Back to Document Comments (/document/DARS-2020-0034-0194/comment?sortBy=postedDate)

Share

PUBLIC SUBMISSION

Comment on FR Doc # 2024-18110

Posted by the **Defense Acquisition Regulations System** on Sep 12, 2024

Docket (/docket/DARS-2020-0034) / Document (DARS-2020-0034-0194) (/document/DARS-2020-0034-0194) / Comment

Comment

"Require the contractor to complete and maintain on an annual basis, or when security changes occur, the affirmation of continuous compliance with the security requirements identified at 32 CFR part 170. The affirmation of continuous compliance is made by a senior company official (see definition of “senior company official” at 32 CFR 170.4 in the proposed rule published at 88 FR 89058) to affirm that its CMMC self-assessment of CMMC certification for each DoD UID applicable to the contractor information systems that process, store, or transmit FCI or CUI during contract performance remains current and the information system(s) covered by the CMMC self-assessment or CMMC certificate continue to be in compliance with the security requirements identified at 32 CFR 170.

Require the contractor to notify the contracting officer of any changes in the contractor information systems that process, store, or transmit FCI or CUI during contract performance and to provide the corresponding DoD UIDs for those contractor information systems to the contracting officer. The contractor is required to provide the DoD UIDS to the contracting officer so the Government can review associated CMMC certificate or CMMC self-assessment results and contractor affirmations of continued compliance in SPRS for those additional contractor information systems."

Firstly, "Security Changes" is ambiguous, especially when looking at the amount of ODPs listed in 800-171. For instance if an organization changes their password length, that could be considered a "security change". This language directs contractors to re-attest, despite this change not impacting CMMC (which only requires it to be defined and enforced). If the intent is that changes are being evaluated for their impact to CMMC compliance then this should state that, as opposed to requiring an attestation for anything that could, possible, impact security. (NOTE: There is already a requirement in CMMC to evaluate changes for impact to Cybersecurity, which if that is the intent would already be covered under 7012 via NIST SP 800-171).

Secondly, what is the value for requiring annual self attestation? If self attestation worked, we would not need 7021/7YYY and would be perfectly fine with 7012, 7019 and 7020. One of the main selling points of

the CMMC program is that based on data sensitivity the DIB is required to have their compliance validated by a 3rd Party. This requirement just adds paperwork and burden without delivering value.

Lastly, As wrote any change would include updating information systems, are contractors expected to notify the contracting officer every time they patch an Operating System, or add an asset to the Information System? The scope of this should line up with the what contractors are required to attest to. Furthermore, Contracting Officers are supposed to review these changes compared to the CMMC Cert and Attestation, however there is no approval requirement here, so I ask again what is the value of this? If the intent is for communication of these changes, what is the impact to the contracting officers workload?

Comment ID

DARS-2020-0034-0213

Tracking Number

m0y-3vbl-ffdh

Comment Details | **Submitter Info**

Submitter Name

Damian Golladay

City

Arlington

Country

United States

State or Province

VA

More Details

Give Feedback