CASC | Coalition for Academic Scientific Computation

1930 18th St NW
Suite B2 2469
Washington, DC 20009
202.670.5798 | kelley@casc.org
http://casc.org
Unique Entity ID: ZTULLH6J6AD1

August 13, 2026

Ms. Leanne Condren
CMMC Reform Task Force
U.S. Department of War

RE: Coalition for Academic Scientific Computation (CASC) Response to Department of War "Reforming CMMC and Reducing Compliance Burden for the Defense Industrial Base (DIB)"

Dear Ms. Condren:

On behalf of the Coalition for Academic Scientific Computation (CASC), we appreciate the opportunity to respond to the Department of War's (DoW) Request for Information on the Cybersecurity Maturity Model Certification (CMMC) framework.

CASC is a coalition of research computing and cyberinfrastructure organizations at 112 leading research universities and national laboratories across the United States. Our member institutions support federally funded research across NSF, NIH, DOE, DoW, and other agencies, including research conducted under DoW contracts and subawards that may involve Controlled Unclassified Information (CUI).

With many of CASC's member organizations seeking CMMC certification, or already certified, CASC meetings and communication channels have been a venue for institutions to discuss compliance questions around CMMC and NIST SP 800-171. The CASC organizations represent a distinct subset of the Defense Industrial Base (DIB) focused on basic and open science, and through contracts with the DoW, the translation of that science into applications that further the readiness of America's defense. As such, this response centers on how CMMC implementation affects the continuity and pace of the research our members support — not on ranking security architectures — and aims to help ensure CMMC reform accounts for the distinct risk profile, governance structure, and open-science mission of research universities.

We welcome the opportunity for continued dialogue with the CMMC Reform Task Force and DoW stakeholders as this process moves forward.

Sincerely,

Kathryn Kelley
CASC Executive Director

II. Responses to RFI Questions

The following responses draw on input from CASC member institutions' research computing security leadership, framed around how CMMC implementation affects the continuity and pace of the research those institutions support.

1. Top five most prohibitive cost drivers, administrative burdens, or operational challenges

1. Security Protection Assets (SPAs) at academic research institutions.
   CASC member institutions are increasingly investing in both physical- and cyber-security in support of their teaching, research, and administrative operations. These investments fund substantial shared infrastructure — identity systems, log aggregation/monitoring platforms, and physical security systems — that serves research computing environments across the institution. Bringing SPAs into the CMMC scope forces academic research institutions to stand up redundant systems to meet specific NIST SP 800-171 controls even where no CUI data is present on those systems. Standing up and maintaining this parallel infrastructure diverts staff time and budget away from the shared research computing services those same institutions depend on, slowing support for active research projects rather than improving it.

   Beyond the infrastructure costs above, perhaps the most underappreciated cost driver is institutional compliance itself. Perhaps the most underappreciated cost driver is institutional compliance itself — the organizational transformation that CMMC readiness requires, independent of any single technical control. As Rob Groome, a research security leader, has put it, ‘CMMC isn’t just an IT project. It is an organizational transformation disguised as a cybersecurity compliance project.’ At research institutions, this transformation touches procurement, HR, legal, sponsored programs, and departmental IT — units that were never built to operate under a unified compliance framework, and that must now coordinate policy, documentation, and accountability in ways that create substantial administrative burden and cost well beyond the security controls themselves.
2. CMMC specifies technical certifications such as FIPS-validated cryptography and FedRAMP Moderate. These specifications narrow the field of compliant architectures among both commercial and open-source offerings available to research IT teams. Remaining commercial options carry a price premium and often a reduced feature set relative to the research-computing tools institutions currently rely on — directly constraining what researchers can do with a given budget. In a multi-mission environment, the added cost and reduced flexibility of certified products pushes institutions toward yet more redundant infrastructure just to keep CMMC-scoped projects moving without disrupting the rest of the research portfolio. It would be expected that certification would reduce administrative overhead by creating a common understanding of implementation priorities. In practice, however, the OSA still bears responsibility for describing how a FedRAMP-certified service meets NIST SP 800-171 controls, and FedRAMP-certified providers have been unprepared to provide current information responsive to these questions — leaving research IT staff to chase down answers instead of supporting projects.
3. Academic research institutions often centralize computation in High-Performance Computing (HPC) or High-Throughput Computing (HTC) clusters that give researchers the scale and economies needed for complex projects. These environments differ architecturally from the office workstation/server setting NIST SP 800-171 was written around, and applying office-oriented controls to them is disruptive to how research actually gets done. In practice, CASC member organizations have reported moving CMMC-scoped work into isolated 'enclave' virtual machines to satisfy required controls, and pairing this with network restrictions such as a prohibition on split tunneling. For a researcher, that means a single working session can no longer reach the CMMC enclave and the institution's shared HPC cluster, external data repositories, or collaborator systems at the same time — turning what was one workflow into several disconnected ones and materially slowing the pace of the underlying research, with no corresponding gain in protection for the CUI itself. The lack of a feasible path for enduring exceptions, together with the

absence of supplementary guidance for HPC/HTC systems, leaves institutions building redundant systems that do less to address the DIB's actual needs while doing more to slow down the research those systems were meant to support.

4. While academic research institutions may regularly take part in the DIB, DIB activities are on average a small share of an institution's overall research portfolio. As a result, not only is implementation costly, but the cost of C3PAO assessments is disproportionate to the average award amount — resources that would otherwise support a broader base of research. Reports from CASC members show wide variation in C3PAO guidance about allowable architectures, which slows institutions' ability to plan toward compliance without first engaging (and paying) a C3PAO for pre-assessment services, and adds financial and scheduling risk to research programs whenever re-assessment requires engaging a new assessor whose determinations may not align with the last one.
5. Institution-level attestations are a challenge for academic research institutions, many of which delegate operational authority to the School or College level. Of the many units at a research institution, only a small number are typically engaged in DIB activities, and principal investigators (PIs) operate with additional autonomy in how they run their research — a structure that exists specifically to serve the teaching and research mission and that enables CASC members' distinct contributions to the DIB in the first place. The already document-heavy CMMC program adds further administrative layers to bridge institutional attestations down to PI-level operations, adding process overhead that competes directly with the time PIs and research IT staff would otherwise spend on the research itself.

2. Controls delivering the most tangible cybersecurity uplift

Academic research institutions are already a prime target for phishing and ransomware attacks, which creates a strong incentive to invest in practices that protect ongoing research from disruption. The NIST SP 800-171 controls most likely to deliver tangible uplift are those covering areas where institutions are already investing to keep research operations running safely. This includes:

- Multifactor authentication for access to all sensitive systems and data
- Architectures that limit the scope of intrusions and malicious code, so an incident affects the smallest possible slice of ongoing research
- Encryption at rest and in transit, to limit the utility of intercepted research data
- Separation of duties to mitigate insider threats
- Practice of "Least Privilege" operations
- Maintenance of an asset inventory
- Establishment of system baselines with essential capabilities enabled
- A timely process for identifying and correcting information system flaws

However, due to CMMC's scoping guidance and detailed specifications, academic research institutions find that these institution-level investments cannot be made fully compatible with CMMC requirements without standing up duplicative systems — pulling resources away from the shared research computing environment those investments were originally meant to protect.

3. Requirements creating the highest burden with the least measurable security improvement

A. CMMC compliance and C3PAO assessment is heavily focused on maintaining documentation as ongoing evidence of alignment with controls. While there is some benefit to keeping documents from going stale, the practical effect on the ground has been research IT staff spending their time maintaining paperwork rather than supporting active research or reducing real risk. OSAs are also incentivized to deploy generic environments that C3PAOs will recognize, rather than the newer or more research-appropriate technologies that might serve a project better but are unfamiliar to assessors.
B. The prohibition on split tunneling is a clear example: it is a significant burden to support and a direct impediment to research continuity, since it prevents researchers from simultaneously reaching the CMMC enclave and the other systems — shared HPC/HTC resources, external collaborators, non-CUI data — their work depends on, without a clear, corresponding improvement in the security of the CUI itself.

C. The FedRAMP Moderate requirement for Cloud Service Providers (CSPs) narrows OSAs to a small set of vendors but does not reduce the documentation burden — OSAs still need to extract information about how their cloud vendor meets CMMC controls to populate their System Security Plans (SSPs). This adds administrative burden without a security improvement to show for it, since the CSP has already been externally certified, and that time is time not spent supporting research users of the platform.
D. The CMMC SPA scope applies the NIST SP 800-171 control list to core institutional infrastructure that cannot be brought into compliance while still serving its institutional purpose (see Q1). These SPA assets are critical to institutional functioning and already subject to ongoing external audits and penetration testing. Identity systems illustrate the problem well: to meet CMMC objectives, institutions stand up a redundant identity system solely for CMMC operations, complete with its own provisioning and de-provisioning workflow. This fragments the researcher experience, increases the chance of access errors that stall project work, and makes it harder for research IT staff to correlate user activity across CMMC and non-CMMC systems. Because this special-purpose system covers a smaller share of the institution's overall footprint, institutions are incentivized to invest the bare minimum needed to stay technically compliant — meaning it is likely to receive less scrutiny, not more, than the centralized system it duplicates.

4. Use of commercial cybersecurity capabilities, platforms, and managed services

Many CASC member institutions rely on shared, institution-wide security infrastructure rather than project-specific solutions, including:

A. Cloud environments authorized at FedRAMP High / DoD IL (e.g., GCC High or equivalent)
B. Centralized or managed Security Operations Center (SOC) services
C. Shared, campus-wide compliance and identity infrastructure

CASC recommends the DoW better recognize inherited controls from institution-wide FedRAMP- or StateRAMP-authorized environments, so that CMMC-scoped research projects can draw on infrastructure the institution has already invested in, rather than requiring redundant re-certification at the individual project or award level that slows project start-up.

5. Phase I self-assessment challenges

Member institutions report the following challenges in maintaining, verifying, and reporting Phase I self-assessments — each of which translates into time and uncertainty that slows down the research the self-assessment is meant to protect:

Controls interpretation is a significant challenge for both self-assessment and pre-C3PAO assessment. The NIST SP 800-171A Assessment Guide and Discussion state operational objectives without enough detail to guide implementation.

NIST SP 800-171 R2's controls are structured around a workplace configuration of desktop/laptop computers in an office environment, treating cloud services, remote servers, and external workspaces as add-ons. CASC members all operate research computing infrastructure, commonly in the form of HPC/HTC clusters, whose configuration differs substantially from this baseline. Where a member's systems differ from the office paradigm, the controls become ill-defined, and conversations with C3PAO organizations reveal widely varying guidance on how they apply. Institutions end up spending substantial effort figuring out what a given C3PAO will accept rather than architecting the solution that best serves the research environment — converting what is meant to be a controls-based assessment into an unguided, risk-based negotiation that adds financial and reputational risk for the OSA and uncertainty for the research program relying on the outcome.

CASC recommends streamlining self-assessment through standardized, reusable templates and clearer guidance distinguishing institution-level versus project-level scope, so research IT staff can spend more of their time supporting active projects and less time re-deriving how the controls apply.

6. Policy changes to reduce costs/barriers for small, medium, and non-traditional entities (next 60 days)

A. Tiered requirements scaled to CUI sensitivity rather than applied uniformly regardless of institutional size or DIB footprint — recognizing that risk depends on the nature of the data at stake, not simply how much of it an institution handles.

B. Reciprocity/shared assessment recognition across federal agencies to avoid re-litigating the same research computing environment for each new award.
C. Subsidized or cost-shared assessment support for academic subrecipients and smaller institutions, so compliance and certification costs don't crowd out research funding that exceed the reach of nearly all smaller institutions
D. More broadly, an increasing number of researchers at smaller institutions are working with controlled data of varying kinds and sensitivity levels, often without the budget for infrastructure (e.g., secure enclaves), services, certification, or external consultants — and without the in-house expertise or staff time to manage controlled data even where funding exists. Any reform of the CMMC program should account for this widening gap between researcher need and institutional capacity.

7. Policy changes to improve operational resilience against cyber attacks (next 60 days)

A. Rework SPA guidance to encourage leveraging centralized institutional systems rather than incentivizing ancillary systems that fragment support and slow researchers down
B. Funding support for shared or regional Security Operations Center capacity, so smaller research programs aren't forced to build stand-alone capability
C. Faster reciprocity pathways for existing FedRAMP-authorized commercial tools, to reduce project start-up delays
D. Clearer flow-down guidance for CUI handling in subawards, so research teams spend less time interpreting ambiguous requirements and more time on the funded work