From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] AIA Comments to NIST SP800-172 r3 IPD
Date: Thursday, January 16, 2025 5:31:47 PM
Attachments: AIA Comments - NIST SP 800-172 r3 IPD.pdf
Importance: High

Dear NIST –

AIA is pleased to submit the attached comments to the NIST SP 800-172r3 IPD.

Thank you for the opportunity to review and comment.

V/R

- Jason

Jason Timm | *Senior Director, Security & Enterprise Management*
AIA | [redacted]
aia-aerospace.org

January 16, 2025

National Institute of Standards and Technology
Computer Security Resource Center
Information Technology Laboratory
Email to: 800-171comments@list.nist.gov

RE: Call for Comments: NIST SP 800-172 Rev 3 IPD, *Enhanced Security Requirements for Protecting Controlled Unclassified Information*

Dear NIST:

On behalf of the Aerospace Industries Association (AIA)[1], I am pleased to offer the following comments in response to the call for public comment to NIST SP 800-172 Rev 3 IPD, *Enhanced Security Requirements for Protecting Controlled Unclassified Information:*

AIA's main concern revolves around segmenting. AIA is pleased to see the discussion of air gapping in Rev 1 has not continued in Rev 3. AIA believes that segmenting for specific functions or system(s), along the lines of segmenting end of life software, and using security boundary tools to protect and isolate them from the rest of the IT system is the best course of action.

If this is the intent of NIST, then AIA can work with DCMA and The Cyber AB to ensure the understanding is that isolation is not air gapping and that isolation is meant to isolate/separate specific types of assets such as end of life operating systems and in the case of CMMC Level 3, isolation is meant to isolate/separate Level 3 systems from the rest of the IT systems using boundary protection tools such as firewalls.

AIA believes that lessons learned demonstrate how requirements and processes in cybersecurity are mutually beneficial when shared through robust collaboration across sector business operations representing all stakeholders. AIA is committed to initiatives that secure information from cyber threats, and we continually work to encourage collaboration between industry and government on cybersecurity matters to include innovation, agility, and flexibility across all businesses and government entities supporting national and international missions.

Thank you for the opportunity to provide the above comments along with the enclosed comments matrix.

Sincerely,

Jason A. Timm
Senior Director, Security & Enterprise Management
National Security Policy Division

Enclosure: AIA Comment Matrix NIST SP 800-172r3

[1] Founded in 1919, the Aerospace Industries Association (AIA) is the premier trade association advocating on behalf of over 330 aerospace and defense (A&D) companies for policies and investments that keep our country strong, bolster our capacity to innovate and spur economic growth. AIA's members represent nation's leading aerospace and defense manufacturers and suppliers of civil, military, and business aircraft and engines, helicopters, unmanned aerial systems, space systems, missiles, equipment, services, information technology, and other related components.

1000 Wilson Boulevard, Suite 1700
Arlington, VA 22209-3928
703.358.1000

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	AIA	Administrative			Missing Critical Artifacts: The IPD should have been released with more artifacts such as the CUI Overlay to help identify changes and differences from NIST SP 800-53 and the prior version which would have helped in identifying concerns or other challenges/suggestions.	For future revisions, make sure that the initial public draft artifacts contain the baseline artifacts needed to provide constructive and informed comments. Examples are the CUI Overlay and assessment documentation.
2	AIA	Editorial			The interrelationship of requirements should be discussed even though these requirements are to be picked individually.	Provide guidance on the interrelationships between requirements if they are jointly selected especially related to impacts, costs, and operational challenges.
3	AIA	General			Privacy Considerations: What policies and operational requirements should the company implement or have in place to ensure error messages do not inadvertently disclose sensitive information, such as personally identifiable information? How will the Department of Defense leverage the technical leadership and standards provided by the Information Technology Laboratory's Special Publication 800-series to enhance the security and privacy of its information systems, ensuring alignment with NIST's guidelines for management, administrative, technical, and physical controls?	Privacy trainings to be mandatory for individuals handling PII and sensitive information. Implementation regarding - Employees managing this information and data should be aware of PII, sensitive information, and other Privacy related considerations.
4	AIA	General			Duplication with SP 800-171r3: Some requirements in SP 800-172r3 may overlap with those in SP 800-171r3.	Ensure the requirements are harmonized b/w both publications to avoid redundancy
5	AIA	General			Incomplete Guidance: Certain enhance security requirementes lack examples, leaving room for misinterpretation e.g. Systems and Communications Protection Encryption Standards: The requirement may mandate encryption of data in transit and at rest. Also there are differences in encryption algorithms specified in NIST SP 800-53 and NIST SP 800-172 r3	Validate inconsistences across publications. Also provide discussion / guidance section, similar to NIST SP 800-53
6	AIA	General			Inconsistent use of terms like "system boundary" or "security control families" compared to NIST SP 800-53	For future revisions, make sure to include consistency in terms definition
7	AIA	General			Access Controls: Establish and maintain an access control policy for systems containing CUI	Recommend specifying role-based access controls (RBAC) to ensure users have the minimal required access tailored to their specific job responsibilities. Additional context can be provided to highlight the importance of RBAC policies to prevent unauthorized access.

8	AIA	General			System and Communications Protection: Protect the confidentiality of transmitted CUI	The document should clarify which specific encryption protocols are suggested for securing data in transit (e.g., TLS 1.3 or IPsec). Highlighting specific protocols can help standardize the implementation and ensure robust protection.
9	AIA	General			Audit and Accountability: Record and maintain system logs for activities associated with CUI	Advocate for the integration with centralized logging solutions, such as SIEM (Security Information and Event Management) systems, to enhance the analysis, detection, and reporting capabilities of suspicious activities within system logs. Recommend mentioning the benefits of SIEM technologies specifically.
10	AIA	General			Access Control: AC requirements for privileged account management potentially overlap with requirements in SP 800-171r3. For e.g. requirement for multi-factor authentication appears multiple times for different scenarios (e.g. system access, remote access) without distinction in implementation details	Clarify the requirements and make sure there is consistency in the terms / definitions used.
11	AIA	General			Supply Chain: Enhanced requirements could contradict guidance from other federal supply chain standards	Clarify the requirements and provide references where appropriate. E.g. Mandating third-party certifications for suppliers. Guidance should be same across publications.
12	AIA	Technical			For all requirements that require automation, how can these be successfully implemented by SMBs without significant cost in technologies or resources? The original intent of the CUI series was to protect CUI that could be implement by SMBs but the requirements for automation (which could be justified due to the requirement) will have significant impact on the ability for SMBs to perform.	Provide more guidance and recommendations where any type of automation is identified as a requirement within the Requirement.
13	AIA	Technical			Data Protection: Ensure all CUI is encrypted at rest using FIPS 140-2 validated cryptographic modules	This requirement should be extended to specify encryption during the transit of CUI as well. Recommend adding verbiage that emphasizes the necessity of FIPS-approved encryption for data in transit to mitigate risks during data transfer processes.
14	AIA	Technical	10	439	03.01.02E: How will this negatively impact cloud implementations?	Most organizations, especially SMBs use cloud offerings or service providers and thus this will directly impact their ability to implement. This does not seem consistent with currently government initiatives or implementations.

15	AIA	Technical	11	463	03.01.04E: This requirement seems arbitary and undermines automation especially at a global scale.	Provide more context on how this would be implemented, especially on a global scale such that it can be monitored and controlled while also not impeding operational activities.
16	AIA	General	12	514	03.01.07E: Automated Actions for Account Management The verbiage on line 514-16: "The use of automated mechanisms to audit account management activities provides more timely and comprehensive data to guide and inform needed actions by system administrators"	Discuss SIEM as way to automate auditing in account management activities for mechanisms in account creation, modification, enabling, disabling, and removal actions
17	AIA	Technical	16	618	03:02:02E: Does this requirement force interactive training on users which will require additional costs and capabilities in many current training services?	Modify this to say "practical exercises or examples" to minimize costs and impacts to businesses and current training capabilities.
18	AIA	Technical	17	662	03:03:01E: How is this going to be successfullly implemented in cloud without forcing additional costs into other regions that may not meet other requirements such as non-US persons?	Provide more context on how this would be implemented, especially on a global scale and in the cloud that would not cause challenges with significant additional costs or forcing to other services in other regions that may conflict with other requirements such as US persons only requirements.
19	AIA	Administrative	20	743	3.4: Configuration Management Review and approve configuration-controlled changes to systems with CUI	It may be beneficial to incorporate a periodic review cadence to ensure changes are not only approved once but are continuously evaluated. Recommend specifying that configuration reviews occur quarterly in addition to approval of individual changes. This ensures compliance and addresses any overlooked changes.
20	AIA	Editorial	25	914	03.05.03E: Problems with the font on the requirement text	Make the text consistent with the rest of the document
21	AIA	Editorial	26	933	03:05:04E: The Title doesn't match the requirement and should be changed.	Change from "Embedded Unencrypted Static Authenticators" to "Prohibit Embedded Unencrypted Static Authenticators".
22	AIA	Editorial	26	948	03.05.05E: The requirement and the Title don't match.	Change the requirement to "Expire cached authenticators after [Assignment: organization-defined time period] and prohibit their use after expiration."
23	AIA	Technical	27	981	03.06.01E Security Operations Center: Establish and maintain a security operations center	Clarify if the SOC needs to define sufficient coverage such as 24x7 or 9x5 associate with the risk based approach and location requirements defined by the organization's policy.
24	AIA	Editorial	27	996	3.6: Incident Response "An SOC capability can be obtained in a variety of ways."	Remove the word "An"
25	AIA	Editorial	27	998	3.6: Incident Response "...third -party organizations to provide such a capability"	Change "such a" to "this". third-party organizations to provide this capability

26	AIA	Technical	30	1070	03:07:01E: How do we perform this requirement with external vendors who bring in maintenance equipment to perform required work on systems?	Provide additional guidance on how this could be performed given an external provider is coming to work on internal systems?
27	AIA	Technical	30	1084	03.08.01E: Dual authorization has signficant impact on the ability for all sizes of organizations especially small businesses to perform to the contract and can significantly increase costs. Can dual authorization approvals occur prior to execution such as via a change board?	Discussion should have some flexibility in how to implement beyond just requiring multiple approvals.
28	AIA	Technical	30	1084	03.08.01E: How will this work for removable media such as USB used in operational activities and not impact operational activities and performance?	More guidance on specific impacts especially in very large environments should be provided for common use cases such as USB or other rewritable media.
29	AIA	Technical	31	1107	03:08:02E: How does normal backup overwriting or reuse fall into this requirement?	More guidance should be provided on how this impacts backup procedures that overwrite previous backups on a normal schedule.
30	AIA	Editorial	31	1107	03.08.02E Dual Authorization for System Backup Deletion and Destruction: To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals	Consider changing to: To minimize the risk of collusion, organizations often rotate dual authorization responsibilities among various individuals
31	AIA	Administrative	32	1147	3.9: Personnel Security Line 1176: "Verify that individuals accessing a system processing, storing, or transmitting CUI are U.S. citizens."	CUI distribution is not limited to US citizens in accordance with 32 CFR Part 2002 and NARA guidance. Only CUI with additional limited distribution statements (e.g., NOFORN) are limited to US persons. Also, is "US citizens" correct.? For export controlled information, distribution is limited to US persons, which is different than a US citizen.
32	AIA	Administrative	33	1152	03:09:03E: What equates to "signing"? Does this include clicking OK or reading a banner and logging in?	More guidance should be provided on what is considered "signing" for access agreements that doesn't negatively impact operational activities.
33	AIA	Technical	41	1426	03.11.12E Automated Means for Sharing Threat Intelligence: Implement automated mechanisms to maximize the effectiveness of sharing threat intelligence information.	Clarify if the sharing needs to be automated for internal and/or external feeds or needs to be defined by the organization.
34	AIA	Technical	46	1580	03.13.02E: This requirement seems arbitrary and overly complicated and costly with even the discussion being all over the place on what it could be part of.	Remove the requirement or change to more about diversification and monitoring for abnormalities rather than just implementing "randomness" into an organization that directly impact effectiveness, scalability, operational efficiencies and increases costs. How does randomness differ from abnormalities when you have hundreds or thousands of random items and the SOC is monitoring?

35	AIA	General	47	1599	03.13.03E: Concealment and Misdirection Line 1599: "Use the following concealment and misdirection techniques to confuse and mislead adversaries"	Line 1600: "Organization-defined concealment and misdirection" tailoring techniques to the organization's specific needs can optimize resource allocation
36	AIA	Technical	50	1722	03.13.09E: How do we implement physical separation of subnetworks in cloud environments?	Physical isolation of subnetworks is not feasible or viable for validation in cloud environments and how would you validate or assess?
37	AIA	Editorial	52	1767	03.13.12E: ODPs should be italicized to be consistent with the rest of the document.	Fix the formatting of the ODPs
38	AIA	Technical	55	1879	03.14.04E: "Trusted sources include software and data from write-once, read-only media or from selected offline secure storage facilities."	Line 1879 "Trusted sources include software and data from write-once, read-only media or from selected offline secure storage facilities. **[ADD] Memory-safe programming languages encouraged."**
39	AIA	Technical	56	1887	03.14.05E: How would b. Delete information when no longer needed be impacted by the Dual Authorization requirement for Sanitization?	Provide guidance on the interrelationships between requirements if they are jointly selected.