[redacted] [redacted]

From: Perreault, John [USA] [redacted]
Date: Monday, August 15, 2022 at 10:24:26 AM UTC-4
Subject: Comments on CUI Series Publications
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>

I realize that NIST has more customers than the DoD, but this comment will be made from the perspective of compliance with the CMMC program.

Modify NIST SP 800-171 control 3.13.11. Modify the language to read “Employ FIPS-compliant cryptography when used to protect the confidentiality of CUI” (definition of compliant will be needed, suggest encryption which uses an approved algorithm (i.e. AES, 3DES) but does not have a CMVP certificate).

In addition, add an enhanced control to SP 800-172 which calls for FIPS validated encryption.

This eases the workload on the NIST staff as there will be increased demand for FIPS validated encryption from the 80,000+ DiB companies which will require validated encryption to be compliant with CMMC. The process of validation is a slow and intensive process in order to ensure that it is done correctly. It will be difficult to keep validations current and introduce new validated solutions with current staffing levels. It also requires high value programs (CMMC level 3) to use validated encryption to protect the most sensitive data.

John Perreault
Prin Security Engineer
Information Technology | Corporate

mercury

Mercury Systems
50 Minuteman Road, Andover, MA 01810
[redacted]

[redacted] | mrcy.com

The contents of this email and any attachments are intended only
for the designated recipient(s) and may contain proprietary information
of Mercury Systems, Inc If you received this email in error, please
contact the sender and delete the material from your systems

The information contained in this e-mail and any attachments from Mercury Systems, Inc. may contain confidential and/or proprietary information, and is intended only for the named recipient to whom it was originally addressed. If you are not the intended recipient, any disclosure, distribution, or copying of this e-mail or its attachments is strictly prohibited. If you have received this e-mail in error, please notify the sender immediately by return e-mail and permanently delete the e-mail and any attachments.