From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Pre-Draft Call for Comments: Protecting CUI
Date: Thursday, September 22, 2022 11:57:37 AM
Attachments: image001.png
NIST Comments.zip

Leidos Proprietary

My apologies,
The email was stopped in the outbox. Attached are comments from Leidos.

Thank you,
Jonathan

To create a request for CIS Compliance, click [redacted].
[redacted]

Jonathan E. Jowers | Leidos
Sr. Cybersecurity Compliance Principal | CIO Services
phone: [redacted]

ADVANCE SOLUTIONS | CIVIL | DEFENSE | HEALTH | INTELLIGENCE & HOMELAND

Please leave Tracking on

1. **Answer the following questions.** NIST wants comments in three areas: “Use of the CUI series”; “Updates for Consistency with SP 800-53 Revision 5 and SP 800-53B”; and “Updates to improve visibility and implementation.”

   On use, NIST asks for information on:

   - *How organizations are currently using the CUI series (SP 800-171, SP 800-171A, SP 800-172, and SP 800-172A)*
     a. *Org uses regularly uses 171a for internal assessment in preparation and validation of implementing NIST -171.*
     b. *Use 171 and 171a to understand the intent of the controls.*
     c. *Use 171 Help build the baseline for policies and procedures.*
     d. *Used -171 to cross reference other frameworks.*
     e. *Org uses -171 to evaluate 3rd parties, suppliers and subs.*
     f. *Org uses -171 control discussion sections to define (refine) scope for internal assessments.*
     g. *Org -171 to determine SMEs and documentation for ISO-27001*
     h. *Org use -171 to develop internal (non-DFARS) technical control sets.*
     i. *Org views -172 as future state.*
     j. *Org self-assessed to -172 to determine effort to meet -172.*
     k. *Org used -172a to understand (interpret) -172 controls.*
   - *How organizations are currently using the CUI series with other frameworks and standards (e.g., NIST Risk Management Framework, NIST Cybersecurity Framework, GSA Federal Risk and Authorization Management Program [FedRAMP], DOD Cybersecurity Maturity Model Certification [CMMC], etc.)*
     a. *Org -171 to determine SMEs and documentation for ISO-27001.*
     b. *Org uses other frameworks to map -171 controls.*
     c. *Org used -171 to map to AIA NAS9933 controls.*
     d. *Org used -171 to map to international frameworks.*
     e. *Org used -171 to prepare for CMMC.*
   - *How to improve the alignment between the CUI series and other frameworks*
     a. Better equivalency between NIST CUI Series with other NIST and non-NIST frameworks.
     b. Update -171 mappings to the new ISO 27001 controls.
     c. Update -171 to CSF.
     d. Update -171 to SP 800-53 Rev 5.
   - *Benefits of using the CUI series*
     a. Protect CUI.
     b. Conformity of security across the DIB.
     c. Win and keep contracts. (Revenue)
     d. Create defense to APT.
     e. Meets regulatory compliance requirements. (DFARS, FAR)
     f. Enterprise standardization of CUI baseline.
   - *Challenges in using the CUI series*
     a. *Lack of precise alignment between -171 and -53.*
     b. *Use of government language rather than industry technical language.*
     c. *Outdated technical terms. (Mainframe, etc.)*

Please leave Tracking on

d. *Too holistic, needs specificity.*
e. *Lacks clear definitions, and examples of solutions that meet the intent of the control. (Ex: -171 controls 3.13.4 Shared resources, 3.13.3 Mobile code)*
f. *Lacks applicability to control platform. (Ex: Application, Operation System, Database level)*

2. **Answer the following questions.** The pre-draft call asks for feedback on the "[i]mpact on the usability and existing organizational implementation (i.e., backward compatibility) of the CUI series if it were updated for consistency with SP 800-53 Revision 5 and the moderate security control baseline in SP 800-53B."

- When it comes to visibility, NIST wants input on:
- *Features of the CUI series should be changed, added, or removed. Changes, additions, and removals can cover a broad range of topics, from consistency with other frameworks and standards to rescoping criteria for inclusion of requirements. For example:*
  - *Addition of new resources to support implementation: The benefits and challenges of including an **SP 800-53 Control Overlay** and/or a **Cybersecurity Framework Profile** Appendix as an alternative way to express the CUI security requirements.*
  - *Separate -171 from SP 800-53 to ease updates and provide independence.*
  - *Scoping guidance for CMMC.*
  - *Including use of the same terminology for types of assets like "Security Protection Asset", "Specialized Assets..." (either use the terms CMMC invented or develop NIST ones with clear definitions).*
  - *NIST Definitions of what is a security protection asset.*
  - *Change to the security requirement tailoring criteria: Impact of modifying the criteria used to tailor the moderate SP 800-53B security control baseline (e.g., the potential inclusion of controls that are currently categorized as NFO – Expected to be routinely satisfied by nonfederal organizations without specification)*
  - *NFO is not a good category. Should be excluded or included, not subjective or assumed.*
  - *NFO should be rationalized and include.*
  - *NFO should be added to assessment criteria.*
  - *Any additional ways in which NIST could improve the CUI series*
  - *Create an automated assessment process. Eliminate inconsistency, subjectivity, continuous update to SSP. Ex: OSCAL for FedRAMP automation process.*
  -

*Type: E- Editorial, G -General T -Technical
Link: SP 800-171A

Comments for
NIST SP 800-171A

Please submit responses to: [redacted] by August 18, 2022

#	Organization Name	Submitted By	Type	Page #'	Starting Line #'	Ending Line #	Section #	Comment (Include rationale for comment)	Suggested Change
1	EXAMPLE Leidos	Jonathan Jowers	G	12	483	490	3.11.5e Assess the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence	Is the intent of this control to provide a prescriptive Organization Define Value (ODV) for control reviews?	Suggest changing the "at least annually" statement to "organizationally defined".
1							3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services	Remove "Non-essential". Keep assessment objectives: a, b, d, g, j, m, n, and o. Delete or combine objectives. For o combine l, i, f, and c into one. 	Delete or combine objectives accordingly.
2							3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	Separate architectural design from this control. Note: add to SP 800-171r2 comments.	Reword to simplify understanding of the control intent.
3		Leigh Musicof		24			3.4.1[e] the system inventory includes hardware, software, firmware, and documentation.	Remove firmware because it does not add to the security of a program to track this information, especially with how infrequently it is updated. What documentation is required to be inventoried?	Remove firmware and documentation.

4		Leigh Musicof		28			3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	Combine a-d and e-h to reduce the number of tests while maintaining the same level of security This will help reduce the burden of the people preparing the SSP.	Combine the number of tests to two. Remove Defined and Documented because implemented means it is defined and documented.
		Leigh Musicof		38			3.7.2 techniques used to conduct system maintenance are controlled.	This control is satisfied by 3.7.4, 3.7.5, and 3.7.6. It is also satisfied by 3.1.4 and 3.1.5.	Remove this control because it is duplicative, increases the workload, and does not enhance the cybersecurity of the program.

*Type: E- Editorial, G -General T -Technical
Link: NIST Special Publication 800-171r2

Comments for
NIST SP 800-171r2

Please submit responses to: [redacted] by August 18, 2022

#	Organization Name	Submitted By	Type	Page #'	Starting Line #'	Ending Line #	Section #	Comment (Include rationale for comment)	Suggested Change
1	EXAMPLE Leidos	Jonathan Jowers	G	12	483	490	3.11.5e Assess the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence	Is the intent of this control to provide a prescriptive Organization Define Value (ODV) for control reviews?	Suggest changing the "at least annually" statement to "organizationally defined".

1	Leidos	CIS-Compliance Team	G	37			3.13.4 Prevent unauthorized and unintended information transfer via shared system resources. (e.g., registers, cache memory, main memory, hard disks)	This is at the system operation level. If the OS does not provide full functionality to meet the intent of the control, what is the org responsibility to meet this control? Do procedures provide adequate security to meet the control. E.g., reboot OS, scripting to clear cache. "Shared system resources" is confusing and open to interpretation and needs to be defined much better.	Remove the control. This is a derived control. It is routinely met by OS and minimal cyber value is obtained via procedures to enforce an OS level control. No direct mapping to any other control framework. If you choose to keep the control, please use more examples in defining "shared system resources". More clarity in the control discussion about how an organization is to meet this control is badly needed.
2	Leidos	CIS-Compliance Team					3.1.22 Control CUI posted or processed on publicly accessible systems.	Systems that store, process or transmit CUI are not publicly accessible and have identification or authentication. This is a policy only control, not a technical control.	Remove the control. No direct mapping to any other control framework. Minimal cyber value is obtained.
3	Leidos	CIS-Compliance Team					3.13.7 split tunneling.	Please re-write this control because the way it is currently written is open to interpretation and it is causing confusion in the DIB.	Please be more descriptive with what NIST is actually recommending. External system needs to be more clearly explained with regards to CSP cloud.
5	Leidos	CIS-Compliance Team					Note: New NIST identity and authentication updates to align with -171 – 53B. (Laurie) 3.5.7	Please update the recommendations in this control to match current NIST password guidelines.	Please update the recommendations in this control to match current NIST password guidelines.
5	Leidos	CIS Compliance					3.5.10 Store and transmit only cryptographically protected passwords.	This is at the system operation level. If the OS does not provide full functionality to meet the intent of the control, what is the org responsibility to meet this control?	Remove the control

6	Leidos	CIS Compliance					3.5.11 Obscure feedback of authentication information	This is at the system operation level. If the OS does not provide full functionality to meet the intent of the control, what is the org responsibility to meet this control?	Remove the control
7	Leidos	CIS Compliance					3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems	Media is infrequently used in modern data centers and removable media is not allowed in NIST.SP.800-171. As it is currently written, this control does not add to the cybersecurity of a program or organization.	Remove the control or change the wording to “Check files used for diagnostic and test programs for malicious code before the files are used in organizational systems”.
8	Leidos	CIS Compliance					3.7.2 techniques used to conduct system maintenance are controlled.	This control is satisfied by 3.7.4, 3.7.5, and 3.7.6. It is also satisfied by 3.1.4 and 3.1.5.	Remove this control because it is duplicative, increases the workload, and does not enhance the cybersecurity of the program.
4									
4									

*Type: E- Editorial, G -General T -Technical
Link: SP 800-172

Comments for
NIST SP 800-172

Please submit responses to: [redacted] by August 18, 2022

#	Organization Name	Submitted By	Type	Page #'	Starting Line #'	Ending Line #	Section #	Comment (Include rationale for comment)	Suggested Change
1	EXAMPLE Leidos	Jonathan Jowers	G	12	483	490	3.11.5e Assess the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence	Is the intent of this control to provide a prescriptive Organization Define Value (ODV) for control reviews?	Suggest changing the "at least annually" statement to "organizationally defined".
1	Leidos	CIS-Compliance Team					3.1.1e Employ dual authorization to execute critical or sensitive system and organizational operations.	Comment: Important to know which operations require two-person control. Most administrative functions are not designed to support dual authorization making this control hard or impossible to implement at the point of change. Moving the control up stream into a change approval process would negate it's effectiveness since a single actor (the administrator) could still execute an	Remove control or modify according to the adjoining comment and rationale.
2	Leidos	CIS-Compliance Team					3.1.2e Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, remove the components or place	Does this prohibit cloud and cellular mobility (BYOD)? Often contracts require collaboration between multiple contractors including a prime and multiple subtractors. Depending on the nature of the contract it is often critical for more than one contractor's systems to access data in a shared collaboration system. Since the	Remove control or modify according to the adjoining comment and rationale.
3	Leidos	CIS-Compliance Team					3.4.2e Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of	Many companies already achieve this with tools l ke SCCM, JAMF, HPNA, etc… I believe this control would be more feasible to implement if it was written to give the implementor the option to only scope this against configurations and components that are critical to the security and integrity of the	Remove control or modify according to the adjoining comment and rationale.
4	Leidos	CIS-Compliance Team					3.6.1e Establish and maintain a security operations center capability that operates 24/7, with allowance for remote/on-call staff.	May not be as feasible for the smaller contractors. Those contractors may be able to make up for things with outsourcing, but outsourcing brings additional insider threat risks and also can lead to investigations with reduced context. Perhaps the discussion on this control can be written in a way that makes it clear that automated alerting and on-call	Remove control or modify according to the adjoining comment and rationale.

	Leidos	CIS-Compliance Team					3.6.2e Establish and maintain a cyber incident response team that can be deployed by the organization within 24 hours.	Similar to 24/7 SOC, this control is something the larger contractors all do today but may not be as feas ble for smaller contractors. That said, I still think this control would be necessary for the protection of highly sensitive CUI.	Remove control or modify according to the adjoining comment and rationale.
	Leidos	CIS-Compliance Team					3.11.2e Conduct cyber threat hunting activities on an on-going aperiodic basis or when indications warrant, to search for indicators of compromise in organizational systems and detect, track, and	This is very achievable for a larger company but would be very challenging for a smaller company. Threat hunting requires dedicated labor from highly skilled personnel. Smaller companies may either be unable to afford such talent or unable to allocate them to threat hunting tasks which are often fruitless if there is no compromise to detect.	Remove control or modify according to the adjoining comment and rationale.
	Leidos	CIS-Compliance Team					3.11.4e Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination.	Auditing the specific types and reasons for controls within 3rd party provides was a very high level of effort exercise that only resulted in point in time information. Team ultimately decided to depend largely on the less than ideal but industry standard SOC2 reports. I don't see how this is feasible for 3rd party providers given how challenging maintaining	Remove control or modify according to the adjoining comment and rationale.
	Leidos	CIS-Compliance Team					3.13.4 Employ physical isolation techniques or logical isolation techniques or both in organizational systems and system components.	Super high-level and therefore wide open for interpretation. One assessor could interpret this to say that using Windows is sufficient to meet the control because Windows provides different isolated profiles for each account. Another assessor could demand switch rather than VLAN isolation between CUI and non-CUI networks which would be very costly to	Remove control or modify according to the adjoining comment and rationale.
	Leidos	CIS-Compliance Team					3.14.5 Conduct reviews of persistent organizational storage locations at least annually and remove CUI that is no longer needed.	Heavily resist this control. We have had a very hard time getting any direction from COR's about what information is CUI and which information is not. As a result, we have fallen back to assuming anything that could be considered sensitive must be treated as CUI. We would need much more consistent and clear guidance from the customer on what is	Remove control or modify according to the adjoining comment and rationale.
		CIS-Compliance Team							

		CIS-Compliance Team							

*Type: E- Editorial, G -General T -Technical
Link: SP 800-172A

Comments for
NIST SP 800-172A

Please submit responses to: [redacted]
by August 18, 2022

#	Organization Name	Submitted By	Type	Page #'	Starting Line #'	Ending Line #	Section #	Comment (Include rationale for comment)	Suggested Change
1	EXAMPLE Leidos	Jonathan Jowers	G	12	483	490	3.11.5e Assess the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence	Is the intent of this control to provide a prescriptive Organization Define Value (ODV) for control reviews?	Suggest changing the "at least annually" statement to "organizationally defined".
1									
2									
3									
4									