

Kramer, Timothy L (59520) CIV USN NIWC [REDACTED] (USA)

Nov 25, 2025, 8:52:20 AM
to 800-171comments@list.nist.gov

All

Please find attached: the comment sheet for my review of NIST SP 800-172Ar3.

V/R,

Tim K.

Tim Kramer, CISSP, CEH

[REDACTED] 59520 / [REDACTED]
[REDACTED]

Comment #	Submitted By (Name/Org): *	Type (General / Editorial / Technical)	Starting Page # *	Starting Line # *	Comment (include rationale)*	Suggested Change*
1	Tim Kramer / USN/NAVWAR-NIWC-59520	T	8	330	"Non-organizationally owned" needs better definition. Does it mean that it's owned by a DoW org that is external to the ATO-defined security boundary or does it indicate that the system is owned by a non-DOW org?	Better identify what comprises "non-organizationally owned".

2	Tim Kramer / USN/NAVWA R- NIWC-59520	T	18	660	Need a definition of "unsanctioned CUI".	Better identify what comprises "sanctioned" and "unsanctioned" CUI.
3	Tim Kramer / USN/NAVWA R- NIWC-59520	T	21	755	CORs need to be included in the list of "responsible parties" identified for interview.	(Line 773) ... personnel with responsibilities for anti-counterfeit policies, procedures, training, and contracts.
4	Tim Kramer / USN/NAVWA R- NIWC-59520	E	26	921	Side question: should the requirement include the ability to manually add assets which aren't discovered via automation?	
5	Tim Kramer / USN/NAVWA R- NIWC-59520	E	27	957	Side question: Should there be discussion of specific tools having unique use cases. Examples: ACAS is good for network vulnerability scans but can't see inside of containers. Trivy or Clair is good for checking	

					dependencies internal to containers, Triy is also good for compliance scanning of Kubernetes architectures, etc.	
6	Tim Kramer / USN/NAVWA R-NIWC-59520	T	29	1018	A minimum period of time needs to also be declared. Stating "retain 3" when weekly changes are made means that a system would only have configuration data from the last month.	Example: "A minimum of 3 configuration backups, or configuration backups from the last 12 months (whichever comes last) are to be retained."
7	Tim Kramer / USN/NAVWA R-NIWC-59520	T	31	1382	Dislike "Dual Authorization" for sanitizing media. Would much rather see "dual accountability" for the action of sanitizing a given piece of media.	
8	Tim Kramer / USN/NAVWA R-NIWC-59520	T	40	1382	If the goal is to ensure that CUI is deleted once it's no longer useful, need 2-party validation that deletion was accomplished.	"Dual Validation" vice "Dual Authorization".

					"Dual Authorization" does not support such.	
9	Tim Kramer / USN/NAVWA R- NIWC-59520	T	41	1405	Same as above. If goal is to ensure that CUI is properly deleted, such is not accomplished via Dual Authorization.	"Validation" (or similar), vice "Authorization"
10	Tim Kramer / USN/NAVWA R- NIWC-59520	E	65	2164	Recommend a better definition of "thin node". Such implies booting over the network and is a bit vague on whether it's an end-users workstation or a server. In other words, "thin node" implies a server (esp. in a Kubernetes environment) while "thin client" implies a workstation.	
11	Tim Kramer / USN/NAVWA R- NIWC-59520	E	71	2370	Might be worthwhile to indicate that Github, Docker Hub, and Hugging Face	

					are not considered "Trusted Sources".	
12	Tim Kramer / USN/NAVWA R-NIWC-59520	T	74	2480	Stipulations in a product's FIPS Security Policy often includes the process by which initial crypto is loaded. It sometimes includes requirements for periodic inspection of tamper evident labels.	Examination and Testing should include any/all stipulations put forth in the product's FIPS Security Policy.
13	Tim Kramer / USN/NAVWA R-NIWC-59520	T	80	2666	In systems engineering, esp. Kubernetes, "tainting" is a preventive measure, where a taint prevents use of a node as a worker node. The verbiage in this section discusses a reactive/detect ive measure where exfiltration of CUI data is easily detected.	Use a term other than "Tainting".

14	Tim Kramer / USN/NAVWA R- NIWC-59520	T	89	2976	Section should include a statement that requires provenance to be maintained throughout the lifecycle of the product and/or data.	
15	Tim Kramer / USN/NAVWA R- NIWC-59520	T	90	3007	This is another section that should address the stipulations set forth in products' FIPS Security Policies and Common Criteria Validation Reports.	Add FIPS and CC requirements to the Examine and Test sections.