From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] FW: Feedback from small business
Date: Thursday, June 15, 2023 9:00:35 AM

Good morning,

The process is not workable because organizationally defined parameters from USCG, DTRA, Navy, Marine Corps, Air Force and Army may differ, but we have a single IT system, making it nearly impossible to meet without a single DoD ODP.

We have multiple requirements to meet – NIST SP 800-171 Rev. 3, the independent assessment for 171 (and extra requirements in the assessment guide given as clarifications), and CMMC Rev. 2.0 which is a whole separate set which are loosely related. Adding complexity, the plan to move from NIST SP 800-53 as a distinct separate entity is now tightened up, making small businesses look to both documents.

Given CUI has not found any success in getting the organizational guidance on implementation (based on organization input), it seems illogical to follow in that methodology of not having this defined in advance. CUI continues as an example to the failure of lack of standardization at the DoD level – not mention USCG, or other federal entities. Small business actually have multiple contracts within and beyond DoD.

Instead of moving towards a coherent workable set of requirements, the complexity level increases and ability, cost and achievability become stumbling blocks. It reminds me of the comment, “We are from the US Government and we are here to help.” This approach is not helping especially when helping is actually increasing the requirements from 110 to 248 with about 150% increase of work. Our current SSP is 800 pages to address the 110 requirements.

The cost of two independent assessments rather than one (one for NIST compliance and another for CMMC) is not something which the 70% of the defense industrial base can manage and stay in business, not to mention the barriers to entry for new defense contractors, including those in the supply chain (many coming from commercial industry) to provide cutting edge technology to the military.

This approach only widens the valley of death for tech transition. We have seen several subcontractors of ours go out of business due to this ever widening gap in the valley of death, which is a detriment to the U.S. Armed Forces. Our competitors in Iran, China and Russia do not face these same issues, and therefore as we see leap ahead in technology with AI, machine learning, advancements in electrical engineering, mechanical engineering, aerospace, and drones, all applying commercial technology to the military – this requirements spiral continuing to increase only assists our competitors.

Much of the “advancements” are simply taking private sector technology into the US DoD, but it is being blocked from entry. The contracts process is a barrier.

The better approach would be crawl, walk, then run. We were close with Rev. 2 of NIST SP 800-171 and self-assessments. Lack of trust of the DIB is not making national security stronger, but weakening it. The framework was meant to be a process that is risk based. The current path is not risk based, and the bureaucracy is counter to the flexibility required to keep ahead of the threat in cyberwarfare, which industry is defending against without the help of the government.

Frank Koye
Chief Information Officer
Hepburn and Sons LLC
[redacted]
http://hepburnandsons.com/