From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] NIST 800-171 Rev3 comment
Date: Friday, July 14, 2023 10:08:28 PM
Attachments: image001.png
image002.png
SP800-171r3-ipd-comment-template.xlsx

NIST Comment Board,

Thank you for the opportunity to comment on the NIST SPP 800-171 Rev 3 draft. My comments are attached.

Have a good weekend.

Very respectfully,

Bob "Clete" Boyer

Chief Compliance Officer
Export Control Official

Tactical Air Support, Inc.
www.tacticalairsupport.com

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Boyer / TAS	Editorial	Draft Rev 3	14	483	Telework can access files and applications through the secure web access and files are stored on the cloud server, not the external device	ADD, "or allow access through Web based application instead of desktop applications on external systems
2	Boyer / TAS	Editorial	Draft Rev 3	14	506	There is not clear classification guide when something is CUI, not as straight-forward as SP reads	Include guidance as to when something is CUI, similar to Security Classification Guides since the SP 800-171 is similar classified ATO controls.
3	Boyer / TAS	General	Draft Rev 3	15	533	There are a lot of SP categories with definitions when it reaches that SP level. LDCs are defined but don't match scenarios when contractor is producing the material that will become CUI	Discussion should include guidance or reference that provide explanation of SP and LDC that amplifies the Registry definitions. Example, release to contracts working on gov't staff but not releasable to other company contractors on the same contract
4	Boyer / TAS	General	Draft Rev 3	22	821	For medium-sized companies with a diverse business portfolio and a lot of small applications, is there a threshold for what needs to be logged, is it network wide applications, or does it include individual applications on devices	Configuration Change Management is applicable to network or enclave wide applications and software
5	Boyer / TAS	General	Draft Rev 3	31	1177	When an incident occurs is not straight-forward. Is it the report of potential that malware is on the network, is it when malware is found, is it when malware is discovered to have made changes to the network or when it pinged out data?	In discussion define thresholds for when an incident is deemed to have occurred.
6	Boyer / TAS	Editorial	Draft Rev 3	33	1235	When unclassified becomes CUI is not clearly defined, and unless marked, not always discoverable	Verify no known CUI on the equipment
7	Boyer / TAS	General	Draft Rev 3	33	1240	Discussion of how to sanitize. For CUI, is deleting and eShredding the drive sufficient. If a classified spillage on an SSD, it has to be shredded because eShredding isn't deemed sufficient	In discussion define what is acceptable sanitize for types of storage media
8	Boyer / TAS	General	Draft Rev 3	35	1320	Discussion of how to sanitize. For CUI, is deleting and eShredding the drive sufficient. If a classified spillage on an SSD, it has to be shredded because eShredding isn't deemed sufficient	In discussion define what is acceptable sanitize for types of storage media

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
9	Boyer / TAS	General	Draft Rev 3	36	1342	CUI markings are too long to fit on media, especially with multiple SP and LDC	Provide abbreviated CUI markings or allow for media to be marked CUI without any SP or LDC markings
10	Boyer / TAS	General	Draft Rev 3	38	1417	Discussion is very broad and in-depth screening activities that are not possible for new hires who immediately work on a company's network that is contains CUI. Companies don't have two enclaves, the whole domain is treated for CUI	Pre-hire screening should consist of a NACI or Security Clearance confirmation prior to accessing a company's network. On-going monitoring can include screening activities …….
11	Boyer / TAS	Editorial	Draft Rev 3	39	1475	Companies have one domain, if it's CUI, the whole domain is within a secure server. Developing a list of individuals with authorized access is everyone in the company	Develop, approve, and maintain a list of individuals with authorized privileged access….
12	Boyer / TAS	Editorial	Draft Rev 3	40	1493	Monitoring physical access to where network devices are would require a small-medium company to acquire expensive badging systems since the computers are in company spaces. Also, how does this apply for telework, that is in someone's home or off-site office	Monitor physical access to the facility wehre the system servers and/or network switches and devices reside….
13	Boyer / TAS	Editorial	Draft Rev 3	41	1520	The following section is Physical controls, but if alternative worksite, physical controls would be in employee's homes. This is written similar to a classified IS control.	Expand discussion to give consideration for employee residence telwork sites and temporary detachments which are not owned by the company
14	Boyer / TAS	General	Draft Rev 3	41	1531	Can't enforce physcial controls on employee's homes or when on a contract detachment to a facility that is not owned by the contractor or government. This control is written similar to a classified IS physical control, impractical for dispersed unclassifed network that is mobile	Expand discussion to give consideration for employee residence telwork sites and temporary detachments which are not owned by the company
15	Boyer / TAS	General	Draft Rev 3	42	1566	With dispersed CUI network that is mobile and in telework locations, can't put keypad or card reader access controls, and each room isn't locked, the building is locked	Expand discussion that building is locked and devices is either in closed room or inside a desk drawer. The bilding itself is locked.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
16	Boyer / TAS	General	Draft Rev 3	53	1994	Limiting the external network connections is challenging and impractical for a mobile and geographically dispersed workforce that also does telework. Each employee has mobile device and laptop and may access from different locations. If accessing the web and cloud servers, the connection can be secure without having to limit the number of access points	Limit the number of external network connections or allow access through web to secure server and cloud applications where the access point is immaterial and security is still maintained.
17	Boyer / TAS	General	Draft Rev 3	55	2084	With advanced applications, diagnostic feedback, external communications will occur that are not planned by individuals, but are automated responses and to locations not planned by the company. Will increase with AI.	In discussion, require software and application vendors to provide list of diagnostic and performance feedback automated transmission locations and file types so companies can better understand normal traffic. Currently can only compare to past history to look for new trends but don't know if new trend is malicious or new software/application
18	Boyer / TAS	General	Draft Rev 3	60	2283	A lot of these controls are cost prohibitive and/or not available or feasible for small- and medium-size businesses	Have the SBA provide assistance for small and medium - sized business
19	Boyer / TAS	General	Draft Rev 3	61	2307	A lot of these controls are cost prohibitive and/or not available or feasible for small- and medium-size businesses	Have the SBA provide assistance for small and medium - sized business
20	Boyer / TAS	General	Draft Rev 3	61	2326	Discussion should include proper disposal methods for different types of CUI. Does FCI, CUI, Export and CTI material all get disposed of the same way, and what is sufficient type of disposal for the different types of CUI items.	In discussion provide reference that outlines proper sanitization and disposal methods for different types of CUI and different CUI media/materials.