From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Public Comment Response 800-171 Revision 3
Date: Thursday, January 11, 2024 12:33:12 PM
Attachments: 2024_01_10_16_21_47.pdf

To whom it may concern:

Please find attached our question on the proposed revisions to the Special Publication 800-171 Revision 3.

Neal Ridgeway
NIST Compliance Task Force Member
Walsh Group
[redacted]

January 9, 2024

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930
Attn: Computer Security Division

RE: Public Comments/Questions on the Final Public Draft ("FPD") of Special Publication("SP") 800-171 Revision ("Rev 3")

To whom it may concern:

On November 9, 2023, the National Institute of Standards and Technology ("NIST") released the Final Public Draft ("FPD") of Special Publication ("SP") 800-171 Revision ("Rev.") 3, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" and the Initial Public Draft of NIST SP 800-171A Rev 3, "Assessing Security Requirements for Controlled Unclassified Information."
In your request for public comments, our company seeks and answer to the following question:

1. Does the vendor of a commercial off-the-shelf, FedRAMP authorized, cloud software product have to accept the CMMC 2.0 flowdown requirements as described within DFARS 7012? There is a small number of SaaS solution providers with a FedRAMP (moderate and/or high) authority to operate. However, we have encountered only one FedRAMP authorized, SaaS vendor willing to accept the flowdown of the DFARS 7012 terms. This possible single-source option would present a hardship to the entire Defense Industrial Base (DIB).

"If SaaS providers will be required to accept the CMMC 2.0 flowdown requirement, it has the potential to create a solution monopoly within the federal contracting space and dramatically increase pricing to contractors. Additionally, such a requirement may also require some federal contractors to deploy multiple solutions for essentially the same cloud-based service(s), one solution for non-federal contracts, and another similar solution for federal contracts. Such multi-solution approaches will also increase costs plus maintenance burdens. Such hardships will likely be especially difficult for small businesses (thus creating a significant obstacle) who are generally much more resource constrained than large businesses."

Thank you for your attention to this question and please contact the undersigned with any questions. We look forward to your response.

Sincerely yours,

Neal Ridgeway
NIST Compliance Task Force Member
Walsh Group
[redacted]