From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] Comments on NIST SP 800-171 Rev 3 fpd
Date: Friday, January 26, 2024 5:16:51 PM

Please accept the following comments on the final public draft of NIST SP 800-171:

3.1.18, Lines 449-456
The definition of "mobile device" is written such that typical laptop computers and notebook computers meet the definition, and it would seem to make (security) sense to apply this requirement to such systems. However, they are not included in the list of examples on line 454; line 456 distinguishes "notebook" systems from mobile devices. This ambiguity invites confusion as to whether this requirement applies to laptop and notebook systems. Suggest adding laptops and/or notebooks to the list of examples on line 454. Suggest removing "notebook or" from line 456. Conversely, if the intent is that this requirement does NOT apply to laptops and notebooks, recommend adding an explicit mention of the reason for this intent to preclude misapplication.

3.1.20, Line 480
Suggest limiting this requirement to use of external systems to process, store, or transmit CUI. As currently worded, requirement 3.1.20a could be construed to require authorization of every individual web site that a user might visit since accessing a web site is a form of "use" of an external system. Since the security requirements of NIST SP 800-171 only apply to the organizational systems used to process, store, or transmit CUI, the scope of applicability to external systems should be similarly limited. While this may be implied by Section 1.1, it would help to clarify the applicability to external systems.

3.1.22
This requirement is difficult to reconcile with the scoping guidance provided in Section 1.1. Since the NIST SP 800-171 requirements only apply to systems used to process, store, or transmit CUI, and since CUI must be removed from all publicly accessible systems (per 3.1.22b), it is not clear which "publicly accessible systems" requirement 3.1.22b applies to. It is unclear whether there is a way for the organization to limit the scope of applicability of this requirement, or that it must apply to all publicly accessible systems under the organization's control. It is also unclear whether this requirement applies to external publicly accessible systems that the organizational systems exchange data with. For example, if an organization allows its employees to use company-issued laptops to post on publicly accessible social media sites, does this requirement obligate the organization to review the content on those sites for CUI periodically? This requirement's Discussion section should provide meaningful guidance and relevant examples of how to interpret the scope of this requirement.

3.5.2
Based on the information presented in the Discussion section, an ODP should be included in the requirement such that organizations can define which devices require unique device-to-device identification and which require authentication. For example, some devices do not require either. Others may require only identification (e.g., MAC or TCP/IP address), and others may require both identification and authentication. Without the ODP, the requirement may be construed to require both identification and authentication for all devices connecting to

the system.

3.8.1, line 1311
It would seem that this requirement should apply to internal, non-removable solid state or magnetic drives as well. Even internal, non-removable media can be exploited if it is not physically controlled. Physical control of system components is covered by PE family controls, but 3.8.1 addresses specifics of media handling that are not fully addressed by those requirements. In contrast to 3.8.1, 3.8.3, in lines 1340-1342, expands the definition of "media" to include internal, non-removable media. It would be better to have a consistent definition of "system media" for all requirements. It would seem that all MP family requirements would apply to all types of media, but if there's a need to distinguish between protections required for external or removable media and protections required for internal non-removable media, then different terms should be defined so this is clear in all cases. Perhaps the term "removable system media" (introduced in 3.8.7) could be used in all cases when the intent is to exclude internal non-removable media. Using the same term ("media") with different examples is confusing and ambiguous.

3.8.1, line 1322
Since this requirement discusses sanitization of media, it would be helpful to list NIST SP 800-88 Rev 1 as a supporting publication.

3.8.2
In addition to the physical controls discussed, it is common to use cryptographic means to restrict access to CUI on system media. For example, if only authorized personnel have the keys needed to decrypt CUI stored on system media, that effectively restricts access to the CUI. This is an important alternative to physical controls that should be discussed.

3.8.4
There is often confusion in industry as to whether markings must be external to the media, and the Discussion section of this requirement does not help clarify what sort of markings are acceptable. For example, if documents are stored on a USB memory stick, does 3.8.4 require an external label on the outside of the memory stick? Or is it acceptable for each document to have labels that are readable when the document is viewed? Recommend clarifying the intent in the Discussion section of this requirement with an explicit statement as to whether labels need to be external, internal, either, or both.

3.8.4
This requirement defines "system media" differently than 3.8.3. 3.8.3 explicitly states that media sanitization is required for notebook computers, workstations, mobile devices, and network components. However, the examples in 3.8.4 exclude those items with internal, non-removable media. Is it accurate to infer that media marking is not required for notebook computers, workstations, mobile devices, and network components? Of the MP family, sanitization (3.8.3) is the only control that explicitly mentions it applies to those components with internal, non-removable media. Suggest a consistent definition of “system media” that applies to both removable and non-removable media.

3.10.1
It would be helpful to clarify applicability of this requirement to systems that have mobile/portable components that do not reside in a single physical location. For example, laptop/notebook computers are a common component of systems that are sometimes located in

organizationally managed facilities (e.g., offices) but are often relocated to locations/facilities not under the organization's physical control. It is unclear whether this requirement applies to all system components or only those with a defined physical location (i.e., non-portable components). The Discussion section could contain examples of how organizations could apply this requirement to systems containing some (or all) portable components and specifically how they could address situations where one or more system components are in physical locations outside the organization's control (e.g., a notebook computer located in a hotel room).

3.10.2, lines 1508-1509
It would be helpful to clarify when and why physical access monitoring is required for publicly accessible areas within organizational facilities. Presumably, applicability of this requirement is limited to those publicly accessible areas containing system components that process, store, or transmit CUI based on the applicability limitations stated in Section 1.1 (lines 31-32). Based on that global statement of applicability, it would seem that 3.10.2 would only apply to publicly accessible areas that house (i.e., "provide protection for") system components that process, store, or transmit CUI.

3.10.6
The current wording implies that the security requirements for alternate work sites differ from those that apply to work sites in general. It is not clear whether the intent is that the security requirements that apply to alternate work sites are a superset of the 800-171 requirements (i.e., all other requirements still apply plus whatever is applied by the ODP in 3.10.6b) or a subset (i.e., only the requirements applied by the ODP in 3.10.6b). For example, is it required for organizations to "review physical access logs" (3.10.2b) for all work sites? Or is the organization allowed to eliminate this requirement for some work sites, such as the private residences of employees simply by designating those residences as "alternate work sites" under 3.10.6a and then omitting 3.10.2b from the list of requirements specified in the ODP for 3.10.6b? Is this option acceptable even if an employee works on CUI full time in their private residence? The Discussion section should clarify this ambiguity by explaining whether the requirements specified in the ODP of 3.10.6b are in addition to or instead of the requirements that apply to non-alternate work sites.

Also, the criteria to distinguish between a non-alternate work site and an alternate site is not clear. For example, the Discussion section (line 1533) says that "alternate work sites include the private residences of employees..." What if an employee works from their private residence daily? One day a week? Only when the weather is inclement? Intuitively one could consider the private residences of employees "alternate work sites" only if the employees do not work there on a regular basis (e.g., only during contingency operations). Since it is common for employees to work from their private residences on a regular basis (e.g., full time; one or more days a week; evenings/weekends as needed), it is valuable to provide organizations with guidance on whether such regular (i.e., non-contingency) use of private residences (and similarly coffee shops, hotel room, airplanes, etc.) should be designated as "alternate" or simply regular non-alternate work sites. Presumably the organization can, in addressing 3.10.6a, designate any of its work sites as "alternate work sites" (and by default the remaining work sites will be "non-alternate work sites"). It is unclear from the guidance provided why an organization can or should do this. Does designating a work site as "alternate" relieve them of some requirements? Or add additional ones? The Discussion section could illustrate the considerations a company might use to determine whether a site is to be designated as "alternate" or not, and how this affects the

applicable security requirements.

3.10.7
It is unclear whether the intent is for this requirement to apply to all physical locations containing systems or system components that process, store, or transmit CUI, or just such of those locations that are NOT designated as "alternate work sites" under 3.10.6. These requirements are difficult to implement for a number of non-traditional work sites, so organizations might surmise (out of practicality or convenience) that this requirement can be ignored for any sites they designate as "alternate work sites." Similarly, absent any criteria or explanation of what can and cannot be designated as an "alternate," they might designate any/all non-traditional work sites as "alternate work sites" without considering how regularly or routinely their workers work at those non-traditional sites. Absent any guidance or examples to the contrary, the interpretation that this requirement that effectively applies only to organization-controlled office space and not to non-traditional work sites is convenient and often adopted. The notion of "work sites" has changed since these requirements were first written, and the Discussion section should address non-traditional work sites explicitly since such are now common.

3.15.2, line 2038
SSPs typically contain not just an overview of the security requirements, but a complete enumeration of those requirements and how each requirement is implemented for the system. It is not clear why the SSP requirement in NIST SP 800-53 (PL-02) has been tailored to eliminate the requirement to "describe the controls in place or planned for meeting the security and privacy requirements..." as this is typically a fundamental purpose of an SSP.

3.16.2
The two requirements (3.16.2a and 3.16.2b) seem to be worded as alternatives. Is it the intent that organizations choose between these based on their own assessment as to whether the components can or cannot be replaced? Is it acceptable for the organization to determine that the component "cannot" be replaced simply because they find the cost of replacement higher than they wish to bear? The Discussion section states that "exceptions include...", but since this section is neither exhaustive nor normative, presumably organizations can make an "exception" to 3.16.2a for any reason they choose. If this is not the intent, the (normative) wording of the requirement should make this clear.

3.16.3
This requirement covers a wide range of different service provider arrangements with widely differing security requirements. Edge cases can be a significant source of confusion for implementers. The Discussion section could provide examples to help clarify the intended coverage of this requirement, illustrating how the ODP (3.16.3a) and the shared responsibility documentation (3.16.3b) can be used to determine and flow down appropriate, applicable CUI protection measures. The Discussion section could also clarify applicability in situations where external service provider personnel may have access to CUI residing on organizational systems (as contrasted with arrangements where CUI is processed, stored, or transmitted by the external service provider's own systems), for example service provider personnel and tools that remotely manage organizational IT systems where CUI access might occur incidentally. It would also be helpful to clarify applicability in situations where non-IT services are provided, for example personnel and equipment used to handle non-digital media (e.g., paper) containing CUI such as an archival storage or document destruction service provider.