From:	800-171comments@list.nist.gov on behalf of [redacted]
To:	800-171comments@list.nist.gov
Cc:	[redacted]
Subject:	[800-171 Comments] NIST 800-171 Rev3 Comments from SP6 Consulting, LLC
Date:	Friday, July 14, 2023 5:29:33 PM
Attachments:	image001.png NIST_171Rev3_SP6_Comments_Final.xlsx

---

Dear Dr. Ross,

SP6 wholeheartedly supports the National Institute of Standards and Technology (NIST) in its mission to develop standards and guidelines for providing adequate information security for all agency operations and assets. As a reliable partner to Defense Industrial Base (DIB) organizations spanning various sectors and clearance levels, SP6 proactively utilizes NIST's Controlled Unclassified Information (CUI) series of special publications to take protective measures for CUI and determine contractors' adherence to Federal requirements for protecting CUI.

SP6 feels strongly that there are ways to simultaneously accomplish what may be perceived as two competing priorities: strengthening security standards while reducing the burdens of time and cost associated with cybersecurity frameworks and compliance requirements which tie back to these frameworks. Seeing a clear need for support amongst the Defense Industrial Base, SP6 applied our cyber risk and compliance management capabilities to develop software focused on the NIST 800-171 security framework. The goal is to reduce the burden of Defense Federal Acquisition Regulation Supplement (DFARS) and Cybersecurity Maturity Model Certification (CMMC) compliance in overwhelmed organizations. This compliance software was specifically built to (a) automate much of the collection of information tied to DFARS and CMMC compliance and (b) provide real-time, continuous insights and scoring of any DIB organization's security posture and compliance adherence. Through real-time, machine generated evidence collection and security control validation, our mission is to increase the effectiveness of the DIB's continuous monitoring and continuous compliance strategy.

Beyond this, our expertise extends to consulting services including DFARS & CMMC-based security and compliance gap assessments, remediation services, and continuous compliance monitoring, all led by experienced Certified CMMC Assessors and Professionals. Our mission while providing this vital support is to actively facilitate increased compliance across contractors — all in a concerted effort towards the ongoing strengthening of national security.

To further our engagement in the continuous improvement of regulations and requirements, and remain valued contributors to not only our clients, but the DoD and CyberAB, we're eager to provide comments on the latest revision of NIST 800-171 (attached). We appreciate your consideration and look forward to future collaboration. If you have any questions or need additional information, SP6 can be contacted at [redacted].

Sincerely,

James Barge and the committed SP6 team

Jim Barge
Co-Founder
SP6
[redacted]
www.SP6.io

"*There are two ways to do something: the right way, or again*."

"*Be brilliant in the basics.*"
~ Jim Mattis, Call Sign Chaos: Learning to Lead


SP6

1	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	SP6	General	Publicatic	2	30	Recommend we provide clarity to ensure the industry understands the security requirements are NOT only applicable to components of nonfederal systems that process,	Update the definition of a Nonfederal system or of System Components on the footer to include the operating environment and/or controlled environments.
2	SP6	General	Publicatic	5	114	Directly aligns and affects Comment #1, giving the impression that a "system" is an Information Technology system instead of an Information System that may include a process in the physical world of writing down or diagraming CUI, sharing CUI using "sneaker-net," posting CUI on a hardcopy of a flyer, and storing hard copies of CUI in a filing system.	Suggest including the physical aspect of hardcopies of CUI.
3	SP6	Editorial	Analysis	5	131	Recommend disabling account activities to include upon notification of an individual no longer needing access to the system to include within [an organization-defined time period], not just "upon discovery." The requirement, as stated, makes the discovery activity that key enforcement mechanism which should be the compensating mechanism to discover dormant accounts that have been left in the environment due to an oversight.	Update from: g. Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks]. To: g. Disable accounts of individuals within [Assignment: organization-defined time period] from notification (in accordance with IAW 3.1.1[h]) and within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].
4	SP6	Editorial	Analysis	14	503	Recommend including an ODP to define the time allotted to remove the CUI upon discovery.	Review the content on publicly accessible systems for CUI [Assignment: organization defined frequency] and remove such information if discovered within [Assignment: organization defined period].

1	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
5	SP6	General	Analysis	14	501	Recommend removing the "Train authorized" individual from this requirement as this shall be covered within the Awareness and Training Family, under Role-based training or other component. This requirement should focus on identifying the authorized users and the applicable use cases to ensure CUI is not stored on publicly accessible systems.	[a] Identify individuals with access to organizational information systems that are publicly accessible and establish a (select at least one) policy, process, or procedure to ensure publicly accessible information systems do not contain CUI.
6	SP6	General	Analysis	17	604	The use of "specify" in requirement 3.3.1 suggests the organization will include specific details that are not covered within the ODP, and it will confuse the readers in trying to define the specifications required rather than "identifying and documenting" the required logs.	Consider replacing "Specify" with "Identify and Document" which will update the requirement to read: Identify and document the following event types for logging within the system: [Assignment: organization-defined event types]. This will improve readability and the specific requirements will be included within the ODP portion.
7	SP6	General	Analysis	5	120	For continuity, consider removing "Specify" from the requirement and invite the agency or federal contractor to include the criteria/specificity within the ODP portion.	Consider replacing "Specify" with "Identify and Document" to update the requirement to read "Identify and document authorized users of the system, group, and role membership, and access authorization: [Assignment: organization-defined event types].
8	SP6	General	Analysis	21	754	Requirement 3.3.9, Audit Information Access should have a direct traceability to 3.1.4 (AC-5) within NIST 800-171r3	Consider adding AC-5 as source control to align this requirement with the Separation of Duty Requirement.
9	SP6	General	Analysis	26	958	Requirement 3.4.11, information location, is not addressing hardcopy CUI or the physical location of the controlled information, which is part of the sentiment within NIST 800-171's reference of nonfederal systems and organizations, the latter referring to the operating environment.	Consider updating the objectives to a. identify and document the location [(i.e., physical and logical)] within the system where CUI is processed and stored. b. "Identify and document the users who have access to the system [and the operating environment] where CUI is processed and stored.

1	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
10	SP6	General	Analysis	26	972	Consider making the "locations that the organization deems to be of significant risk" an ODP. This ODP can protect the confidentiality of CUI Basic or Specified, based on the Federal Agengy's Limit Distribution statement (i.e., NOFORN, NOFORN/REL, etc...).	Consider making the "locations that the organization deems to be of significant risk" an ODP. This ODP can protect the confidentiality of CUI Basic or Specified, based on the Federal Agengy's Limited Distribution statement (i.e., NOFORN, NOFORN/REL, etc...).
11	SP6	General	Publicatic	31	1171	The reporting requirement feels incomplete without a specific requirement for timely reporting of incidents. This can cause similar confusion as the one we are experiencing today due to high-level requirements.	Recommend including the reporting requirement from NIST 800-53r5, IR-6[a] as an ODP to provide Federal Contractor with clarity in reporting requirements, especially when the Federal Contractor has CUI from various Federal Agencies: "a. Require personnel to report suspected incidents [Assignment: organization-defined cyber incidents] to the organizational [systems] within [Assignment: organization-defined time period]"
12	SP6	General	Analysis	32	1193	The incident response testing requirement can use further refinement. The test is missing what to do with the output from the IR Test, and we need clarity on what is considered a "capability." The incident response capability shall be defined IAW NIST SP 800-53r3, a combination of mutually reinforcing security and/or privacy controls implemented by technical, physical, and procedural means, typically selected to achieve a common information security or privacy-related purpose. This combination of controls includes all the security requirements within the 3.6 family.	Consider updating this requirement and objectives to include the following: 1. The output from the Incident Response Test shall be reviewed by [Assignment: organization-defined role(s)] 2. The Incident Response Test shall include a lessons-learned activity 3. The Incident Response Test plan shall test the following requirements at a minimum, 3.6.1, 3.6.2, 3.6.4.

1	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
13	SP6	General	Analysis	35	1295	This compound requirement, 3.8.1, can be rewritten to improve readability. Breaking the requirement into several statements will also help measure its successful implementation.	a. Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
14	SP6	General	Analysis	35	1320	System media that contains CUI shall be sanitized using approved and authorized methods. This requirement should ensure the organization meets the intent of the requirement by documenting the standards for sanitizing CUI system media explicitly.	Consider including an ODP to document the authorized methods for sanitizing the system media: a. Sanitize system media containing CUI prior to maintenance, disposal, release out of organizational control, or release for reuse; and b. Identify, Document, and enforce [Assignment: organization-defined sanitization techniques and procedures]
15	SP6	General	Analysis	37	1400	As written, the requirement makes encrypting backup of CUI the explicit requirement. The source control from 800-53, and the comment section of this revision, gives the organization the flexibility to protect the confidentiality of CUI at backup storage location with either encryption and/or alternate physical controls.	Consider updating the requirement to include "alternate physical controls." Suggested change: Implement cryptographic mechanisms or [Assignment: organization-defined alternate physical controls and procedures, encryption modules, or a combination of the two] to prevent the unauthorized disclosure of CUI at backup storage locations.

1	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
16	SP6	General	Analysis	42	1577	Requirement 3.11.1 has been diluted too much, making it more ambiguous than previously versions (171r2). Recommend updating the requirement to align with the previous version.	Consider the following: a. Periodically assess the risk of unauthorized disclosure resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. b. Assess supply chain risks associated with suppliers or contractors and the system, system component, or system service they provide c. Communicate the risk assessment results with [Assignment: organization-defined personnel or roles]. d. Update risk assessments (including supply chain risk) [Assignment: organization-defined frequency].
17	SP6	General	Analysis	45	1701	Continuous Monitoring needs to be more specific to ensure the requirement is measurable and achievable. By adding an ODP to define the frequency each security controls shall be monitor, we are inviting the organization to perform a risk-based approach to monitor the control effectiveness for those that are critical to protecting the confidentiality of CUI.	Recommend adding an ODP to better define the intent of the requirement. a. Develop and implement a system-level continuous monitoring strategy that includes ongoing Monitoring and assessment of control effectiveness. b. Establishing [Assignment: organization-defined frequencies] for monitoring [Assignment: organization-defined security controls] for assessment of control effectiveness.

1	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
18	SP6	General	Analysis	46	1717	3.12.5 is mainly focused on achieving impartiality, which is good, but equally important is ensuring the assessment team or assessors have the required skills and technical abilities to conduct a meaningful security controls assessment. I recommend we add an ODP to account for skills and abilities.	[a] Use independent assessors or assessment teams to assess controls. [b] Select the appropriate assessor or assessment team with [Assignment: organization-defined skills, technical expertise, or industry-recognized credentials] for the type of assessment to be conducted. [c] The control assessment report that documents the results of the assessment shall be reviewed by [Assignment: organization-defined individuals or roles] within [Assignment: organization-defined timeline].
19	SP6	General	Analysis	49	1835	The ambiguity in this requirement can make the implementation unnecessary taxing to organizations if applied at the wrong layer. Adding an ODP can help reduce its misinterpretation.	Propose updating to include an ODP to specify the requirement at the system boundary that defines the in-scope security domain: Deny network communications traffic by default, and allow network communications traffic by exception at [Assignment: organization-defined systems and system boundary]
20	SP6	General	Analysis	49	1869	This compound requirement, 3.13.8, can be rewritten to improve the approach to system design or it can be broken into two statements. Breaking the requirement two statements will also help measure its successful implementation.	propose the following: [a] Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission (in-transit) [b] Implement cryptographic mechanisms to protect the confidentiality of CUI while in storage (at-rest).
21	SP6	General	Analysis	53	2008	Flaw remediation needs more structure on what should the organization test vs. deploy, in a timely matter, following a a risk-based approach.	Consider including caveats to allow organizations to make risk-based decisions to address system flaws and vulnerabilities outside of a traditional cycle, including without proper documented testing. This will include addressing zero-day items.
22	SP6	General	Analysis	54	2058	Security alerts and threat intel feeds are only effective when we do something with the information, either report or recomment action.	Recommend we add an ODP to review relevant alerts within an organizational-defined time and report or take action based on the organization's risk-based approach.