Request for Information for Department of War

Subject: Reforming CMMC and Reducing Compliance Burden for the Defense Industrial Base

Background: In support of Secretary Hegseth's vision for the "Arsenal of Freedom," the Department of War (DoW) recognizes that scaling warfighter readiness relies on a secure, innovative, and agile Defense Industrial Base (DIB). While safeguarding federal data remains a critical, non-negotiable priority, recent research demonstrates that prohibitive compliance costs and administrative burdens of Cybersecurity Maturity Model Certification (CMMC) Phase II requirements have created unacceptable bureaucratic roadblocks for the DIB, particularly for small, medium, and non-traditional businesses. Additionally, duplicative overlaps in existing regulatory data requirements lack meaningful operational resilience guidance or requirements. To enable the DIB to field leading-edge commercial capabilities at the speed of need, the DoW Chief Information Officer (CIO) has suspended CMMC Phase II requirements and directed a CMMC Reform Task Force to comprehensively review the program and deliver actionable recommendations for reform.

The official memo is available under "New Items" in the CIO Library at https://dodcio.defense.gov/library/.

Purpose/Objective: This Request for Information (RFI) seeks direct feedback from DIB companies on practical strategies to inform the newly established CMMC Reform Task Force during its review. Specifically, DoW is soliciting input on protecting federal data and uplifting operational resilience against cyber-attacks while also reducing compliance costs and administrative burdens. The DoW is seeking industry input on ideas such as DIB usage of existing commercial cybersecurity capabilities, leveraging and optimizing self-attestation capabilities, and streamlining cybersecurity compliance. Your firsthand insights into navigating federal cybersecurity requirements will directly inform and shape upcoming policy reforms aligned with the Acquisition Transformation System (ATS) and designed to make partnering with the DoW more accessible, cost-effective, and secure.

This RFI is for market research purposes only and does not constitute a solicitation.

Description: This Request for Information (RFI) is issued solely for information-gathering purposes to support the newly established CMMC Reform Task Force. The DoW aims to accelerate the delivery of cybersecure capabilities to the warfighter by fundamentally reforming our approach to supply chain cybersecurity. This RFI seeks industry perspectives on utilizing existing commercial cybersecurity capabilities, leveraging and optimizing self-attestation capabilities, and streamlining cybersecurity compliance requirements. By benchmarking these approaches, the DoW intends to definitively reduce compliance and cost burdens on small, medium, and non-traditional companies while ensuring an uplift of cybersecurity and operational resiliency across the DIB. The DoW is committed to investing in, delivering, and dynamically maintaining a robust, secure, and agile Information Technology (IT) and Operational Technology (OT) environments that are connected, protected, high-performing, and empower the warfighter at speed without stifling DIB innovation.

Request for Information for Department of War

Responding to this RFI is essential for advancing government-industry collaboration and directly informing the actionable recommendations of the newly formed CMMC Reform Task Force. This RFI is issued solely for information and planning purposes. Responses to this RFI are not offers and cannot be accepted by the Government to form a binding contract. The Government does not intend to award a contract based on this RFI, nor will it reimburse any costs associated with the preparation of responses to this RFI. Submissions must not contain proprietary data, as the Government will not consider or review any responses marked as proprietary, and submitted materials will not be returned.

Response Instructions:
RFI responses shall be submitted online, conform to the format below, and provide the following information.

Format: Responses to this RFI must be unclassified and marked with appropriate proprietary information. *The Government is not liable for consequential damages for proprietary information not properly identified.*

- Responses are limited to ten (10) pages, single-spaced, Times New Roman, 10-point font, with one-inch margins. Text included in graphics, tables, and figures may be no smaller than 9-point. The cover letter (1 page limit) is not included in the total page count. Material submitted more than the 10-page limit and the page limitation exclusions may or may not be considered.
- One-page cover letter (will not go toward page count).
- Submittals must be in MS Word or in PDF format.
- Include a proprietary information statement (if applicable).
- Reference “Subject: Reforming CMMC and Reducing Compliance Burden for the DIB”.
- Include:
    - Company name, DUNS/EUI, CAGE Code, and point of contact (name, address, phone number, email address, and fax number).
    - Responses to the requested information.
    - Feedback on feasibility; and
    - Potential risks, challenges, or innovations.

No hard copy submissions will be accepted. Extraneous materials (brochures, etc.) will not be considered. The Government will not consider any submissions to any person other than Ms. Leanne Condren or submissions after the date specified below.

Requested Information:
These questions are designed to gather detailed information about industry readiness, cost drivers, and current cybersecurity control implementation to directly inform the newly formed CMMC Reform Task Force’s recommendations for DIB cybersecurity compliance and the future of the CMMC program.

Request for Information for Department of War

1. Identify the top five most prohibitive cost drivers, administrative burdens, or operational challenges your organization has experienced, or anticipates to experience, when attempting to comply with the CMMC framework and NIST SP 800-171 Rev 2.
2. Which specific security controls has your organization found to deliver the most tangible uplift of cybersecurity and actual risk reduction?
3. Conversely, which specific regulatory requirements or security controls create the highest administrative overhead and financial burden with the least measurable improvement to your actual cybersecurity posture?
4. Describe how your organization utilizes existing commercial cybersecurity capabilities, platforms, managed services, or any other additional strategies or initiatives to safeguard data, improve operational resiliency, and reduce cybersecurity risk, and how the DoW might better recognize or accept these commercial solutions within a compliance or risk framework.
5. Regarding Phase I self-assessments, what specific administrative or technical challenges does your organization face in maintaining, verifying, and reporting compliance, and how could this process be fundamentally streamlined? Have your self-assessments led to a more dynamic cyber posture approach, or are they performed only for compliance purposes?
6. What specific, actionable policy changes or regulatory reforms should the CMMC Reform Task Force recommend over the next 60 days to drastically reduce costs and barriers to entry for small, medium, and non-traditional businesses without degrading the protection of federal data?
7. What specific, actionable policy changes or regulatory reforms should the CMMC Reform Task Force recommend over the next 60 days to drastically improve operational resilience against cyber attacks at your organization?

Response Due Date: All responses to this RFI are to be submitted by 12 PM Eastern Time (ET), on Friday, August 14, 2026. Responses will be accepted via electronic means only to: whs.mc-alex.ad.mbx.eosd-psb-branch-mailbox@mail.mil and leanne.m.condren.civ@mail.mil.

Submissions to this RFI do not equate to self-attestation for CMMC. This is your opportunity to help the DoW shape the future of the cybersecurity and operational resilience of the DIB.