From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Submission of 800-171 comment template
Date: Friday, July 14, 2023 10:06:00 AM
Attachments: CSP-AB_800-171_Final.xlsx

On behalf of the Cloud Service Providers - Advisory Board (CSP-AB), please see attached our comments on SP 800-171 Rev. 3

Best,

Laura

--
Laura Navaratnam
Executive Director
Cloud Service Providers - Advisory Board

www.csp-ab.com

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Line #*	Topic *	Comment *
1	CSP-AB	General		Clear and consistent CUI Guidance	NIST should help users understand the differences between 800-171 and other related NIST publications. An example would be the alignment of 800-171 and 800-172. Additional guidance on when which document applies could reduce confusion by DIB participants. Encourage NARA, DoD, and other agencies to clarify and provide additional guidance for contractors.
2	CSP-AB	General		Alignment of 800-171 to existing NIST documents and federal regulations	Align 800-171 with other procurement-related cybersecurity guidance. Examples include the Department of Defense CMMC 2.0 program and Homeland Security Acquisition Regulation - Safeguarding of Controlled Unclassified Information.
3	CSP-AB	General		Clarify flow-down of obligations between DIB prime and sub-contractors	NIST should provide additional guidance on what requirements apply at the prime and/or subcontractor level. DIB participants have uncertainty about whether and how prime contractors are expected to ensure subcontractor compliance.
4	CSP-AB	General		Responsible entity for organization-defined parameters (ODP)	Who is ultimately responsible for defining ODPs? Is the NIST intent to allow industry participants to define and manage ODPs based on the risk? Or is the intent the ability of federal agencies and contract officers to define ODPs? If the ODP will be the government agency for each contract, how should the DIB deconflict peramiters from one agency from the next? It is not scalable to expect the DIB to spin up a new enclave to accomidate ontracts with differing ODPs.
5	CSP-AB	General		Adherence for existing contracts	Is the new revision applicable for only new contracts? If the revision applies to existing contracts, what is the timeframe for adherence?
6	CSP-AB	General		Ability of small and medium size DIB organziations to meet requirements	With the DIB made up of hundreds of businesses providing technology and professional services to all federal agencies, NIST should consider the impact on of medium and small size businesses and their ability to adopt the 800-171 requirements.
7	CSP-AB	General		Independent Assessment	NIST should revise the definition of an “independent assessment” such that an organization can define internal controls to support conduct of the assessments by in-house employees.
8	CSP-AB	General		Supply Chain Risk Management section 3.17	NIST should align requirements in 3.17 in the software with NIST SSDF's software supply chain security requirements and provide a mapping as it provided for NIST 800-53.
9	CSP-AB	General	31	1.1 Overley broad statement	Existing scoping language is interpreted to be overly broad, resulting in all requirements applying to any component providing security functionality (such as NTP servers, log servers, and configuration management databases) without regard to whether the component could affect the confidentiality of CUI. Suggested change: Change "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." to "The security requirements in this publication are applicable to components of nonfederal systems that process, store, or transmit CUI. Security requirements may be performed by other components in order to protect CUI components. The intent of the NIST current language, and renewed emphasis on "or" in revision 3, is to enhance the security of CUI. However, by expanding the scope of applicability NIST is exceeding their authority under the regulations. NIST has been charged with defininng the security requirements for CUI assets and systems only. As currently worded it opens the door to massive scope expansion for the requirements that is unexecutable. Recommend modification to the language above.
10	CSP-AB	General	137	3.1.1 "Need to know"	Need-to-know is not the standard for access per 32CFR2002. It is lawful government purpose. Refer to 32 CFR 2002.16(a)(1)(ii). Recommend changing the langugage to lawful government purpose.
11	CSP-AB	General	148	3.1.1	Recommend inserting the word "may" before include.
12	CSP-AB	General	166	3.1.2	Consider whether the access control policies should be [Assignment: organizationally defined access control policies]
13	CSP-AB	General	181	3.1.3	Consider if approved authorizations should be [Assignment: organizationally defined approved authorizations]
14	CSP-AB	General	180-209	3.1.3	The discussion section for 3.1.3 does not mention CUI and focuses strictly on the technical aspects of flow control. It is important for organizations to actually control the flow of CUI in order to protect its confidentiality, and this control should include a combination of policy, procedure, and technical flow controls that support these policies and procedures. Recommend NIST add at least some language in the discussion to address this aspect of flow control.
15	CSP-AB	General	186	3.1.3	Recommend changing export-controlled information to CUI. Recommend inserting "may" in front of include.

16	CSP-AB	General	357-385	3.1.12	There are currently multiple different definitions in the NIST glossary for remote access. In particular, " Access by users (or information systems) communicating external to an information system security perimeter. Source(s): NIST SP 800-82 Rev 2" and "Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network. Source(s): NIST SP 800-53 Rev 5." These are two different definitions. In the modern context of commercial networks generally have components that communicate using external networks. Indeed, we would imagine that the Federal Government networks do as well in many ways that are not obvious to the system engineers and generally not considered "remote." Any organization with more than one location likely uses some form of external network for communication even if that is a dedicated leased line. From an OSCs perspective, if a centralized IT organization is accessing parts of the system from a device inside the system, even if that access transits an external network (a commercial ISP) it should not be considered remote. Request NIST for the purposes of NIST 800-171 Rev 3 adopt the first definition (from outside the security perimeter). This is a change from Rev 2, however the R2 definition drives "remote access" controls around systems and operations that are effectively in the world of modern distributed computing not remote. This change would allow these controls to (properly and to the benefit of better security) focus on truly remote connection from outside the system, to inside the system, rather than internal connections that happen to travel over fiber not owned by the organization.
17	CSP-AB	General	630-631	3 3.2	Audit record content. Specifying a physical location for "where" an event occurred will be extremely challenging if not impossible. This information can be developed and correlated but having it contained in each audit record event is not executable. Recommend striking "where" from the list of requirements. Likewise the identity of an individual impacted by an event can require correlative analysis and is not contained in every individual record. Recommend clarifying language that identifies that overall you want to capture all of these data elements so that through analysis when needed you can assessmble the story. It is not needed for each individual logged event to contain all of these data elements.
18	CSP-AB	General	645-646	3 3.3	The combination of 3.3.3b here with 3 3.2 definitely leads to a conclusion that every logged event must contain all of the data elements listed. It is necessary to capture logs that also do not contain all of these elements because they are not available at the appliance doing the logging. If for assessment purposes we must show that each event record must contain what type of event occurred; time; where; source; outcome; identity of an associated individual, subject, object, or entities. Location and identity of a individual are the most problematic. Again this information can be developed from the totality of the audit records/logs however clarifying language is needed to ensure this is not interpreted by organizations and associated assessors that this means all elements are required in each record.
19	CSP-AB	General	705-718	3 3.6	Audit record reduction. Does not directly impact protecting the confidentiality of CUI particularly the record reduction aspect. Recommend removal. It is a good thing to have and provides after the fact analytical capabilities to better examine and mine logs, however this after the fact capability does not really protect the confidentiality of CUI.
20	CSP-AB	General	871-872	3.4.6	As written seems to say that all identified ports, protocols, and functions must be disabled. Suggest ammending "identified in 3.4.6b" to "prohibited or restricted in 3.4.6b." for added clarity. Further in forming the assessment objectives for this following the rev 2 pattern, Ports are Restricted, Functions are restricted led to an assessor requirement for identification of all functions and a restriction of some functions; an identification of all services (as distinct from functions ports and protocols), and a blocking of some of those. Go through that process and try to break them all differently without, for example, using blocked ports to disable a function or protocol. This is both challenging and time consuming but not additative to security. Recommend in the formulation of the AOs leaving this rolled up rather than breaking down by each conjunction as the break down for assessment purposes leads to a lot of effort that does not promote information security or the confidentiality of CUI.
21	CSP-AB	General	895-922	3.4.8	Allow software by exception only. Recommend removal. Although CM-7(5) is now included in the Moderate baseline this is not a moderate control in commercial enterprise. Removal of the blacklist option for the control of software will represent a huge level of expenditure for implementation across commercial IT that is not set up to operate in this fashion. It will be equally challenging across large and small organizations although for different reasons. This should be reserved for 172 implementation and not implemented in 171.

22	CSP-AB	General	940-957	3.4.10	System Component Inventory. The discussion section of this adds considerable requirements that add nothing to the confidentiality of CUI. Saying that the inventory includes system components, and then system components = hardware, software, firmware, system name, software owners, software version numbers, hardware inventory specifications, software license information, machine names, network address (however, how can an IP address be included in the inventory when they are dynamically allocated?) date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location (every time an employee leaves work from home, does the location of their laptop in inventory rewuire updating?). In line 950 insert "may" between components and includes, as in "effective accountability of system components may include..." Also, "Inventory specifications **may** include..."
23	CSP-AB	General	1016	3 5.2	Insert the word "can" into "Systems use shared" as in "Systems can use shared…" in order to not seem to be mandating a particular technology to meet the strictures of the control. For example a small business might meet this control with physical security controls.
24	CSP-AB	General	1060	3 5.5	Insert the word "may" as follows "Characteristics that may identify…" It is unlikely the intent to mandate in the discussion a requirement to say "identify a foreign national" for every email address in the DIB. This is particularly complex for multinational companies.
25	CSP-AB	General	1072-1073	3 5.7	The CSP-AB does not recommend allowing spaces and all printable characters in passwords. Many legacy systems do not allow this and it will cause a large amount of problems while not meaningfully helping security. The exception process for contractors, unlike the government in accommodating legacy system requirements, is very difficult to obtain. This would prove to be effectively impossible for most. It would be better for security and more implementable to mandate a minimum password length, rather than a specific character that must be allowable in a password. An eight character password, unfortunately still the standard for many, with a space, is still an eight character password. Recommend inserting "including, where implementable, spaces and all printable..." Consider adding a para for min password length. 12-14 characters at a minimum. Further, this recommendation is a departure from the normal recommendations of not specifying how to implement, however in this case we feel warranted based on the significant impact to security, and relatively low cost to implement. This change (specify a length not a complexity requirement) is consistent with NIST research on how to best reduce risk against brute force password attacks.
26	CSP-AB	General	1090	3 5.7	Insert 'may' as in "passwords may include" in order to not mandate that all elements must be present in all lists
27	CSP-AB	General	1123	3 5.12	On change default authenticators prior to first use. This may often not be possible. For example, an individual receives a new router. It has a default password, Admin. They must login (first use) with the default password in order to change it to something else. From an assessment perspective, how do they prove "no first use" of a default? If an authenticator is something like a CAC card, how it be changed prior to first use? Similarly, with biometrics the thumb print cannot changed prior to first use. The goal is not to deploy the router with the default password still set. As worded though and when authenticator has been defined to mean many different things, this needs to be removed, moved, or reworded. One possible approach is the addition of "when possible." at the end of the sentence. Another would be to specify "change a variable default athentictor set on a system or device before use in a protected system."
28	CSP-AB	General	1234	3.7.4	Recommend remove the word "maintenance" to read "Prevent the removal of equipment containing CUI" This ensures it is not only maintence equipment that is prevented from being removed without being CUI checked but all equipment.
29	CSP-AB	General	1301	3.7.5	Insert "may" into "Physically controlling media may include…" otherwise the discussion could be interpreted to mandate a serialization, control, and check in and out of all digital and non digital media. So every printed piece of CUI paper would have to be numbered, entered into the CUI inventory, logged tracked etc. Note this is a higher requirement than applied to most classified information and classified digital media.
30	CSP-AB	General	1312-1315	3 8.2	The discussion section seems to expand the requirement to an interpretation that all CUI media must be serialized and accounted for individually. Recommend adding "May include conducting inventories".
31	CSP-AB	General	1320	3 8.3	Recommend adding "offisite" before maintence. Technically as written this says, "Sanitize system media containing CUI priori to maintence." If the organizations authorized CUI IT personnel access a system media this lays a requirement, regardless of their status of being authorized to view CUI, to sanitize the system. Recommend adjusting the wording to make it clear that this is before access by personnel who are not authorized for CUI, it must be sanitized.

32	CSP-AB	General	1337	3 8.4	As written this goes counter to the NARA guidelines for marking system media as contained in the NARA CUI marking guide, version 1.1 December 6 2016. It says specifically on page 23 "Media such as USB sticks, harddrives, and CD ROMs must be marked to alert holders to the presence of CUI stored on the device. Due to space limitations it may not be possible to include CUI Category, Subcategory, or Limited Dissemination Control Markings." Recommend changing this to "Mark system media containg CUI in accordance with NARA or other agency specific marking guidance."
33	CSP-AB	General	1354	3 8.5	This removes the capability to protect digital media during transport through physical protection mechanisms, for example a locked container. As written this moves the 800-53 requirement from organizationally defined media at rest, to all media undergoing transport. Recommend continuing to allow secure transport without encryption as an option. Operationally there are times when this is required particularly when moving from a contractor organization, to a government organization where the governments strict configuration controls do not allow for the capbility to be installed to decrypt the data.
34	CSP-AB	General	1400	3 8.9	The discussion section maintains the "or alternative physical controls" however the base security requirement only lists cryptographic mechanisms. Recommend the addition of "or alternative physical controls" to the base requirement.
35	CSP-AB	General	1474-1491	3.10.1	What happens when there is no facility? In the modern cloud world, no company is starting with on-prem systems. They are all cloud, and many in the current remote work environment have no corporate facilities at all, and are completely a cloud based system. How then can they issue authorization credentials for facility access? What if that facility only has a key, and not a badge reader? How are credentials created and issued when they simply lock the front door? As written this looks at the problem completely through the big governments lens and not through the lens by which busines often operates. "Authorization credentials include ID badges, identification cards, and smart cards." This essentially mandates that every company in the DIB have a badge system of some kind. That does not match the effective secure operation of small and medium sized businesses in many cases. Recommend moving this to an NFO.
36	CSP-AB	General	1601	3.11.2	Insert "potentially" into "when new vulnerabilities potentially affecting the system are identified." If how the vulnerability impacts the system is already known, it doesnt need to be scanned for.
37	CSP-AB	General	1620	3.11.2	Insert "should" into "organizations should consider"
38	CSP-AB	General	1632	3.11.2	Based on the 3.12.2 line 1685 comment, recommend inserting in the discussion section as an additional paragraph, "Vulnerability remediation should be tracked to identify all open vulnerabilities, their risk status, and for those under going remediation or mitigation the timeline for conducting that remedition or mitigation." This or similiar language as a substitute for mandating that vulnerability remediation be tracked on the regulatory manadated POAM as outlined in 3.11.4
39	CSP-AB	General	1638 -1652	3.11.4	Remove the language around POAM insertion. This begins to direct how an organization conducts their risk management process and thinks solely about Risks as IT risks, and appears to conflate risks and vulnerabilities. From a regulatory perspective it also clutters the use of the POAM as a mandated mechanism for recording and tracking control shortfalls. All risks are not control shortfalls nor are they things that can always be fixed or implemented; a mitigation could be ongoing indefinitely. Mandating inclusion in the POAM will cause issues with governance processes broadly in a way that does nothing to decrease the risk to the confidentiality of CUI.
40	CSP-AB	General	1665-1666	3.12.1	"and ensure compliance to vulnerability mitigation procedures." Recommend removal of this phrase. Vulnerability mitigation procedures are just one of the 110 security requirements/controls. This phrase here risks causing confusion.
41	CSP-AB	General	1675-1677	3.12.1	"Organizations can choose to use other types of assessment activities, such as vulnerability scanning and system monitoring, to maintain the security posture of the system during the system life cycle." Recommend removing this sentence. It implies that vulnerability scanning is a substitute for security assessment and that is NOT the case. Nor is the amorphous "system monitoring" a substitute for the required security assessment process.
42	CSP-AB	General	1684	3.12.2	Reword to be "actions to correct weaknesses or deficiencies in controls;" Control failures can be identified at times other than control assessments, like incident response. If a control failure is found, its correction should go on the POAM regardless of where it was found.
43	CSP-AB	General	1685	3.12.2	We note that this is in the CA-5 control, however recommend the removal of bullet 2. We do not think it prudent to mandate the inclusion of all vulnerabilities identified in the system in the POAM. Things like the DoD mandating that assessments cannot start until all POAM items are closed aside, even for a moderate sized organization at any given time this is likely thousands of entries. For large organizations potential 10s of thousands. The vulnerability management process should not be conflated with the controls management process.
44	CSP-AB	General	1710	3.12.3	Add the sentence, "Identified control failures should be added to the POAM as indicated in 3.12.2."
45	CSP-AB	General	1733	3.12.6	Insert "CUI exchange" in front of agreements. So not all agreements but specifically CUI exchange agreements.

46	CSP-AB	General	1782	3.13.1	Insert "may" prior to includes for "systems may include…" to prevent an interpretation of mandating universal implementation of the three listed restrictions
47	CSP-AB	General	1788	3.13.1	Insert "should" into "organizations should consider"
48	CSP-AB	General	1867-1888	3.13 8	The theme seems to be to require encryption at rest for all CUI. This seems to be a significant uplift from the 800-53 moderate requirement which mitigates this with an ODP. By way of example - firm A receives a properly encrypted emailed CUI document from our government sponsor. Firm A opens it and decrypts the email using our medium assurance token. After reviewing the file it is saved to the hard drive of a laptop with bitlocker encryption enabled that would only encrypt when the device was shut down. Based on the not in process standard, it would seem to drive a need for an additional FIPS validated encryption method that would protect the CUI when not in process. If this scenario were extended to servers and databases it coudl add considerable complexity to the CUI handling process across the DIB and exceed the implemented standard in government networks for CUI documents. We recommend that this requirement be reserved for certain types of CUI specified where needed and not be applied to all CUI basic.
49	CSP-AB	General	2001	3.14.1	Flaw Remediation "b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation" This does not directly impact the confidentiality of CUI. Side effects are not the problem of CUI confidentiality but of availability of the system. Effectiveness testing is beyond the capability of most commercial businesses so the testing that would be done could not more reliably determine that for example a zero day has been effectively patched than the testing conducted by the vendor producing the patch. In turn the delays for testing can easily, and do where they are performed, increase the risk for confidentiality because it delays the instillation of needed patches. This requirement will result in a net-negative security for businesses. Many businesses typically configure their systems to accept and install vendor security updates automatically. Automatic patching results in much quicker flaw remediation, which is very important. The vast majority of business IT departments are less qualified than their trusted vendors to test and filter patches. If you are using a vendor, this control means being upable to accept push updates from the vendor, but instead configuring an internal system to reject patches until the internal IT department manually packages them and pushes them to a test group, then to production. For a business, this 1) greatly increases latency before patching from ~12 hours to 15-30 days, 2) requires adding extra infrastructure to manage the process, such as a non-FedRAMP patch management solution, which increases the attack surface of the information system, 3) increases IT burden by at about many hours per week conducting testing activities that are less capable than those of the vendor in most cases. For a typical business implementing this requirement, the proposed benefit (testing patches to determine if they are malicious) is negligible. Unless an explicit control is