossary, but is mentioned in the discussion.  | Add a definition for "security-related system property" to the glossary.   |
| 23 | EDUCAUSE | Technical | FPD | 41 | 1488 | This sentence implies that just removing users from the access list is sufficient to meet this requirement, but 03.10.01 does not require actual access removal. | Add a Requirement "e": "Recover/disable authorization credentials when access is no longer required."  |
| 24 | EDUCAUSE | Editorial | FPD | 43 | 1548 | The grammer is incorrect for this requirement.   | Add the word "when" prior to the assignment block: "Escort visitors and control visitor activity when [Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity]." |

|    |          |           |     |    |      |   |   |
|----|----------|-----------|-----|----|------|---|---|
| 25 | EDUCAUSE | Technical | FPD | 46 | 1658 | Updating the POAM "periodically" does not make sense. The POAM is a living document that is updated based on the findings from security assessments (which are required periodically), independent audits or reviews, and continuous monitoring activities. As these activities themselves are "periodic," there is no need to explicitly update the POAM "periodically." | Reword Requirement "b" to read as follows: "Update the existing plan of action and milestones based on the findings from security assessments, independent audits or reviews, and continuous monitoring activities."  |
| 26 | EDUCAUSE | Technical | FPD | 47 | 1689 | It is completely inappropriate for an outside entity to dictate what kind of agreements are in place between private organizations. This should be an "implied" ODP rather than stated for an external entity to define.  | Reword Requirement "a" to read as follows: "Approve and manage the exchange of CUI between the system and other systems using appropriate agreements, which can include interconnection security agreements, information exchange security agreements, memoranda of understanding or agreement, service level agreements, user agreements, or non-disclosure agreements." |
| 27 | EDUCAUSE | Technical | FPD | 50 | 1809 | It is inappropriate for an outside entity to dictate what internal procedures and processes are for key management. This should be an "implied" ODP rather than stated for an external entity to define.  | Reword the requirement to read as follows: "Establish and manage cryptographic keys in the system in accordance with internal processes and procedures."  |

|    |          |           |                 |             |      |  |   |
|----|----------|-----------|-----------------|-------------|------|--|---|
| 28 | EDUCAUSE | Technical | FPD             | 55          | 2001 | Data retention does not affect the confidentiality of CUI except in the context of data being maintained in systems or storage longer than necessary. Management of information can affect the confidentiality of CUI. | Reword the requirement to read as follows: "Manage and retain CUI within the system and CUI output from the system for the minimum time period consistent with applicable laws, executive orders...." |
| 29 | EDUCAUSE | Technical | FPD             | 56          | 2037 | Why is a.3 part of the system security plan and not already considered as part of Risk Assessment (3.11.1)?  | Remove Requirement 3.15.2.a.3 as redundant and adequately covered by other controls.  |
| 30 | EDUCAUSE | Technical | FPD             | 60          | 2175 | Acquisition is a "supply chain process"; there is no need for it to be covered by a separate requirement.  | Combine Requirements 3.17.2 and 3.17.3.   |
| 31 | EDUCAUSE | Editorial | FPD             | 77          | 2861 | Split tunneling is no longer in any requirements.  | Remove "split tunneling" from the document glossary.  |
| 32 | EDUCAUSE | Editorial | FPD-CUI overlay | Overlay Tab |      | NFO is used but not defined.   | Include NFO in the definitions provided on the Overview tab.  |

| NIST SP 800-171A , Rev. 3 (Initial Public Draft) ( <a href="https://csrc.nist.gov/pubs/sp/800/171/a/r3/ipd">https://csrc.nist.gov/pubs/sp/800/171/a/r3/ipd</a> ) |                           |  |   |                   |                  |  |   |
|--|---------------------------|--|---|-------------------|------------------|--|---|
| 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                              | IPD                                     | 7                 | 435              | The requirement mandates that access be based on "intended system usage," but that term is not defined by the organization or as an ODP, thus making it difficult to assess if something is authorized based on intended system usage. | Add an assessment objective under A.03.01.01.d to define/specify "intended system usage." If NIST accepts the change proposed for 800-171r3 to use "approved system usage" instead of "intended system usage," then that edit should be reflected here as well. |
| 2  | EDUCAUSE                  | Technical                              | IPD                                     | 10                | 560              | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to assess if the action is being performed "periodically."  | Add an assessment objective to define/specify the period in which the review occurs.  |

|   |          |           |     |    |     |   |  |
|---|----------|-----------|-----|----|-----|---|--|
| 3 | EDUCAUSE | Technical | IPD | 11 | 588 | The requirement mandates that users with privileged accounts use non-privileged accounts when accessing nonsecurity functions or nonsecurity information. Without definitions of "nonsecurity function" and "nonsecurity information," though, the assessor must rely on his/her/their opinion regarding the functions and information necessary to fulfill the requirement, a view which may vary from assessor to assessor. | Add an assessment objective(s) to define/specify what the organization considers nonsecurity functions and/or nonsecurity information. |
| 4 | EDUCAUSE | Technical | IPD | 12 | 608 | An organization must define the functions that it considers "privileged" in order for an assessor to determine if privileged functions are being logged and restricted.   | Add an assessment objective to define/specify "privileged functions."  |
| 5 | EDUCAUSE | Technical | IPD | 13 | 651 | This assessment objective requires the assessor to know and determine what the "applicable CUI rules" are for a specific industry/company/project.  | Add an assessment objective to define/specify the system use notification message.   |

|    |          |           |     |    |          |   |  |
|----|----------|-----------|-----|----|----------|---|--|
| 6  | EDUCAUSE | Technical | IPD | 15 | 731      | These assessment objectives leave the assessor to determine what constitutes "privileged commands" and "security-relevant information."                                       | Add assessment objectives to define/specify "privileged commands" and "security-relevant information." |
| 7  | EDUCAUSE | Technical | IPD | 18 | 866      | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add an assessment objective to define/specify the period in which the review occurs.                   |
| 8  | EDUCAUSE | Technical | IPD | 19 | 891, 905 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add an assessment objective to define/specify the period in which the review occurs.                   |
| 9  | EDUCAUSE | Technical | IPD | 20 | 931,935  | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add an assessment objective to define/specify the period in which the review occurs.                   |
| 10 | EDUCAUSE | Technical | IPD | 19 | 888      | This requirement is for security literacy content, not role-based security training.  | Change A.03.02.02.ODP[01] to address events that require security literacy training.                   |



|    |          |           |     |    |         |   |   |
|----|----------|-----------|-----|----|---------|---|---|
| 11 | EDUCAUSE | Technical | IPD | 19 | 884     | For both 3.2.1 and 3.2.2, the ODP for when to give additional training vs. update the existing training should be separated as there may be events that require one, but not the other. As an example: if a user violates policy, the training doesn't necessarily need to be updated, but the user should be reminded of the policy and existing training. | Separate the ODPs in 3.2.1 and 3.2.2 to [01] events that required <type> training are defined, and [02] events that require updating <type> training are defined. |
| 12 | EDUCAUSE | Technical | IPD | 21 | 960,961 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically."   | Add assessment objectives to define/specify the period in which the review and update occurs.   |
| 13 | EDUCAUSE | Technical | IPD | 22 | 985     | Without knowing what an organization has defined as additional information needed for audit logs, an assessor is unable to determine if the logs contain that additional information.   | Add an assessment objective to define/specify additional information needed in audit logs.  |
| 14 | EDUCAUSE | Technical | IPD | 22 | 1006    | Without knowing what the audit log retention period/time is, an assessor is unable to determine if the logs are maintained for that period of time.   | Add an assessment objective to define/specify the time period for retention of audit records.   |

|    |          |           |     |    |      |   |   |
|----|----------|-----------|-----|----|------|---|---|
| 15 | EDUCAUSE | Technical | IPD | 23 | 1022 | Without knowing what audit process failures should be monitored or lead to alerts, an assessor is unable to determine if this requirement is being met.                       | Add an assessment objective to define/specify what the organization considers an "audit logging process failure."   |
| 16 | EDUCAUSE | Technical | IPD | 24 | 1051 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add an assessment objective to define/specify the period in which the review and analysis occurs.   |
| 17 | EDUCAUSE | Technical | IPD | 24 | 1053 | Without knowing to which organizational personnel or roles findings are being reported, an assessor is unable to determine if this requirement is being met.                  | Add an assessment objective that defines to which organizational personnel or roles findings are reported.  |
| 18 | EDUCAUSE | Technical | IPD | 24 | 1054 | Without knowing what organizational repositories should be included in the analysis and correlation, an assessors is unable to determine if this requirement is being met.    | Add an assessment objective that defines what repositories should be included in the analysis and correlation.  |
| 19 | EDUCAUSE | Editorial | IPD | 24 | 1074 | This assessment objective is inconsistent with others in terms of how it is organized.  | Separate record reduction and report generation into distinct assessment objectives: "An audit record reduction capability that supports..." and "A report generation capability that supports...." |

|    |          |           |     |    |            |   |  |
|----|----------|-----------|-----|----|------------|---|--|
| 20 | EDUCAUSE | Editorial | IPD | 25 | 1119       | The assessment objectives for A.03.03.08.a are inconsistent with others in terms of how they are organized.   | Separate the assessment objectives into [01] "... protected from unauthorized access," [02] "... protected from unauthorized modification," and [03] "... protected from unauthorized deletion." |
| 21 | EDUCAUSE | Technical | IPD | 26 | 1148, 1151 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically."                 | Add assessment objectives to define/specify the periods in which reviews and updates occur.  |
| 22 | EDUCAUSE | Editorial | IPD | 27 | 1172       | The assessment objectives in 3.4.3 are broken out for each item (defined, reviewed, approved), vs 3.4.2 where "documented and implemented" are combined                                       | Be consistent with how assessment objectives are broken out (or not) from the requirement statement itself.  |
| 23 | EDUCAUSE | Editorial | IPD | 30 | 1286       | Assessment objectives A.03.04.06.ODP[06] - [10] are not explicit ODPs in the requirement and should not be listed as such. They should still be defined as part of the assessment objectives. | Remove the .ODP designation from .ODP[06]-[10] and make them "normal" assessment objectives.   |
| 24 | EDUCAUSE | Technical | IPD | 30 | 1291       | Mission-essential capabilities should be defined.   | Add an assessment objective for the organization to define its "mission-essential capabilities."   |

|    |          |           |     |    |            |   |   |
|----|----------|-----------|-----|----|------------|---|---|
| 25 | EDUCAUSE | Technical | IPD | 31 | 1341, 1342 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add assessment objectives to define/specify the periods in which reviews and updates occur. |
| 26 | EDUCAUSE | Technical | IPD | 32 | 1367, 1368 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add assessment objectives to define/specify the periods in which reviews and updates occur. |
| 27 | EDUCAUSE | Technical | IPD | 34 | 1427       | "High-risk areas" are not defined by an ODP or an implicit ODP.   | Add an assessment objective to define "high-risk areas."                                    |
| 28 | EDUCAUSE | Technical | IPD | 37 | 1539       | "Personnel or roles from whom authorization must be received" is not an ODP, but should still be defined.   | Remove the .ODP designation from .ODP[01] and make it a "normal" assessment objective.      |
| 29 | EDUCAUSE | Technical | IPD | 38 | 1571       | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add an assessment objective to define/specify the period in which updates occur.            |

|    |          |           |     |    |            |   |   |
|----|----------|-----------|-----|----|------------|---|---|
| 30 | EDUCAUSE | Editorial | IPD | 41 | 1684       | There is an inconsistent separation of requirements into assessment objectives in 3.6.2. This requirement separates tracked and documented into two different assessment objectives, but others would not be separated as such (see Requirement 3.4.2). | Be consistent with how assessment objectives are broken out (or not) from the requirement statement itself. |
| 31 | EDUCAUSE | Technical | IPD | 42 | 1718       | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically."   | Add an assessment objective to define/specify the period in which testing occurs.                           |
| 32 | EDUCAUSE | Technical | IPD | 42 | 1746, 1749 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically."   | Add assessment objectives to define/specify the periods in which reviews and updates occur.                 |
| 33 | EDUCAUSE | Technical | IPD | 45 | 1836       | "Technical competence" is not defined by the organization, leaving an assessor unable to determine if personnel have the required "technical competence."   | Add an assessment objective to define/specify what "technical competence" means for maintenance purposes.   |

|    |          |           |     |    |      |   |   |
|----|----------|-----------|-----|----|------|---|---|
| 34 | EDUCAUSE | Technical | IPD | 46 | 1878 | Without an ODP or an organizational definition of "restricted," an assessor cannot determine if this requirement is being met or not.   | Change the requirement to include "restricted to authorized users" or add an assessment objective to define what "restricted" means.            |
| 35 | EDUCAUSE | Technical | IPD | 48 | 1945 | Requirement 3.8.5 does not have a sub-requirement "c."  | Remove A.03.08.05.c.  |
| 36 | EDUCAUSE | Technical | IPD | 50 | 2016 | Without a definition of what "screening" entails, an assessor cannot determine if the requirement is being met or not.  | Add an assessment objective to define what "screening" is for each organization.  |
| 37 | EDUCAUSE | Technical | IPD | 51 | 2043 | Without a definition of what constitutes "security-related system property," an assessor cannot determine if the requirement is being met or not.                             | Add an assessment objective to define what "security-related system property" an organization is expected to retrieve from departing employees. |
| 38 | EDUCAUSE | Editorial | IPD | 52 | 2082 | The assessment objective uses the phrase "facility access," whereas 800-171r3 FPD uses the term "physical access."  | Be consistent in the assessment objectives regarding the stated requirement.  |
| 39 | EDUCAUSE | Technical | IPD | 52 | 2083 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add an assessment objective to define/specify the period in which the review occurs.  |
| 40 | EDUCAUSE | Editorial | IPD | 52 | 2084 | The wording about what is expected is very confusing.   | Change A.03.10.01.d to "Individuals are removed from the access list when access is no longer required."  |

|    |          |           |     |    |                  |   |  |
|----|----------|-----------|-----|----|------------------|---|--|
| 41 | EDUCAUSE | Technical | IPD | 53 | 2019             | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add an assessment objective to define/specify the period in which the review occurs.                           |
| 42 | EDUCAUSE | Technical | IPD | 53 | 2105             | The way these assessment objectives are broken out is confusing. Generally, you monitor to detect, and then you respond.  | Reword A.03.10.02.a[02] to read "Physical security incidents are responded to."                                |
| 43 | EDUCAUSE | Editorial | IPD | 54 | 2168 - 2170      | Not all keys, combinations, or other physical access devices are used at the same time. One is sufficient to prevent physical access.   | Reword A.03.10.07.d to "Keys, combinations, or other physical access devices are secured where they are used." |
| 44 | EDUCAUSE | Technical | IPD | 56 | 2221             | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add an assessment objective to define/specify the period in which the update occurs.                           |
| 45 | EDUCAUSE | Technical | IPD | 56 | 2245, 2248, 2552 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add assessment objectives to define/specify the periods in which the actions occur.                            |

|    |          |           |     |    |                  |   |  |
|----|----------|-----------|-----|----|------------------|---|--|
| 46 | EDUCAUSE | Technical | IPD | 57 | 2281             | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add assessment objectives to define/specify the periods in which the actions occur.                                  |
| 47 | EDUCAUSE | Technical | IPD | 58 | 2304, 2306, 2308 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add assessment objectives to define/specify the periods in which the actions occur.                                  |
| 48 | EDUCAUSE | Technical | IPD | 60 | 2365, 2366       | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add assessment objectives to define/specify the periods in which the actions occur.                                  |
| 49 | EDUCAUSE | Technical | IPD | 63 | 2487             | Without a definition of "periods of inactivity," an assessor cannot determine if this requirement is met or not.  | Add an assessment objective to define "periods of inactivity."   |
| 50 | EDUCAUSE | Technical | IPD | 67 | 2624             | Without knowing to which organizational personnel or roles security flaws are being reported, an assessor is unable to determine if this requirement is being met.            | Add an assessment objective that defines the organizational personnel or roles to which security flaws are reported. |



|    |          |           |     |    |            |   |   |
|----|----------|-----------|-----|----|------------|---|---|
| 51 | EDUCAUSE | Technical | IPD | 68 | 2655       | Without a definition of "designated locations," an assessor is unable to determine if this objective is being met or not.   | Add an assessment objective about defining the designated locations.  |
| 52 | EDUCAUSE | Technical | IPD | 68 | 2666       | The actions an organization will take in response to malicious code detection should be defined.  | Add an assessment objective about defining what actions the organization will take in response to malicious code detection.   |
| 53 | EDUCAUSE | Technical | IPD | 69 | 2698       | Without a definition of "established time frames," an assessor is unable to determine if this requirement is being met.   | Add an assessment objective to define "established time frames" to implement security directives, *or* require as part of A.03.14.03.b[01] that time frames for security directives are established as part of the generation of such directives. |
| 54 | EDUCAUSE | Technical | IPD | 72 | 2796, 2797 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add assessment objectives to define/specify the periods in which the actions occur.   |
| 55 | EDUCAUSE | Technical | IPD | 72 | 2825, 2826 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add assessment objectives to define/specify the periods in which the actions occur.   |

|    |          |           |     |    |            |   |   |
|----|----------|-----------|-----|----|------------|---|---|
| 56 | EDUCAUSE | Technical | IPD | 73 | 2854, 2855 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add assessment objectives to define/specify the periods in which the actions occur. |
| 57 | EDUCAUSE | Editorial | IPD | 76 | 2959       | "SCRM" is used without it being defined in the glossary or list of acronyms.  | Add "SCRM" to the list of acronyms in both 800-171 and 800-171A.                    |
| 58 | EDUCAUSE | Technical | IPD | 76 | 2975, 2976 | "Periodically" is not defined by an ODP or by the organization itself, thus making it hard for an assessor to determine whether the action is being performed "periodically." | Add assessment objectives to define/specify the periods in which the actions occur. |