[redacted]

From: 'Pete Fagan' via DIG-Comments <DIG-Comments@list.nist.gov>
Sent: Thursday, September 19, 2024 9:56 AM
To: dig-comments@nist.gov
Subject: [dig-comments] Comments on NIST SP 800-63 DIG Rev 4

Good afternoon,

I am providing a few comments regarding the upcoming revision noted above.

It is recommended that as the NIST controls are being more widely adopted and used by a wider lay audience - (including myself) it would be beneficial to provide more examples of the technology referenced in the discussion/supplemental guidance and expand definitions. This is versus having to find clues or examples to info by having the luck to find the digital identity guidelines or implementation guidance on the web (which is difficult to find the first time much less the second time; and thank someone for bookmarks).

I believe examples would be more advantageous in lieu of definitions alone for the technology or control language references such as RP, verifier, authenticator, primary vs second channel or the difference between technical references in the Identity Proofing portions related to authenticators vs. those under IA-5 (1). It is too cumbersome and confusing to try and understand how to relate real world applications vs federal government operations for identity proofing. It is challenging to implement or particularly evaluate technology or implementations without that additional clarification. Someone is not served well by the reference or guidance document if they have to go do a Google search from other sources for an answer.

Wow! Sorry....I think I opened a wound or a trigger - not sure which.

The main reason I had reached, but is an extension of the first suggestion, is to clearly define the scope of what PSTN is in relation to I-A in the 63 series as well as 800-53. It shouldn't be that difficult to determine if control statements or the immediately following discussion or supplemental guidance provide some sort of reference in lieu of going to find the full definition and its scope elsewhere. There are about 12 PSTN references in 800-53 and you have to be lucky enough to know 800-63 exists and or find it and then find essentially two sentences in 63B Section 3.1.3.1 that are a close discernable reference that the mobile phones and network are considered PSTN.

So. Given the wider adoption and use of 800-53 or 171 I am recommending NIST look for opportunities to be more expansive with examples and definitions in the control documents so the reader does not need to go to additional documents to determine meaning and scope of a word as those noted above and others. And if you do nothing else - please expand the definition and clear meaning of the scope of PSTN for what it covers in landline, wired connections or the public wireless networks, devices etc. in 800-53, 63 and 171.

Thanks for the opportunity to comment.

Pete Fagan

Director, CJIS Compliance Program
CJIS Information Security Officer
Global Data Protection - Products
Motorola Solutions, Inc
[redacted]

This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, you should delete this message. Any disclosure, copying, or distribution of this message, or the taking of any action based on it, is strictly prohibited.

For more information on how and why we collect your personal information, please visit our Privacy Policy.

--

To unsubscribe from this group, send email to dig-comments+unsubscribe@list.nist.gov

View this message at https://list.nist.gov/dig-comments
To unsubscribe from this group and stop receiving emails from it, send an email to DIG-Comments+unsubscribe@list.nist.gov.