From:	[redacted] via 800-171comments
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] Comments on NIST SP 800-171r3 initial public draft
Date:	Friday, July 14, 2023 7:17:06 AM
Attachments:	image001.png image002.png sp800-171r3-ipd-comment-Peak InfoSec.xlsx sp800-171r3-ipd-comment-Peak InfoSec.docx

---

Mr. Ross and Ms. Pillitteri;

Attached are our comments on NIST SP 800-171 Rev 3 Initial Public Draft. We have provided our comments in both the requested excel format and word for easier reading.

We do appreciate the work you all have done and we believe Rev 3 will benefit Non-Federal Organizations.

Thanks,

Matt

Matthew A. Titcombe, CISSP, CCA, CCP
Peak InfoSec – A SDVOSB & Authorized C3PAO
CEO & Information Security Consultant
[redacted]
https://www.peakinfosec.com/
[redacted]
[redacted]

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	2	30	Given that the callout box, "THE MEANING OF ORGANIZATIONAL SYSTEMS" section 3 in Rev 2 has been dropped, there is no longer traceability to the industry term "scope of applicability." This term should be added to this sentence.	Change the sentence from "The security requirements in this publication are only" to read "The Scope of Applicability for 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."
2	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	2	30	The term "system component" referenced here is overly IT centric. Given NIST SP 800-171 is primarily an information centric protection framework versus system centric (as normally implemented in FISMA accreditations), the term system should be expanded to be inclusive of the people, processes, facilities, and technologies used to process, store, or transmit CUI or protect it. By including this change, the approach becomes more consistent with systems engineering and architecture principles.	Change Note #9 from "Nonfederal systems include information technology (IT) systems, operational technology (OT) systems, and Internet of Things (IoT) devices." to "Nonfederal systems include the personnel, processes, facilities, information technology (IT) systems, operational technology (OT) systems, and Internet of Things (IoT) devices."
3	Matthew Titcombe; Peak InfoSec; [redacted]	Editorial	NIST SP 800-171 R3 IPD	2	31	With regards to note 10, the note fails to take into account external services, cloud services, and other capabilities a Nonfederal Organization may employ in the system.	Change Note 10 from "System components include workstations, servers, notebook computers, smartphones, tablets, input and output devices, network components, operating systems, virtual machines, database management systems, and applications." to "System components include workstations, servers, notebook computers, smartphones, tablets, input and output devices, network components, operating systems, virtual machines, database management systems, applications, cloud services, external services, and 3rd party providers that process, store, transmit, or protect CUI."
4	Matthew Titcombe; Peak InfoSec; [redacted]	Editorial	NIST SP 800-171 R3 IPD	4	77	The "Table 1. Security requirement families" does not include the family acronyms.	Update the table to include the family acronyms. For example, change "Access Control" to "Access Control (AC)"
5	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	4	89 & 92	Line 89 specifies "The discussion section is informative, not normative." However, line 92 describes references without the same follow-on language.	Add the following sentence to the end of the paragraph, "Unless specified in federal organization guidance, the refrences section is informative, not normative." The "unless" statement allows for use cases like ISOO specifying NIST SP 800-88 must be followed for sanitization procedures.
6	Matthew Titcombe; Peak InfoSec; [redacted]	Editorial	NIST SP 800-171 R3 IPD	5	114	This sentence is not in alignment to the one in para 1.1 (line 30). This sentence should be changes to reflect para 1.1.	Change the end of the sentence on line 114 from "the term system means a nonfederal system that processes, stores, or transmits CUI" to "the term system means components of a nonfederal system that processes, stores, or transmits CUI or that provide protection for such components"
7	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	6	189	The use of "web proxy servers" is an archaic approach to Zero trust architectures and should be removed.	Replace the term "web proxy servers" and replace with "proxy inspection service." See comment 18 for more info.
8	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	12	430	The sentence "The processing, storage, and transmission capability of mobile devices may be comparable to or a subset of notebook/desktop systems, depending on the nature and intended purpose of the device" implies that laptops are not considered mobile devices. This distinction is becoming less relevant with the comparative of devices like iPads versus a laptop being nearly synonymous to a Windows Surface "laptop" running Windows 10/11.	Change the definition in the glossary to include laptops and strike the sentence on line 430.
9	Matthew Titcombe; Peak InfoSec; [redacted]	Editorial	NIST SP 800-171 R3 IPD	15	524	This bifurcation creates a potential disconnect where a laptop doesn't have to meet the same protection requirements as an iPad.	Precede the term "Literacy Training" with "Information Security."
10	Matthew Titcombe; Peak InfoSec; [redacted]	Editorial	NIST SP 800-171 R3 IPD	21	783	The term "Literacy Training" is confusing. Unless preceded by an adjective, the normal interpretation is the "ability to read and write." When preceded by an adjective, literacy now means "able to use and understands..."	This should be reworded to be inline with NIST SP 800-128 para 2.1.1
11	Matthew Titcombe; Peak InfoSec; [redacted]	Editorial	NIST SP 800-171 R3 IPD	23	863	Given that NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, defines configuration items as "An aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process" whereas configuration settings is defined as "The set of parameters that can be changed in hardware, software, and/or firmware that affect the security posture and/or functionality of the information system," it is unclear why his control focuses on settings versus items, especially when it is recognized a baseline configuration is made up of configurations items which in turn are comprised of configuration settings.	Given in line 875, the term is broadened to "essential organizational missions, functions, or operations," it is recommended mission be struck form the line and the sentence changed to "Configure the system to provide only essential capabilities."
12	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	26	959	The term "mission" in the statement "Configure the system to provide only mission-essential capabilities" is contradictory to business terminology.	The sentence on line #959 should be changed from "Identify and document the location within the system where CUI is processed and stored" to "Identify and document the physical and technical locations within the system where CUI is processed and stored." Add the following sentence to the discussion. "Identifying system components where CUI is being processed or stored by users should take into account the business processes, physical assets, and t h l h "
13	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	27	1026	Given the inclination to "techify" the term system, this new requirement should take the larger systems engineering perspective, especially in line with line #960. If this remains tech system centric, physical storage locations for CUI may not be accounted for.	Change the sentence on line 1026 from "Implement multi-factor authentication for access to system accounts" to include an ODP and rephrased to "Implement multi-factor authentication for access to all individual and [Selection organization-defined system account types] account types." And, in the Discussion, the sentence from 3.1.1, "System account types include individual, shared, group, temporary, system, guest, anonymous, emergency, developer, and service" should be restated for clarity
14	Matthew Titcombe; Peak InfoSec; [redacted]	Editorial	NIST SP 800-171 R3 IPD	38	1439	Given the Security Requirement in 3.9.2 does not discuss exist interviews as a requirement, there is a disconnect between the requirement and the Discussion block.	Include the need for exit interviews by adding "a.4. Conduct exit interviews to inform departing personnel they are still required to not share knowledge of CUI they may have and other applicable topics."

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
15	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	39	1477	Given the statement in the Discussion, "Authorization credentials include ID badges, identification cards, and smart cards," the requirement to "Issue authorization credentials for facility access" may force non federal organization to implement legacy technologies where they are using Bluetooth and other technologies to issue physical access credentials.	Change the sentence in the discussion from "Authorization credentials include ID badges, identification cards, and smart cards" to ""Authorization credentials may include ID badges, identification cards, and smart cards."
16	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	46	1717	The new requirement, "Use independent assessors or assessment teams to assess controls" does not define a frequency for 3rd party assessments or the qualifications of the assessing entities.	The requirement should be re-written from "Use independent assessors or assessment teams to assess controls" to include assignment ODPs. Suggest change could look like "Use [Assignment organization defined qualifications] independent assessors or assessment teams to assess controls on an [Assignment organization defined frequency]." Given the relationship to 3.12.1, it may be beneficial to merge this requirement into 3.12.1 as para b.
17	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	48	1815	The Discussion for this requirement dropped the descriptive language from Revision 2. As a result, the reader is not provided any understanding of what shared system resources are. To make matters worse, NIST SP 800-53 Rev 5 provides no further clarification.	Re-insert the following language back into the discussion "The control of information in shared system resources (e.g., registers, cache memory, main memory, hard disks) is also commonly referred to as object reuse and residual information protection. This requirement prevents information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to any current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. This requirement also applies to encrypted representations of information."
18	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	52	1973	The use of the terminology "proxy server" and related methodology in the 3.13.17 requirement, "Route internal network communications traffic to external networks through an authenticated proxy server." Is an archaic design." Proxy servers have been replaced by Next Generation Firewalls (NGFW) that include proxy inspection services and even cloud-based solution (e.g., Zscaler) that extend the protection to remote devices. Furthermore, Endpoint Protection is also providing URL filtering and threat prevention services under a Zero Trust Architecture. The requirement should be updated to reflect the desired outcome, not a legacy technical method.	Change the requirement from "Route internal network communications traffic to external networks through an authenticated proxy server" to "Route internal network communications traffic to external networks through an authenticated proxy inspection service to inspect and identify malicious threats from the internet.".
19	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	53	2008	The sub-requirement, "b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation." is really an availability centric requirement and does not provide significant confidentiality or integrity-based benefits.	Remove the sub-requirement, "b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation."
20	Matthew Titcombe; Peak InfoSec; [redacted]	Editorial	NIST SP 800-171 R3 IPD	54	2028	A negative side-effect of using Cloud Service Providers (CSP) and other external services is organization tend to forget they are still required to implement malicious code protections in there locations or ensure their provider has.	Add to the discussion the following sentence, "Organizations should ensure all components that process, store, or transmit CUI or protect CUI are also protected with malicious code protections.
21	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	56	2114	Given the requirement does not discuss the need to protect against phishing attacks scattered amongst Spam, implementing Spam protection is a pure availability function. As written, this requirement should either be re-written or removed.	Recommend changing the requirement from "a. Implement spam protection mechanisms at designated locations within the system to detect and act on unsolicited messages. b. Update spam protection mechanisms [Assignment organization-defined frequency]." to a. Implement phishing/spam protection mechanisms at designated locations within the system to detect and act on unsolicited messages. b. Update phishing/spam protection mechanisms [Assignment organization-defined frequency]."
22	Matthew Titcombe; Peak InfoSec; [redacted]	Editorial	NIST SP 800-171 R3 IPD	58	2199	The requirement's discussion describes a requirement implementation option, "The increased risk of using unsupported system components can be mitigated, for example, by prohibiting the connection of such components to public or uncontrolled networks or implementing other forms of isolation," for where an organization cannot implement neither sub-requirements a or b. The requirement should provide this as a vial option where an organization may be dealing with legacy technologies tied to legacy components still in use by federal organization (e.g., B-52 bomber, originally produced in 1952).	Change the sub requirements from "a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or b. Provide options for alternative sources for continued support for unsupported components." to "a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; b. Provide options for alternative sources for continued support for unsupported components; or c. Implement [Assignment organization-defined mitigation] for continued usage of unsupported requirements."
23	Matthew Titcombe; Peak InfoSec; [redacted]	Editorial	NIST SP 800-171 R3 IPD	59	2224	The new requirement, "3.16.3. External System Services" does not address the shared services responsibility between the organization and the service provider. This shared service responsibility is critical to accurately implementing the sub-requirement "b. Define and document organizational oversight and user roles and responsibilities with regard to external system services."	Change the requirement from "a. Require the providers of external system services to comply with organizational security requirements, and implement the following controls [Assignment organization-defined controls]. b. Define and document organizational oversight and user roles and responsibilities with regard to external system services. c. Implement the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis [Assignment organization-defined processes, methods, and techniques]." to "a. Require the providers of external system services to comply with organizational security requirements, and implement the following controls [Assignment organization-defined controls]. b. Define and document the shared service responsibilities between the organization and external system services. c. Define and document organizational oversight and user roles and responsibilities with regard to external system services. d. Implement the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis [Assignment organization-defined processes, methods, and

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
24	Matthew Titcombe; Peak InfoSec; [redacted]	Technical	NIST SP 800-171 R3 IPD	88	3046	Per Appendix C, Table 20. System and Communications Protection, the requirements from the Moderate security baseline to protect Domain Name Service (DNS) are labeled "Not Confidentially Oriented." While not confidentiality centric they are truly integrity centric and remain a common exploit by APTs for re-directing traffic and used for command and control. DNS compromise is a key-ongoing tenet of sustained compromise of an organization. To make matters worse, NIST stepped up the risk transfer of the requirements by changing the DNS protections from NFO to NCO in Revision 3. Organizations are even less likely to implement NCO requirements over the NFOs.	NIST should include the NIST SP 800-53 Rev 5 SC-20/21/22 requirement in the CUI baseline set of requirements.