From:	'[redacted] via 800-171comments
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] Totem Technologies" comments on 800-171 rev 3 IPD
Date:	Thursday, July 13, 2023 12:45:58 PM
Attachments:	image001.png sp800-171r3-ipd-comments_Totem-Technologies.xlsx

Hello NIST,

Please find attached Totem Technologies' comments on the SP 800-171 Rev 3 IPD. Thank you for your consideration.

Very respectfully,

Adam Austin | Co-owner, CTO, and Cybersecurity Lead
Totem.Tech | [redacted]
[redacted]
www.totem.tech
[redacted]

*** Do not send Controlled Unclassified Information (CUI) in the body or as an attachment to this email address. If you have CUI you must send me, and do not have a method of secure transmission, please let me know and I'll provide an alternate transmission method. ***

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Adam Austin/Totem Technologies	General	SP 800-171 Rev 3 IPD	5	117	3.1.1 overall control descriptor text has changed from a single sentence ("Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).") to a list of -171A Assessment Objective-type of descriptors. The same is true of 3.1.4, 3.1.5, 3.1.6, and many other controls in rev3. This change will make the transition from rev2 to rev3 much more challenging for those of us used to a high level control descriptor, as the descriptor is filled with minutiae.	Continue the previous practice of a single sentence control descriptor and leave bulleted lists of control details to individual Assessment Objectives in -171A. As an example, in control 3.1.4, instead of "a. Identify the duties of individuals requiring separation. b. Define system access authorizations to support separation of duties. ", make a single sentence: "Identify organizational duties that require separation to different individuals, and apply system access authorizations to support that separation." Then leave the detailed action steps to the assessment objectives in -171A rev 3
2	Adam Austin/Totem Technologies	General	SP 800-171 Rev 3 IPD	8	232	3.1.1 and many other controls in rev 3 now have placeholders for organizationally-defined parameters (OPD). I understand the rationale to align the format of -171 closer to -53, and I understand the the Federal agencies mandating the use of -171 may choose to define the ODP. However, one of the things that makes -171 so wonderful was that it doesn't have so much of -- no offense -- "NIST speak". I.e. -171 is approachable and digestible by the 10s of 1000s of small businesses that must read it and digest it.	Continue the use of control language such as "the organization identifies privileged accounts" instead of convoluted phrasing such as "Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges."
3	Adam Austin/Totem Technologies	General	SP 800-171 Rev 3 IPD	1	21	rev 2 section 1.1 has a description of "isolated security domain" which has been very helpful in describing the concept of "enclaving" to small businesses, and which is referenced from the DoD's CMMC Scoping Guide. I don't see any references to isolated security domains anywhere in rev 3. This is a shame.	Include in rev 3 a description of how CUI can be protected within an isolated security domain.
4	Adam Austin/Totem Technologies	Editorial	SP 800-171 Rev 3 IPD	15	524	The phrase security "literacy" training is going to be lost on most readers/implementers of this standard. I've been a security professional for 14 years and I've never heard it referred to as "literacy" outside of NIST documents.	Suggest changing the phrasing of this control to something like: "Employ security awareness techniques and provide security training to all staff, and ensure staff are competent in security risks and their expected responsibilities." Maybe substitute the word "competence" for "literacy".
5	Adam Austin/Totem Technologies	Editorial	SP 800-171 Rev 3 IPD	17-21	603	If the first AU control is changed to refer to "event" logs, why is "audit" log used in the rest of the controls?	Suggest consistency: just refer to the logs as event logs or records (instead of audit logs or audit records), and the process of analysis of the event logs for anomalies as "auditing".
6	Adam Austin/Totem Technologies	Editorial	SP 800-171 Rev 3 IPD	20	729	Not sure why NIST removed the requirement for an authoritative time source for time stamps	Include the requirement for the organization to sync internal clocks to an authoritative time source for event log time stamp correlation
7	Adam Austin/Totem Technologies	Editorial	SP 800-171 Rev 3 IPD	21	785	Control 3.4.2 uses the phrase "that reflect the most restrictive mode consistent with operational requirements", but then no where in the description text is that phrase explained or elaborated upon.	Explain in the Discussion section of 3.4.2 what is meant by the phrase "that reflect the most restrictive mode consistent with operational requirements". Better yet, get rid of this phrase altogether, as most small businesses, even with interpretation from consultants, will not understand how to implement this. Just speak plain english: choose a hardening guide/STIG/benchmark, and then apply as much of it as you can without affecting functionality.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
8	Adam Austin/Totem Technologies	Editorial	SP 800-171 Rev 3 IPD	27	1016	The removal of the word "verification" from control 3 5 2, along with MAC address explicitly described as an identifier, implies that MAC filtering or whitelisting is no longer an approved method of device verification. But this is confused by the word "or" in this sentence, which seems to imply MAC addresses can be used as authenticators as well as identifiers: "Systems use shared known information (e g., Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers [IEEE] 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks."	Suggest clarifying if MAC address verification, through techniques such as MAC filtering or whitelisting, is still acceptable, and, in general, if device verification (as opposed to authentication) is not acceptable.
9	Adam Austin/Totem Technologies	Editorial	SP 800-171 Rev 3 IPD	52	1973	Control 3.13.17 is confusingly worded and simultaneously too specific.	"Route internal network communications traffic to external networks..." is confusing wording. Why not just make this control about content filtering services, instead of about routing? Specifically, proxy servers seem to be required, where I believe DNS filtering services may suffice to meet the spirit here, but are not proxy by nature.
10	Adam Austin/Totem Technologies	Technical	SP 800-171 Rev 3 IPD	38	1417	CUI screening requirements still too vague. The statement: "The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and criteria established for the level of access required for the assigned position..." does not help the average audience of this document, as there is very little guidance on what exactly the screening requirements are for access to CUI.	Please identify what exactly are the screening requirements for access to CUI. Does e-verify suffice? Background checks? If background checks are required, just state, or federal as well? Are convicted felons, assuming they've completed rehabilitation, allowed to access CUI. ISOO provides very little guidance on this. I'm hoping someone in the Federal gov't will step up the plate and provide explicit guidance.
11	Adam Austin/Totem Technologies	Technical	SP 800-171 Rev 3 IPD	49	1860	A VPN is described in the one example of how a split-tunnel can be "securely provisioned". However, "locking" connectivity to the VPN is actually preventing the user's ability to split tunnel, so this example is confusing.	Provide additional examples of how split-tunneling can be "securely provisioned", or do away with the allowance for secure provisioning.
12	Adam Austin/Totem Technologies	Editorial	SP 800-171 Rev 3 IPD	60	2277	Controls 3.17.2 and 3.17.3 are redundant. Identifying and implementing Acquisition Strategies, Tools, and Methods and Supply Chain Controls and Processes would naturally be part of a Supply Chain Risk Management Plan.	The Supply Chain Risk Management family needs one control: develop and implement a SCRM Plan. Controls 3.17 2 and 3.17.3 can be covered by assessment objectives of this one control.
13	Adam Austin/Totem Technologies	Technical	SP 800-171 Rev 3 IPD	85	3032	PE-6(1) "Monitoring Physical Access – Intrusion Alarms and Surveillance Equipment" in the tailoring criteria changed from NFO to NCO. Is this intentional, or a typo? Does NIST now believe now alarms and surveillance of the physical facilities doesn't contribute to the confidentiality of CUI?	Change the tailoring criteria for this control back to NFO.
14	Adam Austin/Totem Technologies	General	SP 800-171 Rev 3 IPD	multiple	multiple	Is it NIST's intent only to have 109 controls in rev 3? Multiple counts indicate only 109 controls whereas rev 2 had 110.	