[redacted] [redacted]

From: Oaks, Amy E. [redacted]
Date: Tuesday, September 13, 2022 at 12:41:34 PM UTC-4
Subject: JHU/APL comments on 800-171
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>
Cc: Dinsmore, Peter T. [redacted], Hennick, Molly G. [redacted]

The CMMC team at JHU/APL respectfully submits the attached comments for consideration in updates to NIST SP 800-171/171A & NIST SP 800-172/172A. Below is a description of our comment matrix.

We have reviewed the existing NIST documents for protecting CUI in Nonfederal Systems and have the following comments. We have put our comments in the context of related 800-53r5 controls as well as recommendations from the Joint (FBI, NSA, CISA) Cybersecurity Advisory on Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology. Our goal in these comments is to better align NIST SP 800-171 to protect against this activity.

Our comment spreadsheet is arranged in several columns:

Col. A 800-53r5 control related to our suggested new requirement

Col. B Existing 800-171/172 requirement to which we suggest a requirement and/or discussion update

Col. C Suggested wording for change. The change might be an addition or an edit to an existing requirement. If Col B is not filled in, the suggested wording is for a new requirement. If Col B is filled in, it is an edit.

Col. D Our priority of the importance of the change. We recognize that the government needs to be judicious in the amount of change introduced in a new version. We suggest a stronger consideration to our higher priority items. Suggested new items are prioritized 1-12, suggested updates/edits are prioritized A-C. Please note we also have one “error” we suggest correcting.

Col. E Our rationale for why we believe this is an important change to the existing set of requirements/documents. Note this column may include suggestions for discussion points to be made on new requirements.

Col. F This represents the previous 800-171 analysis of the 800-53 moderate baseline and how the applicable control was considered in earlier versions of 800-171. It is context for our rationale of why a control is important for the protection of the nonfederal system, inclusion of new moderate baseline controls, or inclusion of controls “assumed” to be performed that practice has shown are not.

Col. G. This is the mapping to the Joint Advisory AA22-047A. It either shows the MITRE ATT&CK Technique described in the advisory that would be mitigated with the addition of this control, or the recommendation from the advisory that would be followed with the addition of the control.

Thank you,

JHU/APL Team

Suggested addition of 800-53 control to 171/172	Suggested update to reqt or discussion of existing 171/172	Suggested Wording	Priority	Rationale	171 App E NFO?	CISA Advisory Mapping?
SI-8	-	Employ spam protection mechanisms at information system access entry and exit points.	1	Spam and related phishing is often the initial vector for attacks against the confidentiality of data on an information system. Phishing is documented as a Russian technique against the DIB	NCO	T1589 - credential gathering T1566 - phishing
SC-7	-	Implement Domain Name System (DNS) filtering services.	2	This practice is not covered in 171 based requirements. (URL categorization is similar but not the same and not within 171). This might be a form of SC-7, but not clear which enhancement it would fall under. This is not covered under the DNS security controls. This is a specific form of boundary protection (SC-7) that helps protect against adversary action, specifically against links to known adversary domains in spam and phishing emails.	CUI	T1027- obfuscated files or URL shortening T1090.003 multi-hop proxy
SC-35 SC-44	-	Detect and mitigate potentially malicious email.	3	This is directly connected to preventing email attacks to architectures. CISA reports this as a primary problem. Cybersecurity professionals report this as a primary problem. If every company utilized detonation chambers, DNS filtering, and categorized web proxy filtering then the phishing issue of today would be greatly reduced. **Recommend discussion includes:** Utilize sandboxing (SC-44) as an option.	N/A	Partially in terms of training T15622.002.

AU-12(1)
AU-6(4)
	-	Collect audit information (e.g., logs) into one or more central repositories.	4	Centralized log management is essential to cyber operation and any advanced audit reviews. It is a CISA recommendation against the Russian adversaries targeting the DIB. Yes, it is currently in the high baseline, but is necessary to carry out any audit analysis.	not present	Recommendation to unify audit logs and to establish centralized log management

CP-9 CP-9(1)	-	Conduct backups of user-level and system-level information.	5	Backups are essential for protection from ransomware. The current 171 requirements cover protection of backups, but do not require the backups themselves. Need to ensure systems can be rebuilt from scratch from information on backups.	CUI and NCO (9(1))	backup listed as additional best practice
*-1 controls	-	Establish a policy for [each family] that defines the purpose, scope, and the roles and responsibilities of the policy activities; directs the establishment of procedures to carry out and meet the requirements of the policy; identifies any regulatory guidelines that the policy addresses; is endorsed by senior management and disseminated to appropriate stakeholders; and is periodically reviewed and updated.	6	Previously covered under NFOs but we know now that we cannot assume companies are doing this so we must make it a requirement.	Yes	None
*-1 controls	-	Document the procedures to implement the [each family] policy and periodically review and update the procedures.	6	Previously covered under NFOs but we know now that we cannot assume companies are doing this so we must make it a requirement.	Yes	None

PM-16	-	Receive and act upon cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.	8	Suggest adding this to 171 with consideration that there are 172 practices that build upon it. **Recommend discussion includes**: Ensure you are looking at "current" information from reputable sources.		
SA-22	-	Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.	9	SA-22 is now part of the moderate baseline and managing products at end of life is important for security. SA-22 only covers support and does not address the last sentence addressing the case of providing mitigations and restricting usage in lieu of support when no internal or external support is available. **Recommend discussion includes:** Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or provide either in-house or external support from an ESP for unsupported components. If no internal or external support is available, the organization provides mitigations and restricts usage of the product.	N/A	N/A

IR-4(12)
IR-4(4)
	-	Perform root cause analysis on incidents to determine underlying causes.	10	800-53 Rev 4 more closely addressed root cause analysis, it is not addressed as directly in Rev 5 however **it's still important to train organizations to get to the bottom of issues versus just treat the symptoms**.
				CA-7 CONTINUOUS MONITORING and AU-2 EVENT LOGGING facilitate a "security capability" that links to examples in the 800-53 content about root cause analysis.
				Recommend discussion includes: Analyze malicious code and other residual artifacts remaining in the system after the incident, correlate information to identify adversary TTPs, and determine if the failure of one security control can be traced to the failure of other controls.
					N/A	N/A

AC-17(2)	-	Implement cryptographic mechanism to protect the confidentiality and integrity of all network device management sessions.	11	If not protected, altering or obtaining the management information gives an attacker easy access to the underlying infrastructure to compromise the confidentially and integrity of information stored, processed, or transmitted on that infrastructure.	N/A	N/A
SA-11	-	Perform security assessments of all enterprise software developed and used internally and correct flaws identified during the assessment.	12	This is a scoped down version of SA-11 to address internally developed software and systems. Recommend SA-11 be added to 800-171 with the additional suggestion that they add "internally developed for internal use" to 800-171. SA-8, CM-11, and SI-7 also touch on this topic.	SA-11	N/A

-	3.14.3e objective B	Update objective B to the following logic: Systems and system components that are not included in **<3.14.3e_ODP[1]: systems and system components>** and are not included in the scope of the specified enhanced security requirements are segregated in purpose-specific networks.	**Error correction**	The objective B needs revision, to accurately capture the logic of the control and the assignment. Example: Assume the assignment is “**IoT Devices**.” Current wording of objective B when assignment statement is inserted: Systems and system components that are not included in **IoT Devices** are segregated in purpose-specific networks. Results in an automatic NOT MET because non-IoT devices are not segregated in purpose specific networks. Suggested wording of objective B when assignment statement is inserted solves the accidental logic error: Systems and system components that are not included in **IoT Devices** and are not included in the scope of the specified enhanced security requirements are segregated in purpose-specific networks.	-	-
-	3.6.1 (maps to IR-4, IR-8)	Add "predefined procedures" to requirement or discussion of 3.6.1	A	Organizations fail to help themselves by not having predefined procedures to handle incident response actions. On average this would greatly help organizations handle incidents when they are encountered.	Table E-8: IR-8 IR-1 (Incident Response Procedures)	CISA report shows there is nothing to handle this kind of item.
-	3.11.1 (maps to RA-3(f))	Add risk prioritization to requirement or discussion of 3.11.1 or add a new reqt to specifically cover prioritization.	B	Point is prioritizing risks. This is not fully covered in 3.11.1-3.11.3, specifically risk prioritization, categories, sources, and measurement criteria. RA-3(f) covers periodically updating the risk assessment. Not clear where the additional guidance on prioritizing risks would be placed hence the suggestion to modify 3.11.1 or create something new.	Table E-14 (RA-1 NFO) RA-3 is CUI only RA-5(1), RA-5(2), RA-5(5)	Nothing directly, but I would argue the CISA report is actually evidence that Risk Assessment needs to be performed to identify the items listed in the report. The whole report is describing the risks to organizations.
-	3.11.1 (maps to PM-9)	Add development of risk mitigation plans to the discussion.	C	800-53 directly discusses risk management strategy. CISA report discusses the risks to organizations without directly stating the risk assessment or risk mitigation plans are necessary. By the report existing, it is suggested that this is direct support for such actions.	Might be within Table E-14, but hard to say.	The CISA report encompasses part of a risk mitigation plan along with the implementation