From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] NIST SP 800-171 IPD Feedback
Date: Tuesday, May 23, 2023 1:43:26 PM
Attachments: sp800-171r3-ipd-comment-template-complianceforge.xlsx

NIST,

Attached is the feedback is on behalf of ComplianceForge for NIST SP 800-171 R3 IPD.

Respectfully,

Tom Cornelius, CISSP, CISA, CRISC, CDPSE, CIPP/US, PCIP, MCITP, MBA
Senior Partner
[redacted]

COMPLIANCE FORGE

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	ComplianceForge	General	NIST SP 800-171 R3 IPD	57	1718	3.12.5 Independent Assessment a.3.12.5 is sourced from NIST SP 800-53 R5 CA-2(1) and 3.12.5's entire Discussion section is a "cut & paste" from only the first of three Discussion section paragraphs in CA-2(1). b.The second paragraph in CA-2(1) needs to be added to 3.12.5 that clarifies assessor independence. This is due to the significant financial impact to the Defense Industrial Base (DIB) from the glaring omission of the clarifying information from CA-2(1)'s second paragraph that provides context about "independence" as it refers to an assessor.	Include the second Discussion pragraph from CA-2(1) that allows for independent internal resources.
2	ComplianceForge	Technical	NIST SP 800-171 R3 IPD	54	1599	3.5.3 Multi-Factor Authentication & 3.11.2 Vulnerability Monitoring and Scanning a.3.5.3 states, "Implement multi-factor authentication for access to system accounts." b.3.11.2(d) states, "Implement privileged access authorization to the system for vulnerability scanning activities." c.Since authenticated vulnerability scanning generally uses a privileged system account, does this mean that authenticated scans have to leverage Multi-Factor Authentication (MFA) or only an individual's authentication to the vulnerability scanning solution requires MFA?	Clarify that authenticated vulnerability scans do not require MFA.

* indicate required fields

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
3	ComplianceForge	General	NIST SP 800-171 R3 IPD	49	1867	3.13.8 Transmission and Storage Confidentiality & 3.13.11 Cryptographic Protection a. Per the ITAR Final Rule (§ 120.54(a)5(iii)), Advanced Encryption Standard (AES-128) is an acceptable cryptographic protection. b. Per NARA, the CUI Category “Export Controlled” (EXPT) is CUI. c. Given that the ITAR Final Rule allows AES-128 for a defined category of CUI, is AES-128 sufficient to address the “organization-defined types of cryptography” assignment?	Utilize the wording from the ITAR Final Rule, "Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology (NIST) publications, or by other cryptographic means that provide security strength that is at least comparable to the minimum 128 bits of security strength achieved by the Advanced Encryption Standard (AES-128)"