THE COALITION FOR COMMON SENSE IN GOVERNMENT PROCUREMENT

August 14, 2026

leanne.m.condren.civ@mail.mil
Department of War

Subject: Reforming CMMC and Reducing Compliance Burden for the DIB

Dear Ms. Condren:

The Coalition for Common Sense in Government Procurement (Coalition) respectfully provides these comments to the Department of War's (Dow) Request for Information (RFI) on the Cybersecurity Maturity Model Certification (CMMC) program issued on July 13, 2026, with responses due August 14, 2026.

By way of background, the Coalition is a non-profit association of firms selling commercial products and services to the Federal Government. In Fiscal Year 2025, its members collectively delivered over $170 billion in goods and services to the Federal Government. These members include small, medium, and large business concerns. The Coalition is proud to have collaborated with Government officials for more than 45 years promoting the mutual goal of common-sense acquisition.

The Coalition supports DoW's decision to pause implementation of the impending requirement that firms must be certified by a CMMC Third-Party Assessment Organization (C3PAO) in order to be awarded a DoW contract involving Controlled Unclassified Information (CUI). Clearly, there are not enough C3PAOs to meet demand, driving up the cost for this certification. We applaud DoW for soliciting and considering industry input and urge DoW to balance its cybersecurity risks with the burden and costs on industry. We also strongly encourage DoW to engage in dialogue with industry through public meetings after reviewing the comments submitted in response to this RFI.

We note DoW uses NIST SP 800-171, Rev. 2 for CMMC and its CUI safeguarding clause, Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012. The Federal Acquisition Regulatory Council is proposing to use NIST SP 800-171, Rev. 3 for civilian agency contracts involving CUI. It would be helpful for industry if the Federal Government used the same cybersecurity standard for DoW and civilian contracts. Managing compliance with multiple Federal contract cybersecurity standards increases costs for contractors and ultimately American taxpayers. Moreover, multiple Federal cybersecurity standards for the same type of information make it even harder for small businesses and non-traditional contractors to do business with the Federal Government.

With respect to FedRAMP, industry is concerned DoW will not recognize the new Class C certification as equivalent to current FedRAMP Moderate (required per DFARS for external cloud service providers). We urge DoW to update the DFARS and align CMMC (or any successor program) with the new FedRAMP program changes reflected in the 2026 Consolidated Rules.

Our members are small, medium, and large businesses that occupy different spaces in the DoW ecosystem. Thus, their comments (attached) vary based on their specific situation. We note that several of the member companies that responded to the questions are firms in the healthcare industry that raise important points with respect to how cybersecurity in that market is already regulated. For one pertinent example, see "Respondent A." Thank you for your time and consideration. If you have any questions, I may be reached at rwaldron@thecgp.org.

Regards,

Roger Waldron
President

THE COALITION FOR COMMON SENSE IN GOVERNMENT PROCUREMENT

Organized CMMC RFI Responses

Responses are grouped by RFI question, with each contributor presented in a separate table cell.

Question 1: Cost Drivers, Administrative Burdens, and Operational Challenges

Response A:

We identify the following as the five most significant technical and operational challenges in attempting to comply with the CMMC Level 2 framework within a commercial healthcare environment:

1. Scope expansion in co-mingled networks. Establishing an isolated physical enclave is operationally and clinically challenging because duplicating medical and IT infrastructure introduces latency and risks to patient safety. Because potential CUI and commercial PHI are treated identically in a clinical setting and integrated within the same active systems, logical or data-level segmentation can break vital clinical data pipelines.
2. Cryptographic mandates on proprietary medical devices. FIPS-validated cryptographic modules are generally not supported by the medical device manufacturers, and making custom software modifications can void regulatory approvals or warranties. The cost to replace these specialized systems is prohibitive, and in many cases, compliant commercial alternatives do not exist.
3. Duplicative regulatory frameworks. Data and systems in the commercial healthcare industry are already highly regulated under HIPAA Security/Privacy Rules, the HITECH Act, federal medical quality standards, professional medical accreditation data security rules, and State Health Department and Privacy requirements. Forcing a separate, parallel CMMC control framework onto these same systems creates redundant administrative work without providing measurable improvement to actual data security.
4. Personnel qualification requirements. The administrative requirement to qualify and track commercial IT personnel under defense-unique standards, such as DoDM 8140.01, is a significant burden for organizations whose primary business is civilian healthcare.
5. Subcontractor flow-down requirements. Flowing down CMMC Level 2 requirements to specialized medical providers threatens to disrupt the integrated healthcare supply chain. Many of these suppliers are small to medium-size businesses, and compliance with CMMC Level 2 could be financially impactful.

Response B:

Question 1: Top Five Cost Drivers, Administrative Burdens, and Operational Challenges

Our company identifies five interrelated burdens. Although cost is a significant consequence, the larger problem is that these burdens consume limited personnel capacity, delay implementation, and create inconsistent security outcomes.

1. Interpretive uncertainty and assessment variability

The requirements state security outcomes, but contractors are frequently left to determine what practical implementation, test method, evidence, and level of documentation will satisfy them. Consultants and C3PAOs can reach different conclusions about the same environment. A contractor may implement a safeguard in good faith, document it, and later be told that an assessor expects a different technology, artifact, format, or procedure.

This is not merely an administrative inconvenience. It is a security gap in the program itself. When acceptance depends heavily on interpretation, similarly certified organizations may not have implemented equivalent protections. Contractors also spend resources hedging against uncertain expectations rather than correcting known technical risks. A uniform certification result should reflect a uniform security baseline, not the preferences of the individual assessor.

2. Duplicative documentation and evidence maintenance

A single implemented safeguard may be described repeatedly in the system security plan, policies, procedures, configuration records, responsibility matrices, evidence indexes, assessment workbooks, recurring logs, and vendor-generated reports. When a platform changes a setting name, reporting format, administrative interface, or technical function, the safeguard may remain operational while the contractor must locate and update the same information across numerous documents.

Our company is not suggesting that evidence is unnecessary or that controls should be set and forgotten. The concern is the unnecessary multiplication of evidence. One verified security fact should not require repeated manual narration across several artifacts merely because different assessors or templates expect it in different places.

3. Fragmented third-party tools, services, and responsibility boundaries

Small businesses rarely satisfy the framework through one platform. They may require a secure cloud environment, endpoint management, threat protection, backup, password management, logging, training, external service providers, and professional support. Each additional product or provider adds licensing cost, integration work, contract review, responsibility mapping, evidence collection, and another possible point of disagreement during assessment.

The burden is therefore greater than the purchase price of individual tools. Contractors must also determine which party performs each requirement, whether a commercial capability is recognized, how inherited controls are demonstrated, and whether an assessor will accept provider-generated evidence. Unclear responsibility boundaries can produce both duplicated effort and genuine security gaps.

4. Continuous staffing and specialist dependence

For a small business, CMMC is not a temporary certification project. Building and sustaining the environment requires ongoing technical administration, monitoring, documentation, vendor management, recurring reviews, employee support, and assessment preparation. The work can consume the equivalent of a substantial portion of a full-time position, or more, before accounting for consultants, managed services, and C3PAO costs.

This dependence is intensified by unclear guidance. A small contractor that cannot confidently interpret a requirement must purchase outside advice and may then purchase different advice when another provider or assessor disagrees. That market rewards interpretation and document production even when neither activity materially improves the underlying system.

5. Government-side CUI identification and delivery gaps

Contractors cannot protect information correctly if they are not told clearly and consistently what information is CUI before receiving or opening it. Our company has encountered acquisition material marked CUI even when the information appeared to consist solely of publicly available company information. Contractors may also receive files without a clear warning that an attachment contains CUI or encounter acquisition files through Government or third-party systems without an obvious handling notice before access.

This is particularly problematic for enclave models. A contractor may maintain separate commercial and CUI-authorized environments, email addresses, and users, yet Government acquisition and contract systems generally present one business contact and no dependable contract-level mechanism identifying the authorized CUI delivery channel. Surprise or over-marked CUI expands scope, creates preventable spillage risk, and imposes cost before the contractor has an opportunity to route the information appropriately. Government-side identification, marking, and delivery discipline must operate as part of the same security system imposed on contractors.

Response C:

For our small manufacturing organization, the principal burdens are activities that validate, interpret, or document compliance rather than activities that directly prevent, detect, or mitigate cyberattacks. Our five most significant cost drivers and operational challenges are as follows.

1. Third-party assessment and certification

The mandatory third-party CMMC assessment is the largest cost with the least direct return. Independent validation may provide confidence to a customer, but the assessment itself does not deploy a security capability, change employee behavior, or improve operational resilience. By the time a company is ready to be assessed, the security benefit has already been created through implementation of the controls. The assessment primarily produces a certificate of compliance. For a small business, that cost diverts funds from training, monitoring, threat prevention, backup, and other investments that directly reduce risk.

2. Cybersecurity consulting required to become assessment-ready

We hired a cybersecurity consultant to interpret the requirements, conduct gap analysis, assist with documentation, guide implementation, and prepare us for assessment. The consultant provided necessary expertise, but this is a substantial burden for a small company that does not employ dedicated CMMC compliance personnel. The need for specialized outside assistance reflects the complexity and ambiguity of the framework. Clearer government guidance, standardized implementation resources, and stable interpretations could reduce this dependency without weakening security.

3. Migration to FedRAMP-authorized and government-oriented products and services

Organizations are incentivized to migrate to FedRAMP-authorized services and government-specific offerings, because these environments are perceived as the safest path to compliance and a successful assessment. The resulting higher licensing costs, migration expense, consulting, user training, and ongoing administration create a significant recurring burden. In some cases, mature commercial services could provide security appropriate to the actual risk, but assessment uncertainty pushes companies toward higher-cost platforms regardless of whether the migration produces a proportional security improvement.

4. Creation and maintenance of compliance documentation

Developing and maintaining the System Security Plan, policies, procedures, plans of action, inventories, evidence repositories, and related artifacts requires substantial employee time. In a small company, this work is performed by personnel whose primary responsibilities are operations, management, not IT. Documentation is necessary, but the volume and maintenance effort can become an administrative objective of its own. The framework should emphasize whether controls are effective rather than how many artifacts are produced.

5. Uncertainty, changing interpretations, and an immature compliance ecosystem

Changing interpretations and a rapidly evolving market of compliance tools make it difficult to invest with confidence. The ecosystem of products that support compliance documentation, secure environments, and evidence collection has not matured quickly enough to provide timely, consistent, and affordable assistance. Small businesses may delay investments, replace previously selected tools, or retain additional consultants simply to remain aligned with evolving expectations. Stable guidance and authoritative interpretations would reduce rework and allow the commercial support ecosystem to mature.

Response D:

NIST SP 800-171 Rev 2 and CMMC have strengthened cybersecurity and improved the protection of CUI across the DIB. At the same time, companies continue to face significant financial, administrative, and operational challenges as they implement and maintain these requirements. Although those challenges vary based on company size, business model, technical maturity, and the volume of CUI handled, similar patterns emerge across industry. The five issues below consistently drive the cost, administrative burden, and operational challenges associated with compliance.

1. Technology Infrastructure: Upgrading technology infrastructure to support required security controls requires significant investment and ongoing operational effort.

Cost Driver: Purchasing and deploying security technologies, cloud services, identity management, endpoint protection, centralized logging, network segmentation, and other required capabilities often require substantial investments outside normal technology refresh cycles. Inconsistent auditor interpretations of security requirements may force organizations to make technology changes, driving up costs even when existing controls would otherwise be deemed effective.

Operational Challenge: Upgrading technology while maintaining ongoing contract performance requires careful planning, user training, and phased implementation to minimize disruption to business operations. Organizations also must integrate new security capabilities into existing environments while maintaining system availability. Differing auditor interpretations of the controls may create uncertainty and rework, disrupt workflows and make it harder to maintain consistent, predictable security operations. Further, overly prescriptive security requirements may limit inserting new technology which could otherwise advance cyber resiliency.

2. Documentation and Assessment Evidence: Producing and maintaining the documentation and evidence required for CMMC assessments requires continuous effort throughout the compliance lifecycle.

Administrative Burden: Collecting, organizing, reviewing, and maintaining system security plans, policies, inventories, network diagrams, plans of action, and assessment evidence require continuous attention rather than periodic updates before an assessment. Maintaining assessment readiness requires organizations to keep documentation current as systems, processes, and personnel change.

Cost Driver: Dedicating technical and program staff to prepare and maintain assessment evidence increases labor costs throughout the year. Time spent documenting compliance frequently competes with other operational and program priorities.

3. Defining Scope: Defining the systems, services, and data that fall within the CMMC assessment boundary remains one of the most complex aspects of compliance.

Operational Challenge: Identifying how CUI enters, moves through, and leaves an environment requires organizations to analyze data flows across interconnected systems, cloud services, subcontractors, and business processes. Inconsistent CUI marking and differing interpretations of scoping guidance can increase uncertainty and delay compliance efforts. Such controls may unnecessarily hamper collaboration between the DIB and the Government on CUI artifacts.

Cost Driver: Expanding the assessment boundary beyond what is necessary increases the number of systems that require security controls, monitoring, documentation, and assessment. Conversely, defining the boundary too narrowly can require organizations to revisit earlier decisions and perform additional work before an assessment.

4. Sustaining Compliance: Maintaining compliance requires continuous investment after organizations implement required security controls.

Cost Driver: Funding recurring assessments, readiness reviews, monitoring services, security tools, training, vulnerability management, incident response exercises, and policy updates creates ongoing expenses throughout the contract lifecycle.

Administrative Burden: Updating documentation, maintaining assessment evidence, addressing assessment findings, and adapting to evolving guidance requires continuous staff effort. Organizations must maintain an audit-ready posture at all times.

Operational Challenge: Balancing recurring compliance activities with mission delivery requires organizations to dedicate resources to both operational priorities and long-term compliance. As requirements and assessment expectations evolve, organizations must continuously adjust processes, documentation, and training while supporting ongoing contract performance.

5. Workforce: Building and maintaining a workforce with cybersecurity and CMMC expertise remains a challenge across the DIB.

Operational Challenge: Recruiting and retaining personnel with experience in cybersecurity, NIST SP 800-171 Rev 2, DFARS requirements, and the CMMC assessment process remains difficult in a competitive labor market for small and mid-sized contractors. Limited internal expertise can delay compliance efforts and increase dependence on outside support.

Cost Driver: Hiring experienced personnel and supplementing internal staff with consultants or managed security service providers increases both startup and recurring labor costs. Many organizations continue to rely on outside expertise to interpret requirements, develop policies, prepare assessment evidence, and support formal assessments.

These five issues consistently increase the cost, administrative burden, and operational complexity of achieving and maintaining CMMC compliance across the DIB. As cybersecurity requirements continue to evolve, the DoW has an opportunity to simplify compliance, reduce unnecessary regulatory burden, and improve consistency without reducing the protection of CUI. Focusing requirements on activities that produce measurable improvements in cybersecurity can strengthen both the security and resilience of the DIB while reducing costs that do not directly contribute to better security.

Response E:

a. Absence of Assessment Reciprocity. We maintain compliance with NIST SP 800-171 and NIST SP 800-53 via annual independent third-party assessments. Requiring separate SSPs and non-reciprocal CMMC assessments imposes duplicative cost and resource burdens without proportional security improvement.

b. Revision Misalignment. CMMC Level 2 is based on NIST SP 800-171 Rev 2, while FAR requirements may adopt Rev 3. Without harmonization or reciprocity, contractors face parallel SSPs and duplicative assessments for overlapping environments—adding cost without reducing risk.

c. Level 3 Cost and Inconsistent Application. CMMC Level 3 may require multi-million-dollar investments for limited contract opportunities. Broad contracting officer discretion in applying Level 3 creates

inconsistency; we experienced a solicitation where Level 3 was mandated then removed after review—demonstrating the need for objective, uniform criteria.

Response F:

When NIST 800-171 was first published, there were only 110 controls. This gave the appearance of a discrete measure of controls to achieve compliance. However, as the CMMC program matured, the NIST SP 800-171A Rev. 2 was published which included organization-defined parameters (ODPs). This increased the complexity of the program and increased the cost of compliance.

The difficulty of creating a CUI boundary across the Supply Chain

The Challenge: Properly identifying exactly where CUI enters, moves through, and leaves an organization is challenging as the lack of labeling or mislabeling of data hinders the proper identification of CUI. Government program managers frequently mislabel data, leading to "CUI creep" where unclassified text or commercial-off-the-shelf metrics are treated as highly regulated data.

The Burden: If scoping is done poorly, the entire corporate network falls under assessment scope. Forcing everyday business systems (like standard HR or accounting) to comply with federally mandated requirements creates crippling operational friction and skyrockets total compliance costs.

The Critical Shortage of Specialized Cybersecurity Talent (Resource Constraint)

The Challenge: Implementing technically complex controls—such as multi-factor authentication for legacy machines or centralized audit log management—requires high-level engineering skills.

The Burden: Midsize and small contractors must compete against massive primes and commercial technology firms for a limited pool of qualified compliance talent. Relying on external consultants creates a perpetual cost driver, while trying to handle it internally risks failing self-attestations due to lack of expertise.

Severe Operational Friction from Restrictive Controls

The Challenge: Strict NIST controls require restricting software installations, blocklisting unsanctioned tools, and mandating complex conditional access rules.

The Burden: These measures slow down daily business operations. Software engineers cannot download open-source libraries to run quick tests, and field personnel struggle to access data due to strict location-based firewalls.

Response G:

The Department's own rule models a Level 2 certification assessment at approximately $101,752 for a small entity, and that figure covers only assessment, reporting, and affirmation. It does not include implementation costs. The January 2025 draft FAR CUI rule projected an estimated $488,000 over three years for a small business to achieve and maintain Level 2. A fixed cost of that size is insignificant to a large prime, but likely prohibitive to a small business. Roughly 73% of the DIB is small business. The cost structure works as a filter that favors incumbents and screens out the small, non-traditional companies

where much of the innovation the Department is asking for actually lives. Many of those companies are dual-use and have a choice traditional defense firms do not, to stay commercial. If reform keeps a five to six figure fixed entry cost, the innovative DIB expansion this RFI describes will not happen.

Our evaluation of Level 2 came down to three factors, and cost was not the deciding one. First, the fixed entry cost above, weighed against uncertain CUI revenue. Second, scope we cannot predict. We have no way to know what would arrive marked as CUI, and a January 2026 DoD Inspector General advisory found that DoD organizations frequently mark documents incorrectly and default to unnecessarily restrictive dissemination controls, a problem the IG traced to conflicting and insufficient guidance and one that repeats findings from years earlier that remain unfixed. Scope we cannot predict is risk we cannot price. Third, and most important, instability. CMMC 1.0 launched in 2020, was replaced by 2.0 in 2021, was finalized as a rule in October 2024, and had Phase II and all later milestones suspended in July 2026. No small business can amortize a six-figure investment against requirements that have historically changed before payback.

Question 2: Controls Delivering the Most Tangible Cybersecurity Uplift

Response A:

The following controls would provide the most direct risk reduction:

- Identity management and database access controls (NIST SP 800-171 Controls 3.1.1-3.1.22 and 3.5.1-3.5.11).
- Network micro-segmentation (Controls 3.13.1, 3.13.5).
- Continuous logging and central correlation (Control 3.3).

Response B:

We have found the greatest measurable risk reduction in controls that directly harden identities, endpoints, cloud access, and data. These controls prevent unauthorized access, reduce the attack surface, and produce technical information that can be monitored and acted upon.

Identity and access protection

Multifactor authentication and strong authentication methods that reduce the usefulness of stolen passwords.

Conditional access policies that evaluate the user, device, application, and access conditions before permitting access.

Least-privilege access, separation of administrative accounts, and controls over privileged roles.

Managed endpoint hardening

Centrally managed device security baselines that enforce required configurations rather than relying on individual users.

Endpoint detection and response, anti-malware protection, attack-surface reduction, vulnerability identification, and timely remediation.

Encryption, secure startup protections, screen locking, device compliance, and restrictions on unmanaged devices or applications.

Why these controls matter

These safeguards are valuable because they are implemented and measurable in the operating environment. They can block access, enforce a configuration, detect a threat, identify a vulnerable device, or protect data if a device is lost. They also align with our broader recommendation: the program should emphasize implementation, validation, and monitoring of hardened systems. Training, policies, and evidence remain necessary, but they should support the operation of these safeguards rather than become the primary measure of security.

Response C:

Employee awareness and training

The controls requiring employee cybersecurity awareness and training have delivered the greatest improvement to our cybersecurity posture. Before our CMMC efforts, cybersecurity was more likely to be viewed as an information technology responsibility. Training, phishing awareness, acceptable-use expectations, and incident-reporting practices changed that perspective. Cybersecurity is now a shared responsibility and has become a core value within our corporate culture. Employees are more likely to question suspicious activity, recognize social-engineering attempts, report concerns promptly, and understand their role in protecting federal and company information. This behavioral and cultural change creates durable risk reduction across the organization.

Email filtering and phishing protection

Email filtering and phishing protection have also produced a tangible security benefit. These capabilities block or flag malicious messages, suspicious links, impersonation attempts, and harmful attachments before many threats reach an employee. Combined with employee training, they create an effective layered defense: technology reduces exposure while employees are better prepared to recognize and report threats that bypass automated controls. This combination has provided far more practical risk reduction than many activities focused solely on compliance evidence.

Response D:

NIST SP 800-171 Rev 2 contains an integrated set of security controls that work together to protect CUI. While every control contributes to a strong cybersecurity program, experience across the DIB indicates that a smaller group consistently delivers the greatest reduction in cyber risk. These controls address the most common attack vectors, improve visibility into malicious activity, and limit the impact of successful attacks. They also provide a practical foundation for organizations seeking to strengthen cybersecurity while managing implementation costs and operational complexity. Table 1 provides the NIST controls that produce the most significant improvements to corporate security posture.

Table 1. NIST SP 800-171 Rev 2 Controls Impacting Cybersecurity Posture and Reducing Risk

NIST Requirement	Effectiveness of Control	Operational Security Outcome
IA.L2-3.5.3: Multi-Factor Authentication	Prevents unauthorized access when passwords are compromised through phishing, password spraying, or credential theft.	Reduces account compromise, limits unauthorized access, and strengthens identity security across remote and privileged access.
SI.L2-3.14.1, SI.L2-3.14.2: Patch and Vulnerability Management	Removes known vulnerabilities before attackers can exploit them and reduces the available attack surface.	Reduces successful exploitation of known vulnerabilities, lowers ransomware exposure, and improves overall system resilience.
SI.L2-3.14.9, AU.L2-3.3.5: Endpoint Detection and	Detects malicious behavior that traditional signature-based tools may	Improves threat detection, reduces attacker dwell time, accelerates incident

Response / Continuous Monitoring	miss and provides continuous visibility across endpoints.	response, and strengthens forensic investigations.
AC.L2-3.1.5, AC.L2-3.1.7: Least-Privilege, Role-Based Access Control, and Privileged Access Management	Limits unnecessary access and reduces opportunities for privilege escalation and lateral movement.	Reduces insider risk, limits the impact of compromised accounts, and strengthens control over administrative privileges.
SC.L2-3.13.1, SC.L2-3.13.5: Network Segmentation and CUI Enclave Isolation	Restricts attacker movement and isolates systems that process CUI from the broader enterprise environment.	Contains security incidents, reduces enterprise-wide risk, and limits the number of systems subject to CMMC assessment.

Additional High-Value Controls: Other controls also provide significant security value. Secure configuration baselines (CM.L2-3.4.1 and CM.L2-3.4.2) reduce misconfigurations that attackers commonly exploit. Email protection (SC.L2-3.13.16 and SI.L2-3.14.6) reduces phishing risk, while backup and recovery controls (CP.L2-3.12.2 and CP.L2-3.12.3) improve resilience and support rapid restoration following ransomware or other disruptive events. Centralized logging and security information and event management improve visibility, accelerate investigations, and support both operational monitoring and compliance activities.

Prioritized Baseline: These controls could serve as a practical baseline for a risk-based compliance framework because they address the most common techniques used to compromise information systems, including credential theft, exploitation of known vulnerabilities, privilege escalation, and lateral movement. They also produce measurable operational improvements, such as fewer successful compromises, faster detection and response, reduced ransomware impact, and better containment of security incidents. Collectively, the NIST SP 800-171 Rev 2 control set provides a comprehensive framework for safeguarding CUI. Future reforms should preserve those security outcomes while promoting greater reciprocity between NIST SP 800-171 Rev 2 compliance and CMMC assessments, allowing organizations to demonstrate implementation once rather than satisfy overlapping compliance processes.

Conclusion: While every NIST SP 800-171 Rev 2 control contributes to a comprehensive cybersecurity program, these controls consistently provide the greatest measurable reduction in operational risk across a wide range of environments. Prioritizing them within a risk-based framework would help organizations reduce cyber risk more quickly while preserving the comprehensive protections provided by the full control set.

Response E:

The NIST SP 800-171 control set is appropriate and effective. If additional specificity is warranted, a DoD control overlay is the recommended approach.

Response F:

Identity & Authentication: Phishing-Resistant Multi-Factor Authentication (MFA)

The Framework Practice: NIST SP 800-171 (3.5.3) – Use multi-factor authentication for local and network access.

Why It Uplifts Security: Standard password policies and basic SMS/push-notification MFA are routinely bypassed by modern adversary toolkits (such as AiTM phishing proxies). Transitioning to FIDO2/WebAuthn hardware keys or managed cryptographic device certificates has effectively eliminated credential theft as an entry vector for our networks.

Access Control: Application Whitelisting and Restricting Local Admin Rights

The Framework Practice: NIST SP 800-171 (3.1.5) – Employ the principle of least privilege; (3.4.7) – Restrict, disable, or prevent unauthorized software.

Why It Uplifts Security: Removing administrative privileges from standard user endpoints stopped roughly 80% of opportunistic malware execution. By coupling this with strict application Whitelisting the administrative the burden of what should be blocked is eased. This can be done via our endpoint management tools, we prevent unauthorized or malicious binaries from running, severely limiting a hacker's ability to establish a foothold.

System & Information Integrity: Behavioral Endpoint Detection and Response (EDR)

The Framework Practice: NIST SP 800-171 (3.14.2) – Monitor system security alerts; (3.14.6) – Monitor organizational systems to detect attacks.

Why It Uplifts Security: Traditional, signature-based antivirus software fails against novel, "living-off-the-land" attacks that use legitimate administrative tools (like PowerShell) for malicious intent. Deploying an advanced commercial EDR tool gives us real-time, behavioral visibility across all endpoints. It detects anomalous activities as they happen and can automatically isolate a compromised laptop from the network before lateral movement occurs.

Question 3: Requirements with the Highest Burden and Least Measurable Security Improvement

Response A:

- FIPS 140 cryptographic module validation (NIST SP 800-171 Control 3.13.11). There are proprietary third-party vendor products that cannot support FIPS encryption modules.
- Software flaw remediation timelines (Control 3.14.1). Under CMMC, flaw remediation is assessed against strict timelines that often conflict with the operational realities of healthcare IT. Currently, proprietary medical device manufacturers require months to compile, test, and release security updates to maintain safety and regulatory clearances.
- Treating Protected Health Information (PHI) as CUI/FCI. Treating standard PHI and associated medical information as separate, distinct data classes requiring a parallel security apparatus is operationally and financially burdensome. As stated, data and systems in the commercial healthcare industry are already highly regulated under HIPAA Security/Privacy Rules, the HITECH Act, federal medical quality standards, professional medical accreditation data security rules, and State Health Department and Privacy requirements. These frameworks are specifically designed to protect PHI, which inherently encompasses the operational data associated with medical data. Requiring contractors to segment and treat identical data as CUI/FCI under defense frameworks requires redundant capital investments and increases ongoing administrative overhead. This operational friction delays essential services and creates a significant financial burden for commercial vendors without providing measurable improvement to actual data protection.
    - Recommendation: To remove this barrier, the DoW should decouple PHI from CUI. The compliance framework should allow commercial healthcare providers to assess their co-mingled systems against the NIST SP 800-171 standard strictly at the logical data layer (e.g., access control, encryption-at-rest, and user authentication). This logical assessment secures the data without requiring system-wide physical infrastructure audits of the entire commercial network. Under this approach, clinical healthcare providers can demonstrate compliance with the NIST SP 800-171 controls utilizing alternative mitigating controls in cases where FIPS implementation is not technically feasible.

Response B:

We do not identify one NIST SP 800-171 safeguard that should simply be removed. The highest burden with the least measurable improvement comes from the parallel compliance apparatus layered around the safeguards: repeated interpretation, duplicative evidence, manually synchronized documents, and assessor-specific formatting or artifact preferences.

The burden is in the compliance lifecycle, not the need for validation

A security-focused lifecycle should be straightforward: implement the safeguard, validate that it works, monitor its continued operation, remediate failures, and retain the evidence naturally produced by those activities. The current experience can become substantially longer: interpret an abstract requirement; obtain consultant advice; select a technology; implement and test it; describe it in multiple documents; create separate screenshots, logs, and trackers; prepare an assessor-specific evidence package; then revise the package when another reviewer prefers a different interpretation or format.

The additional steps do not necessarily make the safeguard more effective. In some cases, they divert the same limited personnel away from monitoring and remediation. Our organization therefore recommends standardized evidence expectations and acceptance of reliable system-generated reports wherever those reports demonstrate the required outcome. Evidence should prove security performance, not require contractors to reproduce the same fact in several formats.

Illustration: remote access

Remote access illustrates the interpretive problem. NIST SP 800-171 Rev. 2 requires organizations to monitor and control remote access sessions, protect their confidentiality through cryptographic mechanisms, and route remote access through managed access control points. A virtual private network is one possible method, but the practical expectation is less obvious in a cloud-only environment where users connect directly to an authorized cloud service through encrypted provider-managed connections, strong identity controls, conditional access, managed-device policies, and platform logging.

This does not mean that cloud use automatically satisfies the requirements or that a VPN is never needed. The contractor must still show that the applicable outcomes are implemented and monitored. The problem is that one consultant may present a VPN as mandatory while another assessor may accept a cloud-native implementation. Authoritative guidance should state when the requirement applies, distinguish examples from mandatory methods, identify equivalent approaches, explain how the safeguard is tested, and specify the evidence assessors should consistently accept. Contractors should purchase security capability, not competing interpretations.

Response C:

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?

Third-party certification assessment

The third-party certification requirement creates the highest administrative and financial burden with the least measurable improvement to our actual security posture. The assessment validates that controls have been implemented, but it does not itself deploy technology, train employees, strengthen system defenses, or improve recovery capabilities. The security work is completed before the assessment begins. For small organizations, the cost of certification and the effort required to prepare evidence can displace investments that would directly reduce cyber risk. Independent assessment should be reserved for

higher-risk circumstances, while lower-risk organizations should be permitted to use robust self-attestation supported by targeted audits or government verification.

Audit and Accountability control family

No individual security control is, by itself, overwhelmingly burdensome. However, the Audit and Accountability requirements create one of the highest ongoing burdens relative to their practical impact in our environment. We recognize the importance of logs and the ability to investigate security events. The difficulty is the cumulative effort required to configure, retain, review, document, and repeatedly demonstrate the logging environment for assessment purposes. Much of that effort is directed toward proving that the capability exists rather than actively using the information to improve security. Requirements should be scaled to organizational size, system complexity, and risk, with emphasis on whether a contractor can detect, investigate, and respond to meaningful events rather than on the volume of evidence produced.

Response D:

NIST SP 800-171 Rev 2 establishes a comprehensive, risk-based framework for protecting CUI. While those security requirements provide the foundation for safeguarding CUI, experience across the DIB indicates that some CMMC implementation and assessment requirements impose administrative and financial burdens that are disproportionate to their measurable cybersecurity value. The examples in Table 2 distinguish between the underlying NIST security requirements and the additional compliance activities introduced through CMMC, identifying opportunities to reduce compliance friction while preserving the security outcomes necessary to protect CUI.

Table 2. Highest Overhead, Lowest Measurable Cybersecurity Improvements from Controls and Requirements

NIST SP 800-171 Rev 2 Requirement	CMMC Requirement	Why the Burden Is Disproportionate	Suggested Change
3.12.1–3.12.4 (Security Assessments, SSPs, Plan of Action and Milestones [POA&Ms])	CMMC Level 2 assessment evidence for all applicable requirements; CMMC POA&M limitations and closeout requirements	SSPs and POA&Ms are valuable governance tools, but extensive narratives, evidence packages, and CMMC-specific POA&M restrictions create recurring administrative work that often exceeds their measurable cybersecurity value.	Retain the NIST requirements for SSPs, POA&Ms, and periodic self-assessments. Eliminate CMMC certification requirements and permit organizations to determine the level of documentation appropriate to their environment.
3.4.1–3.4.9 (Configuration Management)	CMMC assessment evidence demonstrating configuration baselines,	Routine configuration changes in cloud and DevSecOps environments generate substantial documentation with limited additional reduction in cyber risk.	Continue requiring configuration management under NIST while allowing

	approvals, and implementation		organizations to tailor documentation and approval processes to their operating model through self-assessment.
3.2.1–3.2.3 (Security Awareness and Training)	CMMC evidence demonstrating completion, role-based training, and supporting records	Training improves cybersecurity, but maintaining extensive training records and assessment artifacts adds administrative burden without improving user behavior.	Continue requiring training under NIST while allowing organizations to demonstrate compliance through existing enterprise training systems during self-assessments.
3.6.1–3.6.3 (Incident Response)	CMMC evidence supporting plans, testing, and implementation	Incident response capabilities improve security, but certification expectations for documentation and recurring exercises can impose costs that are disproportionate for lower-risk environments.	Retain NIST incident response requirements while allowing organizations to scale documentation and testing based on organizational risk and validate through self-assessment.
3.3.1–3.3.9 (Audit and Accountability)	CMMC assessment evidence supporting logging and review activities	Extensive log collection, retention, and documentation often produce diminishing returns when they exceed what organizations use operationally for threat detection and response.	Continue requiring logging that supports security operations while allowing organizations to determine appropriate retention and review practices based on system risk.
3.8.1–3.8.9 (Media Protection) and 3.10.1–3.10.6 (Physical Protection)	CMMC evidence demonstrating implementation of applicable controls	In managed cloud environments that prohibit removable media, documenting these controls can require substantial effort despite minimal residual risk.	Continue requiring these controls where applicable under NIST but allow organizations to determine applicability based on their environment and document that determination through self-assessment.
DFARS 252.204-7021 (Flowdown of NIST SP 800-171 Rev 2/CMMC requirements)	CMMC certification requirements throughout the supply chain	Applying the same certification expectations regardless of actual CUI access increases cost for prime contractors and subcontractors without proportionate risk reduction.	Require NIST SP 800-171 Rev 2 only for subcontractors that store, process, or transmit CUI, accept contractor self-assessments, and recognize reciprocity throughout the supply chain.

NIST SP 800-171 Rev 2 already provides the security requirements necessary to protect CUI. The examples above demonstrate that the greatest opportunities to reduce cost and administrative burden lie not in removing those requirements, but in simplifying how organizations demonstrate compliance with them. Replacing CMMC certification with contractor self-assessments against NIST SP 800-171 Rev 2, while maintaining contractor accountability and recognizing reciprocity across the DIB, would reduce unnecessary compliance costs and allow organizations to focus their resources on implementing and maintaining effective cybersecurity controls rather than preparing for certification assessments.

Response E:

Duplicative Compliance Without Reciprocity. CMMC requires separate certification for requirements already addressed by NIST SP 800-171 and NIST SP 800-53. Mandating additional assessments without recognizing equivalent or more rigorous frameworks imposes cost without commensurate security improvement.

Recommendation: Grant reciprocity for organizations assessed against comparable frameworks or establish a CUI-specific DoD overlay and control crosswalk applicable to existing certifications—preserving assurance while eliminating redundancy.

Response F:

The most burdensome, low-ROI areas in NIST 800-171 include:

1. Media Marking and Accountability

Controls: 3.8.1 (Mark media) and 3.8.2 (Restrict access).

The Burden: Requires physically or digitally labeling every single piece of media containing Controlled Unclassified Information (CUI), including system components, USB drives, backup tapes, and printed paper.

Why it Fails: Modern workflows are overwhelmingly digital and fluid. Spending hundreds of administrative hours manually tracking and stamping paper or USBs does little to stop modern, network-based data exfiltration or cloud-based vulnerabilities.

2. Comprehensive System Security Plan (SSP) Maintenance

Controls: 3.12.4 (Develop, document, and update system security plans).

The Burden: Demands highly detailed documentation of every hardware component, software asset, network diagram, and control implementation details across the entire contractor environment.

Why it Fails: An SSP is a static, backward-looking document. It frequently becomes outdated days after it is written. Organizations spend massive financial resources hiring consultants to write hundreds of pages of text to pass an audit, rather than investing that budget into continuous automated monitoring or active threat hunting.

3. Exhaustive, Multi-Tiered Log Retention & Periodic Reviews

Controls: 3.3.1 (Create and retain audit logs) and 3.3.2 (Review and analyze logs).

The Burden: Forcing smaller contractors to collect, correlate, and retain a massive volume of logs from every device, followed by performing regular manual or semi-automated reviews.

Why it Fails: Without an expensive Security Information and Event Management (SIEM) system and a dedicated Security Operations Center (SOC) to filter the noise, massive log retention results in "data swamps." Contractors incur high storage costs and administrative alert fatigue, rarely identifying a live attack through manual log skimming.

4. Rigid Configuration Baseline & Change Control Management

Controls: 3.4.1 (Establish configuration baselines) and 3.4.2 (Track/review configuration changes).

The Burden: Demands strict, formally approved change management processes for almost all system updates, software installations, and architectural tweaks.

Why it Fails: In a fast-paced, cloud-first DevOps environment, rigid change advisory boards create massive operational bottlenecks. Security teams waste time filing paperwork for benign software updates instead of hardening the actual infrastructure endpoints.

5. Excessive Assessment and Plan of Action & Milestones (POA&M) Over-Documentation

Controls: 3.12.1 (Assess security controls) and 3.12.2 (Develop plans of action).

The Burden: Continually generating formal, bureaucratic POA&M spreadsheets for minor, low-risk vulnerabilities that have clear operational justifications.

Why it Fails: It prioritizes checking boxes over fixing flaws. Security teams often spend more time updating the dates, tracking numbers, and milestone descriptions on a POA&M sheet to satisfy an auditor than it would take to actually patch or mitigate the underlying technical issue.

Response G:

FIPS validation is not the same thing as better encryption. Our security model is simple: everything current, patching enforced. Requirement 3.13.11 penalizes that model. NIST's Cryptographic Module Validation Program acknowledges a significant backlog, and validation has been known to take as long as two years, with changes to a module, including security patches, triggering revalidation and unrevalidated certificates flagged as Historical. The result is a choice between a validated module frozen at an older build and the current patched build of the same library, which is technically non-compliant. A requirement under which staying patched moves a company away from compliance is optimizing the wrong thing. Accept currently maintained implementations of NIST-approved algorithms as compliant, or fund CMVP to validate at the speed of patching.

Question 4: Commercial Cybersecurity Capabilities and Recognition

Response A:

Consistent with the federal preference for commercial marketplace procedures in DFARS Part 212 and FAR Part 12, the DoW may want to consider establishing a formal reciprocity model. Active compliance programs under the federal HIPAA Security Rule, federal medical quality standards, professional medical accreditation data security rules, and independent SOC 2 Type II audits should be accepted as equivalent to CMMC Level 2. Recognizing these existing commercial standards would eliminate duplicate audits, lower entry barriers, and allow commercial providers to partner with the government more efficiently.

Response B:

Our organization uses an integrated set of commercial cybersecurity capabilities to protect data and sustain a small, cloud-based environment. The value of these products is not that any one product makes an organization 'CMMC compliant.' Their value is that they provide enforceable security capabilities, centralized administration, monitoring, and system-generated information that can demonstrate whether safeguards are operating.

Commercial capabilities used by our organization:

Microsoft 365 GCC High as the core cloud environment, including identity and access controls, device management, endpoint protection, email and collaboration security, data protection, and administrative reporting.

A separately procured backup capability hosted in an appropriately authorized environment to improve recoverability and operational resilience.

An enterprise password-management platform used to centralize and protect credentials, enforce credential policies, prevent unmanaged browser password storage, and provide administrative auditing and reporting.

Microsoft Authenticator and related identity controls to support multifactor authentication and reduce reliance on passwords alone.

The recognition gap

Commercial platforms already contain substantial security and reporting capability, and vendors may provide security baselines, shared-responsibility information, compliance mappings, scores, workbooks, or assessment templates. These resources are helpful, but they are not an authoritative answer to what the Government or every C3PAO will accept. Some platform assessments also require manual input even when the relevant configuration exists elsewhere in the same ecosystem. Contractors are therefore left to translate product settings and reports into CMMC assessment objectives and then recreate that translation in their own documentation.

When a vendor updates the product, renames a setting, changes a report, or modifies functionality, the underlying safeguard may remain fully operational while the contractor must locate and update the same description across policies, procedures, system security plan narratives, configuration records, evidence

indexes, and assessment workbooks. This recurring document-synchronization burden produces little measurable security improvement and creates a new risk: conflicting records can make it harder to determine the actual current configuration.

How the Department could better recognize commercial solutions

The Department should establish a standardized, reusable method for mapping commercial security capabilities and machine-generated reports to applicable assessment objectives. A verified configuration or system-generated report should be capable of serving as the primary evidence wherever it demonstrates the required outcome, without requiring the contractor to restate the same fact across multiple documents.

For requirements that routinely generate conflicting interpretations, the Department should also translate the abstract security outcome into clear, technology-neutral implementation and validation guidance. That guidance should identify when the requirement applies, common acceptable implementations, equivalent alternatives, the validation method, and the evidence that C3PAOs should consistently accept. Industry and vendors can maintain product-specific mappings as technologies change; the Government's role should be to define and enforce the common outcome, validation, and evidence standard.

This approach would not create an out-of-the-box compliant system or shift responsibility away from the contractor. Contractors would remain responsible for selecting, configuring, monitoring, and evidencing their safeguards. It would, however, allow small businesses to spend more of their limited resources on operating secure systems and less on repeatedly narrating what those systems can already prove.

Response C:

Our organization uses a layered security model that combines commercial technology, managed services, and employee awareness. Major components include:

Microsoft GCC and Microsoft Defender for secure productivity, identity, endpoint, and threat-protection capabilities;

Managed Detection and Response services for continuous monitoring and response support;

a Managed Service Provider that administers cybersecurity capabilities and additional tools on our behalf;

INKY for email security and phishing protection;

Cisco Meraki for managed network infrastructure and security;

Duo multifactor authentication for stronger identity verification;

Datto for backup, recovery, and continuity capabilities; and

ThreatLocker for application control and restriction of unauthorized software.

These products and services provide practical protection across identity, endpoints, email, networks, applications, monitoring, backup, and recovery. They also allow a small business to obtain expertise and continuous capabilities that would be difficult to maintain entirely with internal staff.

The Department should formally recognize mature commercial certifications, platforms, and managed security capabilities within its risk framework. A civilian standard such as SOC 2 Type II should not automatically replace every requirement associated with protecting CUI, but it should provide meaningful credit as independent evidence that an organization maintains an established control environment. Similarly, commercial cloud and cybersecurity solutions should be accepted based on demonstrated security outcomes and equivalency, rather than whether they were developed specifically for government compliance.

A reciprocity model could map recognized commercial certifications and independently validated services to corresponding CMMC requirements, leaving contractors to demonstrate only the controls or data-handling requirements not already addressed. This would reduce duplicative assessments and documentation while encouraging businesses to adopt proven, continuously improving commercial security solutions.

Response D:

Commercial cybersecurity platforms and managed security services have become the primary means by which organizations implement the security requirements of NIST SP 800-171 Rev 2. These capabilities provide continuous monitoring, automated policy enforcement, advanced threat detection, and specialized expertise that strengthen protection of CUI, improve operational resilience, and reduce cyber risk. As these technologies continue to mature, DoW compliance frameworks should recognize and credit their capabilities through greater equivalency, reciprocity, and outcome-based assessment.

Leveraging Commercial Platforms, Managed Services, and Industry-Leading Tools: Organizations across the DIB increasingly rely on commercial cybersecurity platforms (e.g., FedRAMP Moderate) and managed security services as the primary means of implementing and sustaining the security requirements of NIST SP 800-171 Rev 2. Rather than relying on periodic manual reviews, these technologies provide continuous protection through automated monitoring, policy enforcement, and rapid response to emerging threats.

Commercial identity platforms, endpoint protection technologies, cloud security tools, and managed security operations continuously protect CUI by enforcing authentication requirements, restricting unauthorized access, monitoring for malicious activity, and protecting sensitive information across cloud and on-premises environments. Data protection capabilities such as encryption, data loss prevention, secure collaboration platforms, and information classification help ensure that CUI remains within authorized environments while reducing the likelihood of accidental disclosure or data exfiltration.

Commercial managed detection and response (MDR) providers, managed security service providers (MSSPs), and Security Operations Centers (SOCs) improve operational resilience by providing around-the-clock monitoring, threat hunting, incident investigation, and coordinated response activities that many organizations—particularly small and mid-sized contractors—could not practically maintain with internal resources alone. Cloud-native architectures further improve resilience through automated patching, resilient infrastructure, immutable backups, and standardized system baselines that reduce downtime and accelerate recovery following cyber incidents.

Continuous vulnerability management, threat intelligence integration, cloud security posture management, and automated remediation workflows also enable organizations to move beyond periodic compliance activities toward continuous risk reduction. These capabilities allow security teams to identify vulnerabilities based on exploitability, prioritize remediation, monitor emerging threats, and continuously strengthen their security posture as adversary tactics evolve.

Collectively, these commercial capabilities do more than satisfy many NIST SP 800-171 Rev 2 requirements. They deliver continuous protection, measurable operational improvements, and ongoing risk reduction that extend well beyond traditional point-in-time compliance activities.

Specific Platforms and Service Categories in Use:

Cloud Identity and Access Management: Enables multi-factor authentication, conditional access, identity governance, and privileged access management to reduce unauthorized access and credential compromise.

Endpoint Detection and Response: Detects malicious activity, accelerates incident response, and reduces attacker dwell time.

MDR and MSSPs: Provide 24x7 monitoring, threat hunting, incident investigation, and coordinated response by dedicated cybersecurity professionals.

Email, Web, and Domain Name System (DNS) Protection: Blocks phishing attacks, malicious websites, and command-and-control communications before they reach users.

Cloud Security Posture Management: Continuously identifies cloud misconfigurations, configuration drift, and policy violations while maintaining secure cloud baselines.

Enterprise Vulnerability Management: Continuously discovers vulnerabilities, prioritizes remediation, and supports automated remediation workflows based on exploitability.

Data Loss Prevention and Information Protection: Protects CUI through automated classification, encryption, access controls, and secure collaboration.

Governance, Risk, and Compliance Platforms: Automates control mapping, evidence collection, compliance monitoring, and executive reporting while reducing manual administrative effort.

Current DoD Compliance Framework Recognition of Commercial Solutions: Current DoW compliance frameworks do not consistently recognize the maturity or effectiveness of commercial cybersecurity capabilities. Assessments often emphasize documentation, screenshots, and point-in-time artifacts rather than measurable security outcomes such as continuous monitoring, automated policy enforcement, rapid threat detection, and incident response performance.

Similarly, managed security services receive limited recognition despite providing capabilities that many organizations cannot economically maintain internally. Contractors frequently must recreate evidence for controls already implemented by qualified service providers.

Current frameworks also provide limited reciprocity for commercial and government-recognized security authorizations. FedRAMP-authorized cloud services, ISO 27001-certified information security

management systems, and other recognized frameworks receive little credit despite substantial overlap with NIST SP 800-171 Rev 2 requirements.

Recommendations for Incorporating Commercial Capability Equivalency and Reciprocity: While the current approach centers on FedRAMP-authorized solutions, commercial cybersecurity platforms and managed security services can also provide robust security capabilities when they meet equivalent security and compliance standards, particularly for international contractors (e.g., third-party parts manufacturers outside of CONUS). Many commercial offerings undergo rigorous third-party assessments or align with internationally recognized frameworks, such as ISO/IEC 27001, and can provide security outcomes comparable to Government-authorized solutions when implemented within appropriately governed environments. Expanding recognition of these capabilities would enable organizations to leverage mature commercial technologies while maintaining the cybersecurity protections required to safeguard CUI.

To better recognize and accept these solutions within the CMMC compliance framework, we recommend that the DoW:

Recognize outcome-based implementations by accepting commercial cybersecurity platforms and services that demonstrate equivalent security outcomes, including internationally recognized certifications such as ISO/IEC 27001 and other independently assessed offerings, rather than relying exclusively on FedRAMP authorization.

Explicitly identify where FedRAMP-authorized and other appropriately vetted commercial platforms satisfy specific CMMC and NIST SP 800-171 Rev 2 control requirements, allowing organizations to inherit those protections rather than re-demonstrate equivalent capabilities.

Clearly define responsibility for security controls within FedRAMP-authorized and commercial cloud environments, recognizing inherited controls provided by the service provider and limiting contractor assessment activities to customer-managed controls. This would reduce duplicative evidence collection while improving consistency and reinforcing reciprocity across Government-recognized security frameworks.

Publish standardized mappings between commonly used FedRAMP-authorized and vetted commercial cybersecurity platforms and applicable CMMC and NIST SP 800-171 Rev 2 requirements to simplify implementation, improve assessment consistency, and provide organizations with a clear understanding of how commercial capabilities satisfy compliance requirements.

Accept tool-generated dashboards, audit logs, configuration reports, and other automated evidence as primary artifacts for demonstrating control implementation and effectiveness, reducing manual evidence collection and unnecessary documentation while improving the timeliness and accuracy of compliance assessments.

Commercial cybersecurity platforms and managed security services have become integral components of modern cybersecurity programs across both Government and industry. Recognizing these capabilities through greater equivalency, reciprocity, standardized control mappings, and appropriate recognition of inherited controls would better align DoW compliance requirements with current cybersecurity practices.

These reforms would reduce unnecessary administrative burden, improve assessment consistency, and enable organizations to focus resources on reducing cyber risk while preserving the comprehensive protections provided by NIST SP 800-171 Rev 2.

Response E:

FedRAMP Authorized Cloud Enclaves and Saas Platforms: Rather than managing physical hardware, we isolate Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) within secure environments.

Data Isolation: We use FedRAMP Authorized hyperscalers—such as Microsoft GCC High or AWS GovCloud—which feature built-in compliance boundaries for data residency.

Shared Responsibility: Leveraging these platforms allows us to inherit physical and environmental controls directly from the cloud provider, reducing our internal compliance scope.

Managed Security Services (MSSPs / MDRs) As a mid-sized organization, maintaining a 24/7 internal Security Operations Center (SOC) is operationally inefficient.

Continuous Monitoring: We contract with a Managed Detection and Response (MDR) vendor to provide continuous log aggregation, threat intelligence, and behavioral monitoring.

Incident Response: The provider supplies automated orchestration tools alongside human analysts, ensuring rapid isolation of endpoints if a breach occurs.

3. Zero Trust & Identity Infrastructure: We enforce access governance through FedRAMP Authorized Identity and Access Management (IAM) platforms.

Robust Access Controls: We utilize standard enterprise identity providers to mandate Multi-Factor Authentication (MFA) and device-health checks before data access is granted.

4. Enterprise Endpoint and Visibility Tools: We safeguard data at rest and in transit across all corporate endpoints using commercial software suites.

Continuous Vulnerability Management: Automated enterprise patch management and endpoint detection tools keep our surface area secure, reducing risk profile variations.

Response F:

The RFI asks how the Department might better recognize existing commercial cybersecurity capabilities. Our answer comes from direct experience. We run a Mac and Linux environment on Google Workspace with strong controls. But the Level 2 ecosystem, meaning the reference architectures, enclave products, consultant playbooks, and assessor familiarity, is built almost entirely around a single vendor's government cloud, where licensing alone runs roughly $36 to $98 per user per month, plus a migration project starting around $15,000 to $25,000 for a 25-user organization. For a company on a different modern stack, the implied path is not "demonstrate your security." It is "replatform, then demonstrate your security." That is a vendor migration tax presented as a security requirement, and it lands hardest on the non-traditional companies this reform is meant to attract. The Department should publish stack-

neutral equivalence criteria and accept continuous commercial attestation, such as FedRAMP authorizations and SOC 2 Type II reporting, as evidence against overlapping requirements.

Question 5: Phase I Self-Assessments

Response A:

The main challenge in self-assessments within co-mingled networks is the lack of specific scoping guidance that decouples PHI from CUI. This could be streamlined by creating a standard scoping template that maps HIPAA, federal medical quality standards, and professional medical accreditation controls directly to NIST SP 800-171. Doing this would allow clinical healthcare providers to meet the requirements of NIST SP 800-171, without having to build separate enclaves for CUI, or bring the entirety of their systems and network into scope for CMMC.

Response B:

Our self-assessment activities have driven meaningful system hardening, including conditional access, sensitivity labeling, data loss prevention, managed endpoint protections, and related safeguards. At the same time, a substantial portion of the continuing effort remains documentation-centered and is performed primarily to satisfy compliance requirements rather than to reduce cybersecurity risk. This experience illustrates the central structural problem with CMMC: the program too often produces documentation-centered compliance instead of implementation-centered security assurance.

Maintaining and verifying compliance

The principal challenge is not completing a questionnaire or calculating a score. It is maintaining the parallel compliance system surrounding the operating environment. Each assessment objective must be interpreted, mapped to one or more technical configurations or procedures, assigned to the responsible party, tested, and supported by evidence. The same implementation may then be described again in the system security plan, control-family documents, configuration records, validation logs, evidence indexes, and assessment workbooks.

Verification is similarly fragmented. Commercial platforms generate configuration, device, identity, alert, vulnerability, and audit information, but those reports do not consistently map to CMMC assessment objectives. Contractors must manually translate operating data into assessor-ready evidence. Safeguards may also span a cloud provider, a separately procured product, an external service provider, and an internal procedure, requiring the contractor to reconstruct the complete implementation and responsibility boundary for each review.

Reporting limitations

The reported assessment score is a static, point-in-time representation of a much more dynamic environment. By itself, it does not show whether a safeguard was technically validated, when it was last tested, whether monitoring is occurring, whether a configuration has drifted, or whether a failure was detected and remediated. Small businesses therefore expend substantial effort maintaining the records behind the score, while the formal reporting mechanism communicates comparatively little about the continuing operation of the safeguards.

Fundamental streamlining

The Department should establish one standardized, authoritative assessment record for each requirement. That record should identify the applicable assessment objective, the implemented safeguard, responsibility, validation method, accepted evidence, date last tested, current status, and any required remediation. It should feed the score and reporting requirement without forcing contractors to recreate the same information in multiple documents. Reliable commercial system-generated reports should attach to or populate the applicable objectives, and unchanged implementations and evidence should carry forward subject to defined periodic revalidation.

This approach need not provide the Government continuous access to contractor environments. Standardized, machine-readable reports and contractor-controlled evidence submission could improve consistency and reduce manual effort without creating an additional Government access point or unnecessarily exposing sensitive security information.

A mixed result with a clear lesson

Our self-assessments have contributed to a more dynamic cybersecurity posture where the requirements led directly to technical implementation, testing, and monitoring. Other portions remain largely compliance-driven because the required activity centers on maintaining duplicative narratives, mappings, and evidence packages. The lesson is broader than the self-assessment mechanism. The entire CMMC program should be reoriented from documentation-centered compliance to implementation-centered security assurance. Documentation and reporting should verify and summarize the security lifecycle, not operate as a separate parallel system competing for the same limited resources.

Response C:

We have completed a formal NIST SP 800-171 self-assessment and reported the required score. We likely would not conduct an assessment of the same scope and form absent the compliance requirement. The initial assessment was useful in determining whether required practices were in place and identifying implementation gaps. Beyond that initial determination, the assessment itself has not materially changed our cybersecurity posture.

The principal burden is maintaining the documentation and evidence required to verify and report the same control environment repeatedly. Once a mature program is established, a comprehensive reassessment provides diminishing returns. It verifies that previously implemented controls remain in place, but it does not necessarily cause the organization to respond more dynamically to current threats. It is unrealistic to expect every company to view an extensive recurring assessment as something other than a compliance exercise when the assessment is structured around proving conformance to a static set of requirements.

The process could be streamlined through an abbreviated annual self-attestation focused on material changes, significant deficiencies, incidents, and remediation status. A comprehensive review could occur less frequently or be triggered by objective risk indicators. Contractors should be able to maintain a living record of changes rather than recreate a complete evidence package each cycle. This would preserve

accountability while allowing resources to be directed toward monitoring, training, emerging threats, and continuous improvement.

Response D:

The Government intended CMMC Phase I self-assessments to provide a streamlined mechanism for contractors to demonstrate cybersecurity compliance through annual self-assessments and reporting in the Supplier Performance Risk System (SPRS). In practice, maintaining, validating, and reporting those self-assessments has become a significant administrative and technical undertaking. Organizations must continuously maintain assessment evidence, defend scoring decisions, manage POA&Ms, and attest that SPRS submissions accurately reflect their current cybersecurity posture, creating a compliance process that often resembles a formal audit without the benefit of standardized tools or consistent guidance.

Administrative and Technical Challenges in Maintaining, Verifying, and Reporting CMMC Phase I Self-Assessment Compliance

Documentation Burden: Maintaining documentation remains the most resource-intensive aspect of Phase I self-assessments. As systems evolve through software updates, cloud migrations, infrastructure changes, and configuration modifications, previously collected evidence quickly becomes outdated. Organizations must continuously update screenshots, configuration exports, inventories, policies, procedures, and other artifacts so they can demonstrate that their self-assessment remains valid. Because CMMC provides limited automation for evidence collection or validation, technical personnel perform much of this work manually. They spend significant time maintaining compliance evidence instead of monitoring, hardening, and defending operational environments.

Scoring Consistency: Organizations also face challenges applying the CMMC Phase I scoring methodology consistently. Determining whether evidence fully satisfies a requirement, whether a deficiency warrants score reduction, or whether corrective actions support maintaining an existing score often depends on organizational judgment. Without standardized implementation guidance, similar environments may reasonably arrive at different SPRS scores. This inconsistency reduces confidence in reported scores and increases the burden on senior officials responsible for certifying their accuracy.

Internal Resource Requirements: Maintaining self-assessment compliance requires sustained commitment from cybersecurity, information technology, compliance, contracts, and executive leadership. Organizations must continuously collect evidence, maintain documentation, manage POA&Ms, validate corrective actions, and coordinate recurring reviews before affirming compliance. For many small and mid-sized contractors, these activities compete directly with operational priorities and consume resources that could otherwise strengthen cybersecurity capabilities.

Limitations of the SPRS Submission Process: The SPRS submission process requires organizations to affirm that their reported compliance status remains current, even as technical environments continue to evolve. Because documentation often lags operational changes, organizations may struggle to maintain evidence that fully supports their reported SPRS scores. Prime contractors also face limited visibility into

subcontractor compliance status, increasing administrative effort and reducing confidence in supply chain risk assessments.

Impact of Self-Assessments on Dynamic and Continuous Cyber Posture: For many organizations, Phase I self-assessments remain primarily compliance-driven activities performed to satisfy contractual requirements and maintain eligibility for DoD work. Without automated evidence collection or continuous monitoring, compliance documentation quickly becomes outdated, turning self-assessments into periodic documentation exercises rather than accurate reflections of current cybersecurity posture.

Organizations that have invested in Governance, Risk, and Compliance (GRC) platforms, automated evidence collection, continuous control monitoring, and integrated security tooling report different results. These capabilities improve visibility into compliance drift, strengthen ownership of remediation activities, and allow evidence to be reused across multiple compliance frameworks. However, implementing these capabilities requires significant investment that may not be practical for many contractors, particularly smaller organizations.

Recommendations to Fundamentally Streamline the Self-Assessment Process: The Department should modernize Phase I self-assessments by emphasizing automation, continuous monitoring, and risk-based reporting rather than manual documentation.

Adopt Open Security Controls Assessment Language (OSCAL) to standardize machine-readable system security plans, assessment results, and POA&Ms, reducing manual document preparation and improving consistency.

Recognize automated evidence collection and continuous control monitoring as primary sources of assessment evidence, reducing dependence on manually generated artifacts.

Encourage integrated compliance platforms that consolidate evidence management, POA&M tracking, workflow management, and executive reporting into a single source of truth.

Publish standardized implementation guidance and assessment templates to reduce inconsistent interpretation of NIST SP 800-171 Rev 2 requirements and improve scoring consistency.

Replace fixed affirmation cycles with a risk-based reporting model that ties updates to significant changes in system architecture, CUI scope, or security posture rather than arbitrary reporting dates.

Phase I self-assessments provide an important mechanism for demonstrating compliance with NIST SP 800-171 Rev 2, but the current process places substantial administrative demands on contractors without consistently improving operational security. Greater use of automation, continuous monitoring, standardized guidance, and risk-based reporting would reduce compliance burden while providing a more accurate representation of an organization's cybersecurity posture.

Response E:

Phase I was straightforward. We maintain active NIST SP 800-171 and NIST SP 800-53 compliance with annual third-party assessments and have sustained a mature security and risk management program for over a decade. Minimal incremental effort was required.

Response F:

Organization-defined parameters: To achieve a transparent self-assessment, we leverage NIST SP 800-171A Rev. 2. However, given the complexity of organization-defined parameters (ODPs) most organizations would require consultants to understand how to implement the controls in a compliant manner. Small companies with limited resources are almost immediately priced out of this approach.

Scope creep: Over-scoping (applying all controls to the entire infrastructure) or under-scoping (omitting endpoints that process FCI/ CUI) is a costly technical challenge. Recommendation – Provide effective resources to help the DIB properly identify FCI and CUI in the environment.

Evidence documentation – having the staff to generate and maintain verifiable artifacts (logs) can become an administrative burden. Recommendation: Leverage automated evidence collection tools.

Response G:

We currently maintain a CMMC Level 1 self-assessment. We do not currently receive CUI, and on initial evaluation did not see Level 2 with C3PAO assessment as valuable. Our stance has been to evaluate this approach and remain ready to shift to Level 2 if needed.

Our environment already met or exceeded modern commercial best practice before CMMC was considered. Every FAR 52.204-21 requirement was met before we documented it. The Level 1 self-assessment was a documentation exercise that did nothing to improve our security posture. It was performed purely for compliance. The assessment in its current form measures documentation, not security.

Question 6: Reforms to Reduce Costs and Barriers

Response A:

We recommend the CMMC Reform Task Force consider the following changes within the next 60 days to reduce barriers for commercial healthcare providers:

- Establish a 'Healthcare Safe Harbor' Scoping Guide. Establish a Healthcare Safe Harbor Scoping Guide. For non-traditional DoW contractors where potential CUI is co-mingled with commercial PHI, the DoW should provide a specialized scoping guide. This guide needs to decouple PHI from CUI and let contractors assess their co-mingled systems against the NIST SP 800-171 standard strictly at the logical data layer. Limiting assessments to logical, data-level controls like database access control, data-at-rest encryption, and user authentication rather than physical and system-wide infrastructure audits removes the scoping barrier while keeping data secure. The guide would also need to clarify that contractors can meet the NIST SP 800-171 controls with or without FIPS encryption, accepting network-level mitigating controls when FIPS is not possible on specialized medical devices.
- Define a CMMC exemption for standard commercial services. Utilizing the authority of DFARS Part 212 and FAR Part 12 and the preference in DFARS 212.272(b)(1) and precedence in FAR 12.102(c), explicitly exempt standard, unmodified commercial services that are identical to those offered in the civilian marketplace, aligning the policy with the existing exemption for COTS products.

Response B:

The Task Force should recommend a focused reform package that removes activities that do not improve security, aligns the level of independent verification with actual information risk, constrains assessment variability, and corrects Government-side CUI identification and delivery failures. These reforms would reduce barriers without reducing accountability for protecting federal data.

1. Reorient the entire program around implementation-centered security assurance

For each requirement, the Department should define the security outcome, applicability, common acceptable implementations, equivalent technology-neutral alternatives, validation method, monitoring expectation, and evidence that assessors must consistently accept. Contractors should be accountable for implementing, testing, monitoring, and remediating safeguards. The program should eliminate duplicative narratives, assessor-created documentation expectations, and formatting exercises that do not contribute to those outcomes.

2. Make the existing Level 2 assessment decision transparent and risk-based

CMMC already provides Level 2 self-assessment and Level 2 C3PAO certification paths, and the Government identifies the required level for the contract. The Department should publish binding, contract-usable criteria explaining when each path applies and ensure the decision reflects the applicable CUI category and authority, operational context, aggregation, and consequence of compromise. Level 2

self-assessment, supported by standardized technical validation and system-generated evidence, should be used when those factors do not justify the cost of independent certification. If Level 2 third-party assessments remain broadly required, they must be redesigned around uniform technical validation, standardized Government-issued documentation formats, and reliable operating evidence, not assessor-specific documentation preferences.

3. Bind assessors to uniform Government-defined standards

When a third-party assessment is required, the assessor should evaluate the operating security environment: applicable configurations, technical validation, monitoring, remediation, and reliable supporting evidence. The assessment objectives are already standardized through NIST SP 800-171A; the remaining inconsistency lies in evidence sufficiency, interpretation, and the absence of a binding dispute-resolution mechanism. The Department should publish authoritative evidence guidance and provide a binding interpretation and appeal channel. C3PAOs should not impose individual preferences regarding particular technologies, screenshot collections, or the number of artifacts used to describe one implementation.

4. Standardize the minimum documentation set

Implementation-centered assurance still requires accurate documentation, but every contractor should not have to design a unique compliance architecture. The Department should issue common, scalable formats for the system security plan, plan of action and milestones, policies and procedures, configuration records or checklists, validation results, and evidence index. Contractors would document their own environments within the same structure, and assessors would evaluate the same information in the same locations. These formats should be minimal and capable of being populated directly by system-generated evidence, so standardization reduces authoring effort rather than adding another documentation layer. This would reduce consulting and preparation costs, simplify updates, and make certification results more consistent without substituting documents for technical verification.

5. Recognize reusable commercial evidence

The Department should publish standardized mappings between assessment objectives and common categories of commercial system-generated evidence. A verified configuration or authoritative report should be reusable wherever it demonstrates the required outcome. Industry and vendors can maintain product-specific mappings as technologies change, while the Government maintains the common outcome, validation, and evidence standard.

6. Enforce accurate CUI designation and make the Government accountable for identification and delivery

Agencies should identify anticipated CUI and its category before solicitation or award, distinguish CUI from FCI, and provide conspicuous notice before a contractor accesses or downloads CUI. DoD policy already requires this specificity: DoD Instruction 5200.48, Paragraph 3.4.f, requires the designation indicator on a DoD document containing CUI to identify every CUI type or category present. The problem is not the absence of a rule but its inconsistent application. Information can reach contractors bearing a generic CUI banner without the category identification required in the designation indicator. The Department should enforce the existing requirement, additionally identify the underlying safeguarding

authority, train requirement and contracting personnel, and periodically audit marking accuracy. A marking that omits the required category should trigger controlled quarantine or return and expedited Government review, not, by itself, permanently expand the contractor's assessed CMMC boundary.

Where a designation appears unsupported, including apparently public information marked as CUI, or CUI received without required markings; the Department should operationalize the existing challenge and decontrol procedures in 32 CFR 2002.50 and 2002.18 at the acquisition level, with a responsible official and defined response time. While a good-faith challenge is pending, the contractor should protect the specific information within an authorized CUI channel or controlled quarantine and refrain from disclosing it, but should not be required to permanently enlarge its assessed boundary or absorb recurring cost until the designation is confirmed. This preserves protection of information that proves to be CUI while preventing an unsupported marking from silently enlarging scope.

Routine procurement and business information, including pricing, labor rates, cost data, financial records, and proprietary business information, may or may not be CUI depending on the specific information, its context, and the governing authority. Some falls within recognized CUI categories such as Source Selection or Proprietary Business Information; some does not and is properly treated as FCI, contractor proprietary information, or both. Because the cost of an incorrect or unsupported designation falls on the contractor, the designating agency, not the contractor, should make and communicate that determination, with the category and authority identified. The objective is accurate designation, not reduced protection.

Legitimately sensitive information, including controlled technical information, export-controlled information, protected source-selection information, and PII governed by applicable privacy authorities, should continue to receive the protections its governing authority requires. But the existence of those categories does not justify reflexively marking every nonpublic procurement, financial, proprietary, or technical record as CUI when no category applies. Over-designation imposes real users, systems, backup, monitoring, retention, and assessment scope without a corresponding security benefit, and it dilutes attention to the information that genuinely warrants protection.

This is essential for scoped enclave models. The Government expects contractors to segregate CUI while its acquisition and contract systems may recognize only one undifferentiated company contact. CUI should be transmitted only through contractor-designated authorized channels, and Government and acquisition systems should permit separate FCI and CUI delivery endpoints at the entity and contract levels as access-controlled contract data, not a publicly searchable directory. Government identification, marking, notice, and delivery discipline must operate as part of the same information-protection system imposed on contractors.

Response C:

1. Reduce or eliminate mandatory third-party assessments for lower-risk contractors

The Task Force should replace the broad mandatory certification model with a risk-based validation model. Lower-risk contractors should be permitted to use executive self-attestation supported by retained evidence and subject to targeted audits. Third-party assessments should be reserved for higher-

risk information, complex environments, significant incidents, repeated deficiencies, or other objective indicators that independent validation is warranted. This change would remove the largest direct cost while preserving enforcement and accountability.

2. Recognize commercial certifications, cloud environments, and security solutions

The Department should create a formal reciprocity and equivalency process for recognized commercial certifications, independently assessed service providers, commercial cloud environments, managed services, and proven security technologies. SOC 2 Type II and similar independent validations should provide meaningful credit for overlapping controls. Contractors should need to demonstrate only the CMMC-specific or federal data requirements not already addressed. This would reduce duplicative work and allow organizations to select solutions based on security effectiveness and business needs rather than assessment preference.

3. Establish stable implementation guidance and authoritative interpretations

The Task Force should publish prescriptive implementation guidance, standardized templates, and a single authoritative source of interpretations. Guidance should remain stable for defined periods, and material changes should include prospective effective dates and reasonable transition periods. The Department should also provide a transparent process for publishing questions, interpretations, and updates so that assessors, consultants, vendors, and contractors work from the same expectations. Stability would reduce consultant dependency, rework, delayed investment, and the risk of purchasing tools that later prove misaligned with assessment expectations.

Together, these reforms would lower barriers without weakening protection. They would redirect limited small-business resources from redundant verification and administrative work toward controls that directly prevent, detect, respond to, and recover from cyberattacks.

Response D:

The DoW can reduce barriers to participation in the DIB without weakening protection of federal data by simplifying how organizations demonstrate compliance, limiting requirements to systems and suppliers that handle Federal Contract Information (FCI) or CUI, and providing practical implementation support. As DoW considers broader Government-wide cybersecurity requirements, these reforms also provide an opportunity to harmonize implementation across defense and civilian agencies, reducing duplicative compliance obligations for organizations that support multiple federal customers. The following recommendations represent actions that can be implemented within the next 60 days to reduce compliance costs and barriers to entry while preserving the comprehensive protections provided by NIST SP 800-171 Rev 2.

Expand eligibility for self-assessment: Reserve third-party certification for contracts and systems involving the most sensitive CUI or highest mission risk. Permit contractor self-assessments for other Level 2 environments, supported by targeted Government spot checks and enforcement against materially inaccurate affirmations. This approach would retain accountability while reducing assessment costs and capacity constraints that disproportionately affect smaller and non-traditional businesses.

Standardize and automate self-assessment documentation: Provide free, updated, comprehensive, Government-hosted SSP, POA&M, scoping, evidence, and scoring templates aligned directly with NIST SP 800-171 Rev 2. Establish standardized examples of acceptable evidence and permit dashboards, configuration reports, audit logs, and other machine-generated artifacts as primary evidence. Develop an SPRS interface or application programming capability that reduces manual entry and allows contractors to update scores and remediation information efficiently.

Clarify CUI identification, scoping, and flowdown: Require solicitations and contracts to identify the FCI and CUI expected to be processed, stored, or transmitted and the systems subject to CMMC requirements. Publish standardized criteria for secure CUI enclaves and clarify that requirements apply only to systems within the applicable assessment boundary. Prime contractors should flow requirements only to subcontractors that receive covered information and only at the level appropriate to that information. Flowdown requirements should remain proportional to the FCI or CUI shared with each subcontractor rather than extending identical requirements throughout every tier of the supply chain regardless of risk. Clearer boundaries would reduce unnecessary enterprise-wide implementations and prevent over-scoping throughout the supply chain.

Recognize validated commercial and Government-authorized capabilities: Publish interim crosswalks identifying where FedRAMP, StateRAMP, ISO/IEC 27001, independently assessed commercial platforms and managed security services provide evidence applicable to NIST SP 800-171 Rev 2 requirements. Contractors should be able to rely on inherited controls, provider attestations, and tool-generated evidence rather than recreate documentation for capabilities already independently validated. Guidance should also recognize inherited security controls provided by cloud service providers and avoid requiring contractors to duplicate protections already delivered through appropriately authorized or independently assessed cloud services. Reciprocity should provide credit for overlapping controls without treating every certification as automatically equivalent to full CMMC compliance.

Improve supply chain verification: Allow authorized DIB companies to query SPRS using CAGE codes or another unique identifier to confirm whether a prospective subcontractor has a current assessment or certification at the required level. This would replace repeated requests from multiple primes and provide a consistent method for verifying supplier status without disclosing unnecessary proprietary information.

Provide targeted financial and technical support: Establish an assessment voucher or cost-sharing pilot for qualifying small and non-traditional businesses and publish low-cost reference architectures for common environments, including cloud-hosted CUI enclaves. The DoW should also clarify that reasonable cybersecurity implementation and assessment costs are allowable contract costs when required for performance.

These actions would lower upfront and ongoing costs, reduce duplicative documentation, improve assessment consistency, preserve access to specialized suppliers, and better harmonize cybersecurity expectations across organizations supporting both defense and civilian agencies. By maintaining NIST SP 800-171 Rev 2 as the security foundation while simplifying the mechanisms used to scope, demonstrate, and verify compliance, the DoW can strengthen protection of federal data and sustain the diverse industrial base required to support the warfighter.

Response E:

Grant reciprocity for firms already assessed against equally or more rigorous frameworks. Adopt a DoD-specific overlay rather than duplicating NIST SP 800-171 through CMMC. Define a simplified process for adding cage codes to existing certifications when operating under established IT/security standards.

Response F:

To reduce costs and barriers for small, medium and non-traditional businesses, recommend the Task Force,

Eliminate third party assessment mandates for small, medium, and non-traditional businesses.

Expand reciprocity for recognized security frameworks (FedRAMP Moderate baseline, StateRAMP, ISO 27001) as meeting the baseline for CMMC requirements.

Consider implementing a graduated phase-in period for small, medium, or non-traditional businesses that have a small or minimum contract value threshold or a number of employees under a certain threshold.

Response G:

Our recommendations on cost and scope follow directly. Tier obligations to the volume and sensitivity of CUI actually handled, with expanded self-attestation for low-volume handlers. Hold designating agencies accountable for marking accuracy in both directions, give contractors a fast and formal process to challenge markings, and identify CUI at the contract line item level before award so compliance can be scoped before it is priced. Then commit. Publish a binding multi-year timeline and keep it. Predictability will encourage small businesses to participate.

Question 7: Reforms to Improve Operational Resilience

Response A:

The Task Force should recommend policy changes that prioritize operational resilience and system survivability over check-the-box compliance:

- Establish an active defense offset. Amend CMMC Level 2 guidelines to allow compliance credits for minor technical configuration gaps on legacy hardware if the contractor maintains a verified active defense program, such as 24x7 security monitoring, threat hunting, and rapid isolation capabilities.
- Accept network isolation and virtual patching. Issue clear assessment guidance accepting logical network micro-segmentation and stateful firewall isolation as fully compliant, permanent compensating controls for NIST SP 800-171 flaw remediation requirements.
- Shift cyber incident reporting to a collaborative model. Modify the implementation of DFARS 252.204-7012 to focus on threat mitigation. Establish a real-time, bi-directional threat intelligence feed between the DoD Cyber Crime Center and commercial security centers to proactively block emerging threats.

Response B:

Our organization does not view cost reduction and operational resilience as competing objectives. Properly designed reform would improve both. Much of the current cost comes from activities that do not harden systems, detect attacks, restore operations, or protect data. Redirecting resources from duplicative documentation and assessment preparation toward implementation, monitoring, remediation, response, and recovery would produce greater security value.

Prioritize measurable operation of safeguards

CMMC should measure whether safeguards are correctly implemented and continue to operate. The Department should emphasize hardened identities, managed endpoints, secure cloud access, data protection, vulnerability remediation, threat detection, incident response, tested backups, and recovery planning. Validation should test function, monitoring should identify failures or configuration drift, and remediation should restore the required state within defined risk-based timeframes.

Convert commercial telemetry into operational evidence

Commercial platforms already report identity risk, device compliance, configuration status, vulnerabilities, threats, audit activity, backup success, and other operating conditions. Standardized acceptance would allow the same information to support security operations and compliance verification, linking CMMC evidence directly to the information contractors use to detect and correct risk instead of requiring assessment-only artifacts.

Provide an actionable hardening and validation framework

Small businesses should not have to purchase competing interpretations to understand how to protect federal data. The Department should maintain practical, technology-neutral guidance covering

applicability, acceptable implementation patterns, equivalent approaches, validation, monitoring, and minimum evidence. This would help contractors implement protections correctly from the beginning and give assessors, consultants, vendors, and contractors one common baseline.

Prevent avoidable handling incidents at the source

Accurate Government identification and controlled delivery of CUI would improve resilience. Advance notice and contractor-designated channels allow information to enter the authorized environment intentionally, reduce preventable spillages, preserve enclave boundaries, and apply required protections from receipt. Unnecessarily designating ordinary information as CUI enlarges enclave scope, complicates authorized workflows, and creates additional opportunities for misrouting, access error, and configuration drift. Government handling must reinforce, not undermine, the architecture contractors are required to maintain.

The reform objective

The same reforms that reduce cost would improve resilience by redirecting effort toward the security lifecycle that matters: harden, validate, monitor, detect, respond, recover, and improve. Compliance reporting should verify that lifecycle, not separately measure document production. Reforming CMMC around implementation-centered security assurance would allow the Department to demand stronger proof of actual protection while making participation more feasible for small, medium, and non-traditional businesses.

Response C:

Make continuous employee training and awareness the central resilience investment

The single most effective investment for improving our operational resilience is ongoing employee cybersecurity training and awareness. Technology alone cannot protect an organization from phishing, social engineering, credential theft, business-email compromise, and other attacks that target human behavior. Our greatest improvement occurred when cybersecurity became part of our corporate culture rather than solely an information technology responsibility.

The Department should encourage and, where practical, support recurring role-based training, simulated phishing exercises, concise threat updates, incident-reporting practice, and leadership engagement. Small businesses would benefit from government-provided or government-funded training resources that are current, practical, and tailored to the Defense Industrial Base. Training effectiveness should be measured through behavior and outcomes—such as reporting rates, response time, and improvement in simulation results—rather than attendance records alone.

Shift incentives from compliance production to resilience outcomes

Policy should favor investments in awareness, threat detection, email protection, identity security, incident response, backup and recovery, vulnerability management, and managed security services. Contractors should be able to demonstrate resilience through practical exercises, tested recovery capabilities, and evidence of continuous improvement. Every dollar redirected from duplicative

certification or documentation toward these capabilities has the potential to produce a greater security return.

CMMC reform should be measured not by certificates issued or artifacts produced, but by whether contractors can better prevent, detect, respond to, and recover from cyberattacks. A resilience-centered model would protect federal data while making DIB participation more sustainable for small and non-traditional businesses.

Response D:

The CMMC Reform Task Force has an opportunity to strengthen operational cyber resilience across the DIB by emphasizing policies that improve organizations' ability to prevent, detect, respond to, and recover from cyber threats rather than expanding administrative compliance requirements. Operational resilience is strengthened when organizations invest in technical capabilities, timely information sharing, and continuous improvement rather than duplicative reporting and documentation. The following recommendations represent actions that can be implemented within the next 60 days to improve operational resilience while preserving the comprehensive protections provided by NIST SP 800-171 Rev 2.

Prioritize measurable security outcomes. Continue using NIST SP 800-171 Rev 2 as the cybersecurity baseline while placing greater emphasis on the implementation and effectiveness of high-impact safeguards, including multi-factor authentication, endpoint detection and response, privileged access management, vulnerability management, secure backups, and incident response capabilities. Assessments should prioritize demonstrated operational effectiveness over the volume and source of supporting documentation.

Modernize incident reporting. Harmonize reporting requirements with existing DFARS clause 252.204-7012 to eliminate duplicative reporting while providing clearer guidance on reporting thresholds, timelines, and responsibilities. Define what constitutes a reportable "lapse in information security," clarify when the reporting period begins, and establish a centralized reporting mechanism that supports coordinated Government response while reducing administrative burden. Clarifying reporting responsibilities throughout the supply chain would improve consistency, reduce confusion during active incidents, and improve the accuracy and timeliness of reporting.

Promote Zero Trust and resilient architectures. Encourage adoption of Zero Trust principles through practical implementation guidance, standardized reference architectures, and recognition of secure commercial cloud and managed security services. Support secure CUI enclaves, network segmentation, least-privilege access, and continuous monitoring to reduce attack surfaces and limit the impact of successful compromises.

Measure resilience through continuous improvement. Supplement periodic compliance assessments with indicators that demonstrate operational readiness, including vulnerability remediation, incident response exercises, backup restoration testing, and deployment of key security capabilities. These measures

provide a more accurate picture of an organization's ability to withstand and recover from cyber events while encouraging continuous improvement rather than point-in-time compliance.

These recommendations preserve the comprehensive protections provided by NIST SP 800-171 Rev 2 while shifting emphasis from demonstrating compliance to strengthening operational cybersecurity. Expanding information sharing, modernizing incident reporting, encouraging resilient architectures, and emphasizing measurable security outcomes improve the DIB's ability to prevent, detect, respond to, and recover from cyber threats while allowing organizations to focus more resources on defending federal information and supporting the warfighter.

Conclusion

The objective of CMMC is not simply to measure compliance; it is to strengthen the cybersecurity of the DIB in support of the warfighter. Achieving that objective requires a framework that preserves rigorous cybersecurity requirements while directing contractor resources toward activities that produce measurable reductions in cyber risk.

The recommendations presented throughout this document provide a consistent path toward that goal. NIST SP 800-171 Rev 2 remains the foundation for protecting CUI, while the mechanisms used to demonstrate compliance evolve to reflect modern cybersecurity practices. Greater use of automation, continuous monitoring, machine-readable reporting, standardized implementation guidance, recognition of equivalent commercial capabilities, reciprocity, and risk-based compliance models reduces administrative burden while improving the quality, consistency, and timeliness of compliance information.

A modernized compliance framework reinforces the DoW's broader mission by aligning compliance activities more closely with measurable cybersecurity outcomes. This approach strengthens the DIB's resilience, expands access to commercial innovation and supplier diversity, and enables industry to invest more resources in defending operational environments. The result is a stronger cybersecurity posture, a healthier industrial base, and a more capable partner in delivering secure capabilities to the warfighter.

Response E:

Extend reciprocity to organizations with Third-Party Assessment Organization (3PAO) assessments against NIST SP 800-171 and NIST SP 800-53. Broaden contractor access to DoD Secure Access File Exchange (SAFE) for CUI transmission. Mandate DoD SAFE use for all government personnel, primes, and subcontractors sharing CUI.

Response F:

In DFARS 252.204-702 it says, CUI will be "(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract" but in practice no such marking is provided by the government. This regulation should be completely re-written or adhered to by the US Government

NARA's catalogue of CUI is archaic. To operate in the world of AI, Data Governance is required, but it must occur at machine speed not manual marking of documents. Instead, there is technology that provides data security, privacy, and governance. Such solutions are available on the FedRAMP Marketplace.

Response G:

Finally, the RFI's stated goal of operational resilience against cyber attacks cannot be met by NIST SP 800-171, which Level 2 is based on. We are not suggesting the standard be scrapped. Confidentiality of federal data is a legitimate interest and 800-171 addresses it. But Rev 2 states its purpose is protecting the confidentiality of CUI, and excludes the contingency planning family from scope. Rev 3 says it plainly: the Contingency Planning family is not included because it addresses availability. Availability is what resilience means. The one backup requirement that survived, 3.8.9, requires only that the confidentiality of backup CUI be protected. Nothing in the standard requires that backups exist, that restoration be tested, or that operations can recover. A contractor can hold a perfect SPRS score and have zero ability to survive a ransomware event, in full compliance the entire time. If the Department wants a DIB that can absorb an attack and keep delivering, it needs a small set of outcome-based resilience requirements: tested restoration from protected backups, defined recovery objectives for contract-critical work, and response plans that are actually exercised. Fund that by retiring low-value documentation requirements, not by stacking new burden on top.

Additional Member Feedback

Response A:

Feasibility

The proposed reforms, including the Standard Commercial Services exemption, decoupling PHI from CUI, and HIPAA/RMF reciprocity, are highly feasible because they utilize existing statutory authorities under DFARS Part 212, FAR Part 12, and standard federal risk management frameworks.

Risks of Inaction

Applying CMMC Level 2 standards uniformly, without incorporating clinical healthcare-specific harmonizations, may introduce operational and financial friction that compels some commercial providers to re-evaluate their participation in government programs. Because these organizations must safeguard extensive clinical healthcare networks from disruptive, non-clinical requirements, the cost and operational complexity of compliance could ultimately outweigh the viability of supporting federal programs.

Security Innovation

Integrating NIST CSF 2.0 design principles with NIST RMF assessment processes proves that active, outcome-based defense (including rapid network isolation and logical data protection) provides superior operational resilience compared to static, paper-based compliance checklists.

Response B:

The central problem with CMMC is not simply that compliance is expensive. The current model requires each contractor to interpret, engineer, document, and repeatedly defend what an acceptable secure environment looks like, and substantial investment still does not ensure that another assessor will reach the same conclusion. Limited cybersecurity resources are therefore consumed by interpretive uncertainty, duplicative documentation, fragmented third-party solutions, and assessment preparation rather than implementation, monitoring, and continuous improvement of hardened systems.

Our organization does not advocate weakening the protection of Controlled Unclassified Information or returning to unsupported self-attestation. Security requirements should be meaningful, verifiable, and enforced. However, accountability should focus on whether safeguards are correctly implemented, operating effectively, monitored, and supported by reliable evidence, not on whether each contractor has built a unique compliance program around the preferences of a particular consultant or assessor.

Our unifying position is that CMMC should translate abstract requirements into clear, practical implementation expectations; establish consistent validation and evidence standards; and better recognize the security capabilities already built into commercial platforms. This would reduce cost and administrative burden while making certification a more consistent and meaningful indicator of security across the DIB.

Response D:

Executive Summary

The Department of War's (DoW's) ability to deliver secure capabilities to the warfighter depends on both strong cybersecurity and a resilient, diverse Defense Industrial Base (DIB). Cybersecurity requirements must evolve to combat emerging cyber threats, and the requirements should lead to increased data protection, including Controlled Unclassified Information (CUI). When the administrative burden outpaces measurable reductions in cyber risk, the DoW risks limiting access to innovation, supplier diversity, and commercial capabilities without gaining a corresponding improvement in cybersecurity.

The responses in this document identify opportunities to modernize the Cybersecurity Maturity Model Certification (CMMC) program while preserving the comprehensive cybersecurity protections provided by NIST SP 800-171 Rev 2. Across every topic, a consistent theme emerges: the greatest burden associated with CMMC stems not from implementing cybersecurity controls, but from documenting, validating, and repeatedly demonstrating compliance with those controls.

Several reforms would better align the compliance framework with measurable cybersecurity outcomes. Greater use of automation, continuous monitoring, and machine-readable reporting would reduce manual compliance activities while improving the accuracy and timeliness of assessment information. Increased recognition of mature commercial cybersecurity platforms, managed security services, and existing Government security authorizations through capability equivalency and reciprocity would better reflect current cybersecurity practices. Streamlined self-assessment processes, standardized implementation guidance, and risk-based reporting models would improve consistency while allowing organizations to focus resources on operational cybersecurity rather than administrative documentation.

Collectively, these recommendations would strengthen the cybersecurity of the DIB by directing industry investment toward reducing cyber risk instead of sustaining duplicative compliance activities. Modernizing the compliance framework in this manner will improve efficiency, strengthen supplier participation, encourage innovation, and ultimately better support the Department's mission to deliver secure capabilities to the warfighter.

Response G:

Most responses to this RFI will come from companies that are inside the CUI ecosystem, not those that have opted out. Companies that have already completed a Level 2 assessment have an incentive to defend that investment, and sunk cost may cloud their feedback.

Response H:

Questions/Clarifications:

Will the DOW consider a Level 2 Self-Assessment appropriate for contractors that are creating, storing, or processing CUI which does not contain any data included in the Defense category in the National Archives CUI Registry Index (for example: only in the Privacy category)?

The current rule requires CMMC to be flowed down to subcontractors supporting a prime contractor complying with CMMC; however, generally, prime contracts have 4 distinct phases: (1) RFP Submission (proposal submission to DoW), (2) Award of Prime Contract, (3) Transition-In (implementation of new requirements), and (4) Start of Services (creating, processing, or storing CUI to perform services outlined in the contract requirements)

In order to prioritize speed to capability and lower barriers to entry for small, medium, and non-traditional businesses, would DOW consider directing Prime contractors to obtain CMMC certification from their subcontractors prior to the subcontractors initially creating, storing, or processing CUI?

Response I:

Our organization was an early adopter of CMMC and began preparing well before certification requirements were finalized. To date, we have invested upwards of $250,000 in cybersecurity infrastructure, consultants, policies, assessments, training, and remediation efforts in preparation for CMMC Level 2 certification.

As a small business, this has been an enormous financial and operational undertaking. We made these investments in good faith because we understood that CMMC certification would be necessary to remain competitive in the defense industrial base. Unfortunately, the process has been marked by repeated delays, changing requirements, and continued uncertainty.

Our organization supports strong cybersecurity requirements. However, the government must also consider the impact on companies that invested early and acted responsibly. Any revised approach should recognize prior investments, provide clear and dependable timelines, reduce unnecessary duplication, and avoid penalizing compliant small businesses while companies that delayed preparation face little consequence.

Response J:

Our organization supports the Department's objective of protecting federal information and improving operational resilience. However, we believe that a one-size-fits-all approach to securing all Controlled Unclassified Information (“CUI”) is unworkable for nontraditional defense contractors (“NDCs”) as currently implemented.

Strict security standards that are appropriate for state secrets (e.g., ITAR) are disproportionately burdensome for medical technology providers that primarily hold service member health information and personal data (together, “patient data”). The recommendations outlined below are directed at right-sizing verification and cryptographic requirements to identifiable risks posed to the patient data held by medtech.

Background

Our organization is an NDC supplying commercial and dual-use medical technology to the Department. We bring world-class, FDA-regulated medical technology developed in the commercial sector to the

military health system, delivering the same lifesaving and life-enhancing innovations to service members that we provide to private sector healthcare practitioners across the country.

We primarily sell commercial-off-the-shelf ("COTS") medical devices to the Department but also provide additional services that process the health data of service members, some of which is designated as Controlled Unclassified Information (“CUI”). The CUI received we receive from the Department predominantly consists of service member health information and personal information (together, “patient data”). These include NARA and DoD CUI categories of Privacy Information, Sensitive Personally Identifiable Information, and Health Information. We do not receive controlled technical information, defense information, or ITAR/EAR-controlled data in the performance of their contracts with the Department.

II. Cost Drivers and Disproportionate Burdens

CMMC's one-size-fits-all approach to safeguarding CUI does not account for the variable risk profile of data types handled by a diverse DIB. The levels of assurance required to safeguard state secrets and prevent nation-state military espionage are not necessarily appropriate for mitigating privacy risks to patient data held by medtech providers. In our experience, such an approach adds significant administrative overhead that consumes disproportionate cost without a corresponding improvement in security. We highlight four areas of particular concern that are significant cost drivers for the medtech sector below.

A. FIPS-validated cryptography (SC.L2-3.13.11)

CMMC practice SC.L2-3.13.11, drawn from NIST SP 800-171 Rev. 2, requires contractors to "[e]mploy FIPS-validated cryptography when used to protect the confidentiality of CUI". This implementation guideline requires use of specific software or hardware cryptographic modules must be validated through the NIST Cryptographic Module Validation Program ("CMVP"). Use of FIPS-approved algorithms such as AES-256 alone does not satisfy this requirement.

Deploying FIPS-validated cryptographic modules is the single largest cost driver that medtech providers face in meeting CMMC requirements. The infrastructure hosting and processing patient data were designed by our business to meet commercial requirements and rarely employs full FIPS-validated modules. Closing the FIPS gap within these environments would require extensive re-engineering of products or re-homing applications into substantially costlier government cloud enclaves solely to meet CMMC’s mandates. The compliance burden is further compounded by the September 21, 2026, sunset of FIPS 140-2, which will require re-verification of modules against FIPS 140-3.

Applications that process patient data already employ robust, industry-standard cryptography engineered to meet strict confidentiality, integrity, and availability obligations for patient data under HIPAA and other regulations. These deployed cryptographic algorithms are often identical to those utilized in FIPS-validated modules, just in software wrappers that have not been validated through the CMVP.

While CMVP hardening and validation may be appropriate to protect against foreign espionage when protecting CTI and ITAR data, it imposes disproportionate burdens on medtech providers holding only patient data. The innovative solutions our organization provides were designed to commercial standards

and privacy-centric requirements such as those found in HIPAA in which the encryption itself is an “addressable” requirement rather than a hard-and-fast rule.

We believe that it would be more proportionate to require NDCs holding patient data to use FIPS-approved algorithms rather than full FIPS-validated modules. NIST itself has moved away from a rigid module-validation mandate. In NIST SP 800-171 Rev. 3 (May 2024), the successor control (03.13.11, "Cryptographic Protection") no longer prescribes FIPS-validated modules on its face. Instead, it requires contractors to "implement the following types of cryptography to protect the confidentiality of CUI: [Assignment: organization-defined types of cryptography]," with the discussion noting only that FIPS-validated cryptography is "recommended". This is a deliberate shift to an organization-defined-parameter ("ODP") model that gives agencies discretion to prescribe cryptographic rules calibrated to risk. We propose that the Department exercise its discretion to define an ODP for 3.13.11 that right-sizes this requirement for NDCs processing patient data.

B. C3PAO certification versus self-assessment

Medtech companies also face significant burdens in obtaining third-party certification from a C3PAO. Certification carries direct assessment fees, substantial internal preparation costs, and recurring surveillance expense that are challenging for many organizations to meet. As the Department notes, the certified assessor ecosystem is structurally undersupplied relative to the population of contractors that would require assessment. This circumstance produces scheduling backlogs, cost inflation and assessment timelines difficult to reconcile with award schedules and contract performance windows.

Relative to the risk of CUI held by our organization, self-assessment is the more proportionate evaluation method for NDCs. The majority of medtech participation in the DIB involves COTS and dual-use products for which the associated CUI is limited in both volume and national security sensitivity. Imposing the most burdensome assessment tier on this population inverts the risk-based logic that should govern the framework. Compliance obligations should scale to the actual sensitivity of the data at issue, not to the contractor’s incidental status as a defense contractor. A self-assessment pathway under senior official’s affirmation and attendant False Claims Act exposure preserves accountability while calibrating burden to risk.

Furthermore, medtech providers often already maintain several industry-standard security certifications such as SOC 2 Type II and ISO 27001. Each of these audit programs already require substantial evidence collection and independent control testing. For an organization with a limited CUI footprint, CMMC Level 2 certification merely imposes additional administrative burden to assess substantially similar security controls applicable in existing commercial frameworks. The cost is not only the assessment cost but the organizational burden of repeatedly demonstrating the same controls to different assessment bodies, compounded by a constrained C3PAO market and assessment backlogs. We recommend extending the Department’s Phase II pause on C3PAO certification indefinitely for NDCs holding patient data.

C. DFARS 252.204-7012 cloud service provider (CSP) flowdown.

DFARS 252.204-7012(b)(2)(ii)(D) provides that when a contractor uses an external CSP to store, process, or transmit covered defense information, the contractor must "require and ensure" that the CSP meets security requirements "equivalent" to the FedRAMP Moderate baseline and complies with clause

paragraphs (c) through (g) covering cyber incident reporting, malicious software submission, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment. Under the DoD CIO's December 2023 FedRAMP equivalency memorandum, a non-authorized CSP must achieve full compliance with the FedRAMP Moderate baseline as validated by a FedRAMP-recognized 3PAO, with a full body of evidence and annual reassessment. The memorandum places the burden squarely on the contractor (not the CSP) to ensure conformance and to report cloud-related incidents.

DFARS 252.204-7012 assumes contractor ownership and control of infrastructure and is not well-suited to the cloud-first IT strategies that medtech providers employ. Several of the paragraph (c)–(g) obligations are difficult or impossible to satisfy in a shared, multi-tenant commercial SaaS environment, where a contractor cannot image another tenant's media or hand over shared infrastructure. Satisfying these obligations can force migration to a sovereign or government cloud enclave, which is a significant architectural and engineering undertaking for companies that predominantly serve commercial customers and hold limited CUI.

Notably, the same commercial CSPs that cannot provide physical media already provide robust, documented logging, monitoring, evidence preservation, and incident-response capabilities that fully support cyber incident analysis and reporting. In our experience, these capabilities are quite sophisticated and more than sufficient to investigate CUI leaks and report cybersecurity incidents to the Department under the clause.

We propose that the Department clarify in a revised memo that CSP-native forensic and logging capabilities satisfy the forensic-preservation and incident-investigation objectives of paragraphs (c)-(g) for NDCs holding patient data and limited CUI in their CSP tenants. This approach is more commensurate with the risks to the data and would avoid costly migrations that could significantly raise the cost of service to the Department or prevent the government from obtaining life-saving medical technology.

D. QMSR and validated operational technology (OT) environments

Implementing CMMC's documentation requirements to regulated medical device manufacturing environments raises duplicative burdens for medtech providers. To meet FDA's Quality Management System Regulation ("QMSR"), ISO 13485, and applicable GxP requirements, medtech companies maintain extensive risk-management validation, change-control, and corrective-action documentation for their production and quality environments. These processes are well-documented and essential for maintaining FDA validation of the manufacturing environment.

The Department rightly recognized that operational technology ("OT") and IoT devices may be "unable to be fully secured" to the standards of NIST SP 800-171. The Specialized Asset classification was created to exempt such assets from many substantive security obligations while ensuring that they are fully inventoried, documented in the System Security Plan, and managed under a risk-based security policy aligned with CMMC. Yet, each of these requirements are already satisfied by existing QMSR and ISO 13485 requirements.

We propose that the Department clarify that FDA-regulated QMS documentation satisfies CMMC's documentation objectives for Specialized Assets. This would clarify for medtech companies that QMSR-

compliant documentation is adequate for CMMC purposes and avoid implication that separate risk assessments are required to meet CMMC standards.

IV. Recommendations

In conclusion, we recommend that the Department make the following targeted revisions to the CMMC Program for NDCs primarily holding patient data:

FIPS-Approved Algorithms. The Department should deem SC.L2-3.13.11 satisfied where NDCs primarily holding patient data deploy FIPS-approved cryptographic algorithms. Full FIPS module validation should be reserved for CUI categories the Department designates as higher risk.

Self-Assessment to NIST 800-171. The Department should permit NDCs whose CUI is primarily limited to patient data to demonstrate CMMC Level 2 compliance through annual self-assessment and senior-official affirmation. Mandatory C3PAO certification should be reserved for higher-risk CUI environments (e.g., CTI, defense, or ITAR/EAR data).

CSP Safe Harbor. The Department clarify that NDCs satisfy the forensic-preservation and incident-investigation objectives of DFARS 252.204-7012(c)-(g) where they utilize commercial cloud services that provide documented logging, monitoring, evidence preservation, incident response, and investigative capabilities sufficient to support cyber incident analysis and reporting. NDCs primarily holding patient data should not be required to implement separate infrastructure, maintain duplicative forensic capabilities (such as physical media preservation or packet capture in multi-tenant SaaS), or migrate patient data into government cloud enclaves.

QMSR Reciprocity for Validated OT Environments. Where a system is operated under an FDA-regulated quality management system, the Department should permit contractors to satisfy CMMC's Specialized Asset documentation and risk-assessment requirements through existing QMS/QMSR records.

VI. Conclusion

Right-sizing CMMC for the realities of commercial-first, FDA-regulated medical technology will allow medtech NDCs to continue delivering leading innovation to the military health system while fully meeting the Department's legitimate objectives of protecting federal information and improving operational resilience. Each of the reforms above reduces cost and barriers for medtech NDCs without degrading the protection of federal information, and each is consistent with the Department's continued reliance on DFARS 252.204-7012 and NIST SP 800-171.

Response K:

Thank you for reaching out and for providing the means for us to share our assessment experiences and feedback regarding the CMMC certification process. Our organization recently successfully achieved our CMMC Level 2 certification. However, we have observed a potential area for this feedback in the process, particularly in the addition of CAGE codes for wholly owned subsidiaries post-certification.

Following our CMMC Level 2 certification, our organization has undergone no changes in key aspects like personnel, technology, or established processes, as subsidiaries were set up. Yet, every new CAGE CODE

for these entities necessitates a costly, separate full assessment. This requirement adds to our expenses without enhancing our cybersecurity practice or federal data protection in any noticeable manner.

Therefore, we would like to raise the following questions for the CMMC Reform Task Force to consider:

Is it necessary for wholly owned subsidiaries that bring no material change to an already certified environment to undergo separate full CMMC assessments, and what is the specific written regulatory basis for this requirement?

Could the Task Force implement a formal administrative amendment process that permits organizations to add CAGE codes of subsidiaries to existing certifications when no changes to the certified environment have occurred?

How does requiring separate assessments for adding administrative CAGE codes align with the DoD's objective of lessening the compliance load on the Defense Industrial Base, especially when these requirements impose considerable financial impact sans discernible security benefit?

Would the Task Force be able to offer written guidance clarifying how DFARS, which mandates reporting of all CAGE codes associated with an SSP, should be interpreted relating to subsidiary companies operating within a certified parent company's environment?

Your consideration of our experiences and proposals would be greatly appreciated.

Response L:

Issue: DARS Tracking Number: 2024-O0013, Revision 1, Class Deviation—Revision 1, Safeguarding Covered Defense Information and Cyber Incident Reporting requires defense contractors use NIST 800-171 Revision 2 instead of NIST 800-171 Revision 3.

Discussion: There are substantial advantages to using NIST 800-171 Rev to include: stronger support for modern cloud-based architectures and zero trust principles, incorporation of supply chain risk, and alignment to NIST 800-53 Revision 5 controls.

Recommendation: Issue a Revision to the Class Deviation that requires the use of NIST 800-171 Rev 3 or the latest published version of NIST 800-171. The proposed language would make the Class Deviation more durable.

Issue: 32 CFR Part 170 requires the invalidation of a CMMC assessment when an organization’s scope and/or architecture changes citing mergers and acquisitions as one potential trigger.

Discussion: Change in organization scope is generally viewed as the addition of CAGE Codes. When an acquisition does not include IT assets, the scope of the organization changes but there is no impact to the NIST 800-171 security requirements. Similarly, when an acquisition does include IT assets, the addition of assets that fully inherit the assessed NIST 800-171 security requirements, requiring a full re-assessment of the enterprise or enclave versus assessing acquired assets creates an unnecessary burden on defense contractors.

Recommendation: Update 32 CFR Part 170 to exclude acquisitions that involve CAGE Codes but no IT assets from invalidating CMMC assessments. Update 32 CFR Part 170 to require the assessment of

changes in architecture resulting from mergers and acquisitions but not invalidate the existing CMMC assessment.

Issue: The Supplier Performance Risk System (SPRS) is not searchable by defense contractors

Discussion: Defense contractors are required to ensure their teaming partners and subcontractors comply with the CMMC requirements. Currently, companies rely on contractual attestations because SPRS is not searchable by non-governmental organizations. Allowing defense contractors to validate NIST 800-171 and CMMC compliance by searching SPRS will help secure DoD/DoW's supply chain.

Recommendation: Allow defense contractors to search SPRS

Response M:

Not all organizations operating within CMMC Level 2 present the same level of risk to the DoW. Today, an organization handling limited quantities of CUI within a small, tightly controlled environment may face substantially the same assessment burden as an organization whose business is centered on highly sensitive defense technologies and extensive CUI processing.

While both organizations should protect CUI in accordance with NIST SP 800-171, the Department should consider additional differentiation within Level 2 based on factors such as:

Type and sensitivity of CUI being handled

Volume of CUI processed, stored, or transmitted

Number of authorized CUI users

Overall size of the CUI assessment boundary

Operational impact of compromise

Degree of reliance on DoD contracts versus broader commercial operations

Organizations with limited CUI exposure and tightly scoped environments should not necessarily be subject to the same recurring third-party assessment burden as organizations supporting highly sensitive defense programs.

We recommend the Department consider expanding eligibility for self-assessments within CMMC Level 2. Organizations that demonstrate:

Limited numbers of CUI users

Small and well-defined CUI enclaves

Mature implementation of NIST SP 800-171 controls

Documented policies and procedures

Executive affirmation of compliance

Should be allowed to satisfy compliance through enhanced self-assessment, periodic attestation, evidence retention, and targeted government review when necessary.

Third-party assessments should remain available and required for higher-risk environments, but the current model places significant financial and administrative burden on smaller contractors whose environments present substantially lower risk.