From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] SP800-172r3 IPD Comments
Date: Friday, January 17, 2025 12:00:02 PM
Attachments: image001.gif
sp800-172r3-ipd-comment-template -SEI-APL.xlsx

Attached are combined comments from the SEI and JHUAPL on NIST SP 800-172 r3 IPD.

Please let us know if you have any questions.

v/r

Frank

Frank Smith, CISSP
Cybersecurity Team Lead
CERT Division
[redacted]

www.sei.cmu.edu | www.cert.org

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	SEI/APL	G	2	footnote 11	The definition for system components in footnote 11 and footnote 18 differ	Use the definition in footnote 18 in footnote 11 as it is broader. Delete footnote 18
2	SEI/APL	G	8	392		Reference footnote 11 instead of 18
3	SEI/APL	G	2	203	Availability/integrity which are key enhancements that 172 purports to address are not effectively considered with the current limited 172 r3 treatment of information recovery and restoration. 171 r3 includes only Backup (3.08.09). To be effective backup environments are required along with testing/ documentation. Experience with the loss of key systems/infrastructure from threat actors or disruptive events has proven how essential viable recovery/reconstiution solutions are to the nation, its people, and its economy.	Expand 172 r3 to include additional controls from the NIST 800-53 such as CP-04, CP-06, CP-09 (01), and CP-10. These recommended adds may not be the optimal mix or fully inclusive, but it would be worth additional consideration to explore how to best address availability/integrity exposures.
4	SEI/APL	T	10	440	The requirement for organizationally **OWNED** systems or components is overly prescriptive as many systems used by NFOs are leased, subscribed, GFE, or BYOD and while controlled and provisioned by the NFO, are not in fact owned by them. Language should reflect the broader way resources are acquired. Eliminate the ODP with broader language	change to : Restrict the use of systems or system components to process, store, or transmit CUI to only the systems or components which are provisioned, managed and controlled by or on behalf of the organization, which includes both organizationally owned and non-owned systems.

5	SEI/APL	T	21	774	Previous language was more direct to the requirement and did not rquire an ODP. As written the ODP requires an automated solution of the NFO's choosing which was what the previous requirement stated.	change to: Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components.
6	SEI/APL	t	23	877	Cryptographic bidirectional authentication is not always technologically possible especially within the IoT/OT environments. Requirement should allow for this limitation without the need to scope it within the ODP	change to: **Where feasible,** authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a system connection using bidirectional authentication that is cryptographically based.
7	SEI/APL	t	25	915	ODP is not required. Requiremnt for Device Attestation is sufficient.	change to: Implement device identification and authentication based on attestation
8	SEI/APL	t	47	1630	Isolation as used here is not a dictionary definition but rather reflects degrees of restiction that may range fron full physical isolation (air gap) to logical controls to prevent types or paths of traffic. Add a phrase that the degree of isolation should be based on the data being protected and the solution implemented chosen based on that	In the Discussion: update The degree of isolation varies depending on the mechanisms selected to: The degree of isolation varies depending on the mechanisms selected **and should be selected comensurate with the criticality of the data protected.**
9	SEI/APL	G	10	440	03.01.02E would imply that Cloud services should not be used, unless they are on a private cloud. If a private cloud is acceptable, then why not GovCloud?	Update: "Non-organizationally owned systems or system components include systems or system components owned by other organizations as well as personally owned devides." to append "unless they are approved systems maintaned at a same or higher security level"

10	SEI/APL	T	15	593	The discussion notes that anomalous behaviors can be almost anything and that the users should be aware of them. The ODP then allows to train on only a subset of behaviors. Shouldn't the users be aware of all the possible behaviors?	Remove ODP. (everything after and inculding "using")
11	SEI/APL	T	21	785	If one insistes on inculding "cost" into the list of things that must be tracked, "Replacement cost" would be of more value. Noting that a particular item was obtained for $10 back in 1972 through a deal of some sort is not going to be usefull in calculating impact. The current list comes across as prescriptive.	Add the word "can" between specifications and include.
12	SEI/APL	G	25	914	Does 03.05.03.E need to be met if the device meets 03.05.01E? This control appears to be to handle devices that cannot meet 03.05.01E.	
13	SEI/APL	G	27	988	Is there a more percise definition or implication of "a timely manner"? Is this within a week, 24 hours, etc... For example can I operate my SOC every Wednesday, or M-F 9-5? Or does it need to be a 24/7 operation? Will on-call for critical events be sufficient?	Update: "This requirement enhances SP 800-171 requirement 03.05.02" with "This requirement enhances SP 800-171 requirement 03.05.02 and can be used inconjuction with 03.05.01E for systems unable to support 03.05.01E."

14	SEI/APL	G	4	252	The use of external services providers is suggested as an option for implementing potential security solution. External service providers/outsourcing while a common and attractive option, represents one of most material risks to CUI/systems today. This risk is realized and evidenced by the ongoing breaches, failures, and disruptions that occur frequently in todays technology enviornmens.	Either add an additional assumption or add content to the existing assumption on line 266. That assumption/content should state that the use of external suppliers does not absolve organizations of accountability for managing CUI and risk. It should also be noted that the use of external service providers adds risks that require a comprehensive set of controls and oversight processses to ensure suppliers meet/exceed the security requirements established by the outsourcing organization.
15	SEI/APL	T	3	220	Including modern strategies in the example to ensure that the guidance aligns with modern IT/Cloud concepts and practices. Examples should avoid generalities, like the use of "other".	Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls, **software-defined perimeters (SDPs), micro-segmentation, zero trust network architectures,** and information flow control mechanisms). These techniques are particularly effective for dynamic and distributed environments such as hybrid IT and cloud infrastructures.
16	SEI/APL	T	4	271	Providing examples helps with clairty.	Include: Examples include secure enclave deployments, immutable infrastructure practices, automated patching pipelines, and cloud-native technologies such as serverless computing and containerized environments
17						
18						