[redacted]

From: Adam Austin [redacted]
Date: Friday, August 5, 2022 at 2:35:11 PM UTC-4
Subject: 800-171 Rev 3 Comments
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>
Cc: Aliahu Bey [redacted]

Hello NIST. We at Haight Bey & Associates / Totem Technologies offer the following pre-draft comments for the impending 800-171 Rev 3:

- NIST 800-171 as it is now is too much for most small business members of the DIB. Most of our clients come nowhere near meeting the assumed "NFO" implementations as listed in Appendix E. The one-time and recurring costs associated with implementing the 110 additional controls and 320 Assessment Objectives in 800-171/A are causing many DIB small businesses to re-think doing business with the Federal government. The tragic result of this will be a loss of diversity in the Federal government supply chain. At the government's request, I'd be happy to provide examples of our small business clients who have decided to stop doing business with the DoD simply because of the costs associated with DFARS 252.204-7012, NIST 800-171, and the CMMC.

- We'd suggest Rev 3 include a small business section that further tailors of 800-171 to align with the CSF subset published in NISTIR 7621 Rev 1 "Small Business Information Security: The Fundamentals". We estimate there would be between 35-45 of the existing 800-171 controls that would satisfy the 7621 Fundamentals. Small Businesses that meet the SBA threshold would only need to implement those controls to satisfy the protections required by DFARS 252.204-7012.

- We'd also suggest doing away with or narrowing the scope of the requirements for FIPS Validated cryptography, at least as part of an initial implementation of 800-171 for small businesses. Many small businesses (ourselves included) have had to re-architect on-premise networks to implement FIPS Validated crypto in, for instance, wireless routers and VPN. This has been very costly, and for many small businesses will be prohibitively so. Additionally, as referenced in this post https://www.totem.tech/cui-credentials-password-managers/, the DoD has taken a VERY liberal interpretation of when FIPS Validated crypto is required to protect the confidentiality of CUI, including in password managers. Furthermore, in some cases -- FortiGate for instance, to take advantage of a FIPS Validated mode of operation the firmware on the device must be downgraded to an older version that went through the Validation process. As a security

professional, I'd rather have the latest firmware version on my network device than ensure that the same encryption implementations have been re-validated.

Thank you for the consideration and thanks for all you do to help secure our Nation!

Very respectfully,

Adam Austin | Cybersecurity Lead

Haight Bey & Associates | Totem.Tech | 1972 W 2550 S Suites A&B, West Haven, UT 84401

Office: [redacted] | Cell: [redacted]

[redacted] | [redacted]

www.haightbey.com | @haightbey | www.totem.tech

www.linkedin.com/in/adam-austin-cybersecurity

*** Do not send Controlled Unclassified Information (CUI) in the body or as an attachment to this email address. If you have CUI you must send me, and do not have a method of secure transmission, please let me know and I'll provide an alternate transmission method. ***