| | |
|---|---|
| **From:** | [redacted] via 800-171comments |
| **To:** | 800-171comments@list.nist.gov |
| **Subject:** | [800-171 Comments] Revision 3 Comments |
| **Date:** | Friday, July 14, 2023 9:23:38 PM |
| **Attachments:** | image002.png<br>image003.png<br>image004.png<br>image005.png<br>sp800-171r3-ipd-comment-Guernsey.xlsx |

---

Good evening, please find attached comments from Guernsey regarding revision 3 of NIST SP 800-171.

Warm Regards,
Laura


Laura Fawcett, CISM, CGEIT

*Sr. Governance Risk and Compliance Consultant*

guernsey

[redacted]

[redacted]

guernsey.us


**REALIZE THE DIFFERENCE**

| Comment # | Submitted By (Name/Org):* | Type (General / Editorial / Technical) | Source (publication, analysis, overlay) | Starting Page # * | Starting Line #* | Comment (include rationale)* | Suggested Change* |
|---|---|---|---|---|---|---|---|
| 1 | Guernsey | General | publication | 2 | 30 | Specifically states the requirements only apply to assets (IT, OT, IoT) that process, store, or transmit CUI, as well as protection of such components. Is there a concept of risk-managed assets (or similar) where some requirements would apply? | Add clarification regarding assets used to access CUI assets (assets that processes, store, or transmit CUI) but do not hold CUI themselves. For example, do workstations used to access a cloud environment containing CUI (but will not hold CUI) fall under any of the configuration requirements (application control, least functionality). 3.1.18 as currently written seems to cover any mobile devices connecting to the system (CUI asset) under parts a. and b., but by the description provided these requirements wouldn't apply to a mobile device that doesn't contain CUI. |
| 2 | Guernsey | General | publication | 5 | 116 | Federal agencies likely won't specifiy the policies/procedures a company will use to manage account lifecycles, these will be internal documents. | 3.1.1.b - remove ODP and just say organization policies and procedures (similar to 3.14.2.b). |
| 3 | Guernsey | General | publication | 5 | 131 | Since this relates to a high-risk person, rather than account, there are multiple groups and activities involved, and not just a simple 'disable account'. | Remove 3.1.1.g as part of these account lifecycle practices. This also appears to be addressed in the current version of 172 (3.9.2.e) |
| 4 | Guernsey | General | publication | 8 | 232 | the requirement from AC-6(1) (3.1.5.b) should move to 3.1.6 (dealing with privileged access) and better goes with AC-6(2). | Move 3.1.5.b to replace 3.1.6.a and reword to something like "Restrict privileged access to roles tasked with the configuration, maintenance, or security of CUI systems. |
| 5 | Guernsey | General | publication | 8 | 234 | remove ODPs for users on 3.1.5.c and make CUI specific | 3.1.5.c (based on suggestion above would become 3.1.5.b) - Review [Assignement: organization-defined frequency] the permissions assigned to users with access to CUI to validate continued need. |
| 6 | Guernsey | General | publication | 8 | 254 | remove ODP and specifically state security of CUI. | 3.1.6.b: Require that users or roles with privileged access to systems or security related functions, use non-privileged accounts or roles when accessing non-security functions. |
| 7 | Guernsey | General | publication | 8 | 256 | Add a requirement that mirrors current 3.1.5.c to set period for review of privileged access in the event it is reviewed at a frequency different from standard (CUI) users. | add 3.1.6.c - Review [Assignement: organization-defined frequency] privileged access assigned to users or roles to validate continued need. |

| Comment # | Submitted By (Name/Org):* | Type (General / Editorial / Technical) | Source (publication, analysis, overlay) | Starting Page # * | Starting Line #* | Comment (include rationale)* | Suggested Change* |
|---|---|---|---|---|---|---|---|
| 8 | Guernsey | General | publication | 12 | 418 | Add clarification that is applies to mobile devices that can connect to the system. | 3.1.18.a - add: used to access or store CUI |
| 9 | Guernsey | General | publication | 15 | 525 | Because this only applies to system components that process, store, or transmit CUI or provide protection of those components, 3.2.1 should apply to users of a CUI system. | Update 3.2.1.a.1: Before authorizing access to the system containing CUI and [Assignment: organization-defined frequency] |
| 10 | Guernsey | General | publication | 16 | 553 | With the recommended update to 3.2.1, it is suggested that 3.2.2 apply to security roles. | Update 3.2.2.a.1: Assigned security-related duties, roles at least [Assignment: organization-defined frequency]. |
| 11 | Guernsey | General | publication | 17 | 604 | Because logged events for 'the system' will include a variety of hardware, software, and security tools, the expectation should be that the organization identifies and details what events will be logged to meet other objectives of AU family. | 3.3.1.a: Specify and document the event types for logging based on the types of events that system component(s) is/are capable of logging in support of the audit function |
| 12 | Guernsey | General | publication | 20 | 722 | For correlation requirements, time synchronization is important, and included in the 800-53 controls referenced by 3.3.7 | Add a requirement for synchnronization through the user of a single time source. |
| 13 | Guernsey | General | publication | 22 | 815 | Make specific to CUI impacts. | 3.4.3.a - Determine the types of changes to the system that could impact the confidentiality of CUI. Adjust wording on the remaning requirements to align with changes to '.a.' |
| 14 | Guernsey | General | publication | 23 | 864 | Reference to software in 3.4.6 b. & c. isn't clearly explained in discussion, so it seems redundant with 3.4.8 without applicable discussion. | Either remove reference to software in 3.4.6.b and completely remove 3.4.6.c , or add additional detail in discussion about the scope of 3.4.6.c (based on CM-7(2)) and setting standards for software (e.g., company policy, terms of use, licensing) |

| Comment # | Submitted By (Name/Org):* | Type (General / Editorial / Technical) | Source (publication, analysis, overlay) | Starting Page # * | Starting Line #* | Comment (include rationale)* | Suggested Change* |
|---|---|---|---|---|---|---|---|
| 15 | Guernsey | General | publication | 24 | 895 | Given the varying sizes and complexity of non-federal system owner's environments, the option for whitelisting or blacklisting in rev. 2 was helpful. The discuss seems to infer that this can be procedural or automated, but 3.4.8.b wording 'deny-all, allow-by-exception….execution' seems to indicate an automated solution requirement. | Update 3.4.8.b wording to more clearly indicate procedural *or* technical controls, or include the option for blacklisting. |
| 16 | Guernsey | General | publication | 25 | 945 | 3.4.10 discussion needs to provide more specific information related to non-federal companies and their obligations. In many cases their assets in-scope as part of the "CUI System" are not all assets. Further, the level of detail of asset inventories (date of receipt, cost, supplier info, etc.) mentioned in the discussion seems excessive for this application. | Discuss if the non-federal companies need to maintain inventory of all components with an indication of those assets that process, store, transmit, or provide security to protect the confidentiality of CUI, or just those specific assets.<br>If specific information is expected in the inventory, that should be called out in the security requirement, not the discussion. |
| 17 | Guernsey | General | publication | 26 | 971 | Practices only applies to devices processing, storing, or transmitting CUI, or security of CUI. Is it expected 3.4.12 (and possibly other requirements) also apply to devices that could connect to the 'system'? | Update wording on 3.4.12 to add 'if those devices may process, store, or transmit CUI' while in the high risk area. |
| 18 | Guernsey | General | publication | 29 | 1072 | Concern over 'including spaces and all printable characters' in the control statement rather than discussion. There could be some systems that support long passphrases, but not spaces. While encouraged, inability to support spaces does not necessarily increase risk. | For 3.5.7 remove b, or at least reduce to just state allow use of long passwords and passphrases. |
| 19 | Guernsey | General | publication | 31 | 1173 | Don't see the need for ODP here unless agency wants to set a requirement (which could be specified other ways). | Update 3.6.2 b to require documentation of reporting authorities in the IR plan. |

| Comment # | Submitted By (Name/Org):* | Type (General / Editorial / Technical) | Source (publication, analysis, overlay) | Starting Page # * | Starting Line #* | Comment (include rationale)* | Suggested Change* |
|---|---|---|---|---|---|---|---|
| 20 | Guernsey | General | publication | 35 | 1310 | An ODP for non-Government systems seems too broad here, there could be a large variety of roles/personnel and could change frequently. | Remove ODP and set requirements that access is restricted to approved roles and personnel per policy. Compliance could be demonstrated by sampling of users with access to CUI and their roles. |
| 21 | Guernsey | General | publication | 42 | 1558 | Is ODP really needed here or even this requirement? Fedramp does not set a standard for the ODP and seems very broad and risk of too many different interpretations on the level of specificity required. We understand the concern about sending CUI to printers unattended or unattended computers (that should be locked), but seems this could be addressed by other controls. | Remove ODP for 3.10.8 and require organziations assess risk based on use cases, or remove the practice entirely. |
| 22 | Guernsey | General | publication | 44 | 1639 | This seems to overlap with 3.12.2. Also, based on RA-7, wich is more about responding based on organizational risk tollerance not just responding to all findings. | Reword 3.11.4 to be more specific and tied to RA-7 or roll into 3.12.2 |
| 23 | Guernsey | General | publication | 53 | 1994 | Seems more about somsilidating entry points/access points rather than limits on external connections. Need for external connections will vary wildly across private industry. | Reword 3.13.18 to focus on entry/exit points into the network rather than # of connections. |
| 24 | Guernsey | General | publication | 60 | 2303 | Why have ODP here, especially given the rise in continual monitoring and updates? SI-8 doesn't have ODP | Update 3.14.8.b to more consistently align with SI-8 (b) or just require regular updates. |
| 25 | Guernsey | General | publication | 60 | 2303 | Rather than a ODP here, given variety of non-government systems and use/storage of CUI and third parties, this might be a good place to reference need for 'alignment with organizational supply chain mangement policies' | Update 3.17.3 to remove ODP and require organizational policies to address supply chain risk. |