From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] PSA"s Comment on NIST SP 800-171 Rev 3
Date: Thursday, June 8, 2023 3:14:29 PM
Attachments: image001.png
PSA-sp800-171r3-ipd-comment-.xlsx
PSA-COMMENT-NIST-800-171-REV3.docx

To Whom It May Concern:

Attached is the comment template and a form letter with the comment separated out in case the comment can not be read in the excel document.

Thank you!

DREW BERRY, CSAP
IT | Cyber Security Compliance
Professional Systems
Associates,Inc.
[redacted]

Professional Systems Associates Inc
[redacted]

Comment regarding Initial Public Draft of NIST SP 800-171, Revision 3

3.5.2 – Page 27, Line 1011

Within 3.5.2 of NIST SP 800-171 Rev 2, the requirement states that we are to Authenticate (or verify) the identities of users, processes, OR devices as a prerequisite to allowing access to organizational systems. The "OR" is understood to be an indicator of choice where organizations could choose which way to achieve compliance with this requirement.

Within 3.5.2 of NIST SP 800-171 Rev 3 IDP, the requirement states we are to uniquely identify and authenticate organizational devices and/or types of devices before establishing a system or network connection.

This requirement is radically different than the control in Rev 2 and would be impossible to achieve for external users. If an organizational entity contracts with a government customer and needs to allow them (the government customer) access into resources offered (by the organizational entity) via contract or other means, that organizational entity has absolutely no control over government endpoints (or those who control government endpoints) and has no method in which to enforce access into a resource offered by the organizational entity. Though some government endpoints may use static IP addresses vice DHCP, the mechanism that would identify and authenticate based on that information does not exist (at least as a specific offering by Microsoft in Government Community Cloud High) which is where our resources exist that are offered to the Government.

We have already complied with 3.5.2 in NIST SP 800-171 Rev 2 specifically where we are able to authenticate the identities of external users as a prerequisite to allowing access to organization systems. Enabling 3.5.2 in Rev 3 as written severely impacts our offering to the government.

Thank you for your consideration.

Respectfully,
Andrew Berry
Compliance Team
PSA Inc

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Andrew Berry/PSA, Inc.	Technical	Publication	27	1011	Within 3.5.2 of NIST SP 800-171 Rev 2, the requirement states that we are to Authenicate (or verify) the identities of users, processes, OR devices as a prerequite to allowing access to organizational systems. The "OR" is understood to be an indictor of choice where organizations could choose which way to achieve compliance with this requirement. Within 3.5.2 of NIST SP 800-171 Rev 3 IDP, the requirement states we are to uniquely identify and authenticate organizational devices and/or types of devices before establishing a system or network connection. This requirement is radically different than the control in Rev 2 and would be impossible to achieve for external users. If an organizational entity contracts with a government customer and needs to allow them (the government customer) access into resources offered (by the organizational entity) via contract or other means, that organizational entity has absolutely no control over government endpoints (or those who control government endpoints) and has no method in which to enforce access into a resource offered by the organizational entity. Though some government endpoints may use static IP addresses vice DHCP, the mechanism that would identify and authenticate based on that information does not exist (at least as a specific offering by Microsoft in Government Community Cloud High) which is where our resources exist that are offered to the Government. We have already complied with 3.5.2 in NIST SP 800-171 Rev 2 specifically where we are able to authenticate the identities of external users as a prerequisite to allowing access to organization systems. Enabling 3.5.2 in Rev 3 as written severely impacts our offering to the government.	