From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] NIST SP 800-171 rev3 IPD comments
Date: Friday, July 14, 2023 2:17:47 PM
Attachments: sp800-171r3-ipd-comment_Silva.xlsx

Dear officials at NIST,

Attached you will find my comments on NIST SP 800-171 rev3 IPD for consideration. Please confirm that you received the spreadsheet showing 24 comments.

I will be glad to answer any questions or provide any additional thoughts upon your request.

Respectfully,

Roberto Silva
SAVI, LLC
[redacted]

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Roberto Silva SAVI, LLC	Technical	Publication	5	111	Small business and companies only needing to achieve CMMC Level 1 will be focusing on the 17 basic safeguarding requirements from FAR clause 52.204-21. In rev3 ipd these controls would be (3.1.1), (3.1.2), (3.1.20), (3.1.22), (3.5.1), (3.5.2), (3.8.3), (3.10.1), (3.10.3 withdrawn), (3.10.4 withdrawn), (3.10.5 withdrawn), (3.10.7 new), (3.13.1), (3.13.5 withdrawn), (3.14.1), (3.14.2), (3.14.4 withdrawn), and (3.14.5 withdrawn). One must keep in mind that these controls were codified in the FAR and were probably based on an earlier version of the SP 800-171.	Review the applicable controls to ensure consistency between FAR clause 52.204-21 and NIST SP 800-171 rev3. Ensure that rev3 does not unintentionally turn "basic" controls into more "advanced" controls that would unnecessary increase cost and complexity onto small businesses.
2	Roberto Silva SAVI, LLC	Technical	Publication	5	111	The rev3 ipd has not clearly delineated the basic protection requirements. Enhanced Controls are allocated in SP 800-53B for a Moderate baseline. DoD will be looking at the same SP 800-171 for setting requirements under CMMC for the different certification levels, and therefore rev3 needs to have flexibility in the controls for those who only require basic protection (maybe for CMMC Level 1) and for those who will need enhanced controls for a Moderate baseline to protect CUI (maybe for CMMC Level 2).	Clearly label and identify the basic safeguarding requirements akin to FAR clause 52.204-21 that would enable a company to implement and verify a basic baseline.
3	Roberto Silva SAVI, LLC	Technical	Publication	5	116	While Section 3.1 is all about Access Control, the wording for controlling or limiting access has been lost in the rev3 ipd.	Rename the title for 3.1.1 to "System Access -- Account Management"

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
4	Roberto Silva SAVI, LLC	Technical	Publication	5	117	Control 3.1.1 in rev3 ipd has removed the original wording that was in rev2. That previous requirement was codified word for word in FAR clause 52.204-21, and small businesses that only need to meet basic requirements will need to be able to specifically verify that they meet the requirement of limiting access to authorized users.	For control 3.1.1, bring back the original wording: "Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)." This should be the top bullet "a." and the other items under 3.1.1 would be supporting practices to help meet the overall requirement. Enable specific verification of the basic requirement.
5	Roberto Silva SAVI, LLC	Technical	Publication	5	125	Requirements 3.1.1(f) and 3.1.1(g) come from Control Enhancements SP 800-53 AC-2(3) and AC-2(13) and would therefore contribute to a Moderate baseline. DoD will be looking at the same SP 800-171 for setting requirements under CMMC for the different certification levels, and therefore rev3 needs to have flexibility in the controls for those who only require basic protection.	Clearly label 3.1.1(f) and 3.1.1(g) as Control Enhancements required for a Moderate baseline.
6	Roberto Silva SAVI, LLC	Technical	Publication	6	165	Control 3.1.2 in rev3 ipd has removed the original wording that was in rev2. This previous requirement was codified word for word in FAR clause 52.204-21, and small businesses that only need to meet basic requirements will need to be able to specifically verify that they meet the requirement of limiting access to authorized transactions.	For control 3.1.2, bring back the original wording: "Limit information system access to the types of transactions and functions that authorized users are permitted to execute." This should be the top bullet "a." and the other items under 3.1.2 would be supporting practices to help meet the overall requirement. Enable specific verification of the basic requirement.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
7	Roberto Silva SAVI, LLC	Technical	Publication	11	366	One situation where small companies seem to struggle interpreting cybersecurity controls is when they rely almost strictly on cloud-based computing (e.g. Google Workspace, Office 365, etc.) and do not own any internal servers or network systems. It would be beneficial if the discussion related to remote access would help guide contractors.	Provide guidance in the discussion section of control 3.1.12 for remote access for applicability when utilizing cloud-based computing services, and maybe more specifically what is the difference between control 3.1.12 and the other controls dealing with external services 3.1.20 and 3.1.21.
8	Roberto Silva SAVI, LLC	Technical	Publication	13	453	Control 3.1.20 in rev3 ipd has removed the original wording that was in rev2. This previous requirement was codified word for word in FAR clause 52.204-21, and small businesses that only need to meet basic requirements will need to be able to specifically verify that they meet the requirement of limiting connections to external systems.	For control 3.1.20, bring back the original wording: "Verify and control/limit connections to and use of external systems." This should be the top bullet "a." and the other items under 3.1.20 would be supporting practices to help meet the overall requirement. Enable specific verification of the basic requirement.
9	Roberto Silva SAVI, LLC	Technical	Publication	14	501	Control 3.1.22 in rev3 ipd has removed the original wording that was in rev2. This previous requirement was codified word for word in FAR clause 52.204-21, and small businesses that only need to meet basic requirements will need to be able to specifically verify that they meet the requirement of controlling CUI posted on public systems.	For control 3.1.22, bring back the original wording: "Control CUI posted or processed on publicly accessible systems." This should be the top bullet "a." and the other items under 3.1.22 would be supporting practices to help meet the overall requirement. Enable specific verification of the basic requirement.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
10	Roberto Silva SAVI, LLC	Technical	Publication	15	519	The discussion section for control 3.1.23 should be reviewed for consistency with controls 3.1.10 and 3.1.11. It appears that the new control 3.1.23 aims to force users to logout when they expect a long inactivity period. The discussion states that "Automatic enforcement of inactivity logout is addressed by 3.1.10". However, control 3.1.10 sounds like it is for locking the session which is not the same as logout.	Change discussion sentence in control 3.1.23 to say: "Automatic enforcement of inactivity logout is addressed by 3.1.11."
11	Roberto Silva SAVI, LLC	Technical	Publication	18	648	Small companies that use external services like cloud-based computing (e.g., Google Workspace, Office 365, CUI enclaves, etc.) will depend on the service provider to implement the logging controls. The rev3 ipd does not seem to address a requirement to make logs available or to provide the logs as required.	Add requirement under control 3.3.3 (or somewhere under 3.3) to specifically force a company or service provider to make audit logs available and not just retaining them. Add requirement to read like this: "d. Make audit records and logs available and accessible to audit authorities as required by law or regulation."
12	Roberto Silva SAVI, LLC	Technical	Publication	21	788	Monitoring and controlling configuration settings sounds like a requirement that falls under configuration change control.	Delete requirement under control 3.4.2 bullet c "Monitor and control changes to the configuration settings in accordance with organizational policies and procedures." This requirement is already covered under control 3.4.3.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
13	Roberto Silva SAVI, LLC	Technical	Publication	27	993	Control 3.5.1 in rev3 ipd has removed some of the original wording that was in rev2. This previous requirement was codified word for word in FAR clause 52.204-21, and small businesses that only need to meet basic requirements will need to be able to specifically verify that they meet the requirement of identifying users, processes, and devices. It was noted that in rev3 ipd the device identification was separated onto control 3.5.2. This separation between user (3.5.1) and device (3.5.2) is likely more efficient. However, original text did not have "Re-Authenticate".	If reasonable, recombine the original rev2 controls for 3.5.1 and 3.5.2 under one control for more direct correlation to FAR clause 52.204-21. For control 3.5.1, clearly label or clarify that requirement "a." is the basic control needed, and that "b." is an additional enhancement for advanced protection of CUI or for Moderate baseline. Enable specific verification of the basic requirement. Avoid unnecessary costs for small companies to implement more advanced controls. Unless Re-authenticating is something that current operating systems do anyways
14	Roberto Silva SAVI, LLC	Technical	Publication	31	1158	Incidents should be defined for a user to know what is reportable or to understand what incidents require action. This would support control 3.6.4 Training.	For control 3.6.1 add a requirement something like this: "d. Define [Assignment: organization-defined reportable incidents] the types of incidents that must be reported and that require action."
15	Roberto Silva SAVI, LLC	Technical	Publication	35	1320	Control 3.8.3 in rev3 ipd has modified some of the original wording that was in rev2. This previous requirement was codified word for word in FAR clause 52.204-21. It was noted that in rev3 ipd the rewritten control 3.8.3 is actually an improvement on the original text. However, the original codified text contains "destroying" media.	For control 3.8.3, reintroduce the word "destroy" from the original text to maintain consistency with FAR clause 52.204-21. The requirement should read something like this: "Sanitize or destroy system media containing CUI prior to…" Enable specific verification of the basic requirement.
16	Roberto Silva SAVI, LLC	Technical	Publication	36	1339	The "b." requirement under control 3.8.4 states that exemptions to marking CUI on media would be defined by the company. However, the discussion does not articulate why exemptions are allowed or justified. It would seem CUI data that needs to be marked should always be marked.	For control 3.8.4, delete requirement "b. Exempt [Assignment: organization-defined types of system media containing CUI] from marking if the media remain within [Assignment: organization-defined controlled areas]."

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
17	Roberto Silva SAVI, LLC	Technical	Publication	37	1374	Companies often encounter unexpected media when travelling or presenting information to customers or partners outside of the company environment. For example, many monitors or T.V. displays now are "smart devices". It would be good to have discussion or guidance on the risks those devices may or may bring.	Provide in control 3.8.7 or where appropriate control guidance for connecting to display devices such as smart displays that may not be within the cybersecurity control of an organization.
18	Roberto Silva SAVI, LLC	Technical	Publication	39	1474	Control 3.10.1 in rev3 ipd has removed the original wording that was in rev2. This previous requirement was codified word for word in FAR clause 52.204-21, and small businesses that only need to meet basic requirements will need to be able to specifically verify that they meet the requirement of limiting physical access.	For control 3.10.1, bring back the original wording: "Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals." This should be the top bullet "a." and the other items under 3.10.1 would be supporting practices to help meet the overall requirement. Enable specific verification of the basic requirement.
19	Roberto Silva SAVI, LLC	Technical	Publication	41	1530	New control 3.10.7 in rev3 ipd combined three original controls from rev2. These previous requirements 3.10.3, 3.10.4, and 3.10.5 were codified word for word in FAR clause 52.204-21, and small businesses that only need to meet basic requirements will need to be able to specifically verify that they meet the requirement of escorting visitors, maintaining audit logs, and controlling physical access devices. It was noted that the new combined control 3.10.7 mostly maintains the original requirements under sections 3.10.7 b., c., and d. Combining them may be efficient. However, 3.10.7 includes text to enforce access authorizations which seems more appropriately addressed under 3.10.1.	Move control 3.10.7 requirement "a.1 Verify individual access authorizations before granting access to the facility." over to 3.10.1. Delete control 3.10.7 entire requirement "a". Defining what entrance/exit to use and what types of locks or guards to use should be NFO. Enable specific verification of the basic requirement.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
20	Roberto Silva SAVI, LLC	Technical	Publication	42	1580	Organizations should document their risk processes in a risk management plan (RMP). This helps the organization identify and handle risks in a standardized and consistent manner, and it is also a good project management practice. Granted that control 3.17.1 calls for a supply chain risk management plan, the organization should still have an overall RMP and supply chain risk management would be a subset.	For control 3.11.1, add requirement something like this: "c. Generate a Risk Management Plan (RMP) to document how cyber risks are found, evaluated, tracked, and dealt with. The RMP should include possible risk sources and categories, an impact/probability matrix, and how the organization plans to reduce risks."
21	Roberto Silva SAVI, LLC	Technical	Publication	47	1769	New control 3.13.1 in rev3 ipd combined two original controls from rev2. These previous requirements 3.13.1 and 3.13.5 were codified word for word in FAR clause 52.204-21, and small businesses that only need to meet basic requirements will need to be able to specifically verify that they meet the requirement of protecting boundaries and implementing subnetworks. It was noted that the new combined control 3.13.1 mostly maintains the original requirements under sections 3.13.1 a. and b. Combining them may be efficient. However, the original codified text contains "Protect" boundaries.	For control 3.13,1, reintroduce the word "protect" from the original text to maintain consistency with FAR clause 52.204-21. The requirement should read something like this: "a. Monitor, control, and protect communications…" Enable specific verification of the basic requirement.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
22	Roberto Silva SAVI, LLC	Technical	Publication	53	2006	Control 3.14.1 in rev3 ipd has removed some of the original wording that was in rev2. This previous requirement was codified word for word in FAR clause 52.204-21, and small businesses that only need to meet basic requirements will need to be able to specifically verify that they meet the requirement of correcting flaws in a timely manner. Also, 3.14.1 introduces advanced requirements above the basic requirement to include testing software and firmware updates which would be costly or impractical for a small business to implement.	For control 3.14,1, reintroduce the original text to maintain consistency with FAR clause 52.204-21. The requirement should read something like this: "a. Identify, report, and correct system flaws in a timely manner." Clearly label or clarify that requirement "a." is the basic control needed, and that "b." and "c." are for advanced protection of CUI or for Moderate baseline. Enable specific verification of the basic requirement.
23	Roberto Silva SAVI, LLC	Technical	Publication	55	2076	Rev3 ipd has removed control 3.14.5 that was in rev2. This previous requirement was codified word for word in FAR clause 52.204-21, and small businesses that only need to meet basic requirements will need to be able to specifically verify that they meet the requirement of performing periodic scans or real time scans of files.	Bring back the original control 3.14.5: "Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed." If efficiency is desired with the new combined control 3.14.2, then add the requirement there. Enable specific verification of the basic requirement.
24	Roberto Silva SAVI, LLC	Technical	Publication	60	2277	Supply chain management should also include identifying known suppliers that pose risks. For example, the Gov't is concerned about limiting software and apps from certain countries and companies.	For control 3.17.2, add requirement something like this: "b. Generate list [Assignment: organization-defined off-limits countries and suppliers] that are commonly known to pose cybersecurity risks or that outlawed by laws, contracts, or policies."