Hello!

Thank you for the opportunity to offer pre-draft comments towards the efforts of NIST 800-171 Rev 3.

After speaking with some colleagues, I agree that some things that should be considered include:

- Clarify the document’s intent at the beginning of the document. If it’s 800-171’s intent to be part of DFARS compliance, that should be stated.

- Define both External Service Providers and Cloud Service Providers (they are not the same). This would greatly help limit confusion and it would leave a lot less room for interpretation in the ecosystem. Further, clarifying the applicability of NIST 800-171 to assess CSP and MSPs would be extremely helpful.

- Offer general CUI feedback that currently isn’t covered:
  - How should the appropriate flow of CUI be managed if a device is company-owned versus BYOD?
  - Should SPAs that don’t process/transmit/store CUI be required to follow the same controls of the assets that do process/transmit/store CUI?

- Offer alternatives to FIPS 140 Validation.

Thank you!

Allison K. Giddens
President, Operations
Win-Tech, Inc.
AS9100 Certified, Veteran-Owned
2021 Cobb Chamber of Commerce Top 5 Finalist, Small Business of the Year
2021 Georgia Business Journal Top Aerospace Manufacturer

Win-Tech Office Hours: 7:00am-5:30pm (Monday-Thursday) and closed on Fridays.