Draft SP 800-171B comments

TC

Tom Cornelius <tcornelius@complianceforge.com>

Today, 2:24 PM

sec-cert

Reply all

Inbox

NIST,

Good morning! In reviewing the draft version of SP 800-171B, here are my comments:

- In table D-11, control # 3.11.7e maps to “SR-2: Supply Chain Risk Management Plan” that is not a NIST 800-53 rev4 control, based on the published version of NIST 800-53 rev4 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- In table D-12, control # 3.12.1e maps to “SR-6(1): Supplier Reviews l Penetration Testing & Analysis” that is not a NIST 800-53 rev4 control, based on the published version of NIST 800-53 rev4 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- The addition of the “e” suffix is unnecessarily confusing (e.g. 3.1.1 vs 3.1.1e) between 800-171 and 800-171B. While it makes sense for the numbering in 800-171 to start with the number 3 (since those controls are in chapter three), for 800-171B I would recommend using the “e” as a prefix, since that clearly identifies the control as “enhanced” and still retains the functional area the control addresses (e.g., E.1.1 instead of 3.1.1e or E.13.4 instead of 3.13.4e). This will reduce confusion for companies in managing controls by removing confusing numbering:
  - First field – E for enhanced
  - Second field – appropriate NIST 800-171 family (14 total)
  - Third field – sequential control number

Respectfully,

Tom Cornelius, CISSP, CISA, CIPP/US, CRISC, PCIP, MCITP, MBA
Senior Partner
tcornelius@complianceforge.com
855-205-8437 (office)
503-896-1104 (mobile)

COMPLIANCE FORGE