Response to the Office of the DoD CIO Request for Information: Reforming CMMC and Reducing Compliance Burden for the Defense Industrial Base

1) Cost Drivers, Administrative Burdens, and Operational Challenges.

Lack of Internal Expertise and Budget. Small businesses expected to obtain a CMMC certification often lack the internal expertise necessary to properly interpret NIST SP 800-171 requirements, define an appropriate CMMC assessment boundary, identify Controlled Unclassified Information (CUI), and understand what constitutes assessment-ready evidence.

This lack of internal expertise is largely a function of available resources rather than organizational commitment. During my time supporting the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), I conducted research at the direction of the Deputy Secretary of Defense to estimate the average cybersecurity budget of a small defense contractor. The estimated annual budget of a small business was approximately $100,000 to support all cybersecurity activities**.** At that funding level, most organizations cannot reasonably employ dedicated cybersecurity personnel while simultaneously investing in the technologies, managed services, training, and compliance activities necessary to implement NIST SP 800-171 and prepare for a CMMC assessment. Compounding this challenge is the cost of a single C3PAO assessment, which is widely understood to range from approximately $20,000 to $75,000, consuming a substantial portion of a small contractor's entire annual cybersecurity budget.

2) Specific Security Controls That Deliver the Most Tangible Uplift of Cybersecurity and Reduce Risk

Small set of foundational controls. Based on my recent experience as a Vice President (VP) of Cybersecurity within the Global Security organization of one of the nation's largest financial institutions, **our organization has identified a small number of foundational security controls that serve as mandatory security gates** and must be fully implemented before an application, system, or technology solution is permitted to enter the production environment. While there are many other security controls that remain part of our overall security validation process, the lack of these foundational controls pose an immediate and unacceptable level if cybersecurity risk.
A non-exhaustive list of the mandatory foundational controls include:

- Multi-factor authentication (MFA);
- Encryption of data at rest and in transit;
- Role-based access control (RBAC) and least privilege; and
- Strong identity and access management processes governing authentication and authorization.

3) Specific Regulatory Requirements or Security Controls That Create the Highest Burden with the Least Measurable Improvement to Actual Cybersecurity Posture.

Exclusive Reliance on C3PAOs for Third-Party Assessments. Fundamental business principles and the laws of supply and demand demonstrate that government-created exclusive markets predictably produce higher prices than competitive markets by restricting the supply of authorized providers while requiring consumers to purchase their services. Accordingly, the requirement that organizations obtain an assessment exclusively from a Cyber AB-approved CMMC C3PAO creates an artificially constrained assessment market that limits competition and affords C3PAOs greater pricing power than would exist in a competitive marketplace. The predictable result is higher assessment costs, limited assessment capacity, longer scheduling delays, and fewer choices for contractors.

Cybersecurity assessments have been successfully performed for decades by highly qualified independent organizations, including CPA firms, law firms, HITRUST Authorized External Assessors, FedRAMP Third Party Assessment Organizations (3PAOs), accredited testing laboratories, and other organizations with extensive experience evaluating information security governance, risk management, technical controls, and regulatory compliance. Restricting DoD-recognized assessments exclusively to C3PAOs has not been shown to produce a measurable improvement in cybersecurity outcomes compared to these existing assessment ecosystems. Instead, it

increases compliance costs by preventing contractors from obtaining assessments from other independent, qualified organizations with comparable or greater expertise in cybersecurity and regulatory compliance.

4) Commercial Cybersecurity Capabilities.

Commercial solutions don't guarantee CMMC compliance. Based on my personal experience advising more than 100 defense contractors of varying sizes on CMMC implementation, organizations generally leverage existing commercial cybersecurity capabilities in three primary ways. First, many organizations leverage commercial cloud service providers that offer secure environments for storing, processing, and transmitting CUI. Second, organizations increasingly utilize purpose-built secure enclaves that logically or physically isolate CUI from the remainder of the enterprise, thereby reducing both cybersecurity risk and the scope of compliance. Third, many organizations rely on Managed Service Providers (MSPs), Managed Security Service Providers (MSSPs), and other External Service Providers (ESPs) to perform cybersecurity operations, security monitoring, governance, compliance management, and ongoing administration.

Commercial cybersecurity solutions and services, however, should be viewed as enabling activities rather than complete compliance solutions. Although they substantially reduce cybersecurity risk and automate many technical controls, organizations remain responsible for significant governance, documentation, training, personnel security, physical security, and other administrative activities that cannot presently be outsourced or fully automated.

5) Phase I Self-Assessments.

Little correlation between CMMC assessment score and actual cyber posture. Based on my personal and professional experience, the primary challenge associated with CMMC self-assessments is not an unwillingness to comply, but rather a misunderstanding of how the assessment is intended to be performed. Many organizations evaluate themselves against the 110 security requirements in NIST 800-171 without assessing the corresponding assessment objectives contained in NIST 800-171A. Because the security requirements and assessment procedures are published in separate documents, many organizations are unaware that every assessment objective associated with a requirement must be evaluated. As a result, self-assessments frequently lack the rigor necessary to accurately measure compliance.

Additionally, the DoD's bespoke NIST 800-171 Supplier Performance Risk System (SPRS) scoring methodology, and its incorporation into CMMC minimum score requirements, introduces significant complexity without providing a meaningful measure of an organization's cybersecurity posture or operational risk. Under the current methodology, a security requirement must generally be scored as "Not Implemented" if even a single assessment objective is not satisfied, regardless of whether the remaining assessment objectives have been fully implemented. Consequently, the numerical SPRS score may significantly understate an organization's actual cybersecurity capabilities while overstating the significance of relatively minor deficiencies.

Conversely, a perfect CMMC assessment should not be interpreted as evidence of a mature or resilient cybersecurity program. The assessment reflects only a point-in-time determination of control implementation and does not evaluate the effectiveness, quality, sustainability, or operational maturity of the organization's cybersecurity processes. As a result, the score alone provides limited insight into an organization's actual ability to protect CUI or to respond to evolving cyber threats.

6) Policy Recommendations to Reduce Compliance Costs and Barriers to Entry.

I. Recognize Equivalent Assessment Organizations.
Proposed Policy Language - § 170.XX Recognition of Equivalent Assessment Organizations.

(a) The Department shall establish and maintain a program for the recognition of qualified independent assessment organizations authorized to perform DoD-recognized cybersecurity assessments. Recognition shall not be limited to CMMC Third-Party Assessment Organizations (C3PAOs).

(b) To be recognized by the Department, an assessment organization shall, at a minimum:

1. Be a United States-owned and controlled entity that satisfies all applicable Foreign Ownership, Control, or Influence (FOCI) requirements established by the Department;
2. Conduct assessments using the CMMC Assessment Process (CAP) and CMMC Assessment Guides, or another Department-recognized assessment methodology determined to provide substantially equivalent scope and rigor;
3. Employ assessors possessing the education, technical expertise, professional qualifications, and experience necessary to competently perform independent cybersecurity assessments;
4. Maintain documented policies governing independence, ethics, impartiality, confidentiality, and conflicts of interest;
5. Not have provided substantive consulting, implementation, remediation, or advisory services related to the cybersecurity controls, CMMC assessment boundary, or governing policies and procedures that are the subject of the assessment within the preceding three (3) years;
6. Maintain documented quality assurance and peer review processes to ensure the consistency, accuracy, and integrity of assessment results;
7. Produce a written assessment report suitable for use by contracting officers that is signed by the lead assessor, and contain at a minimum:

    a. the legal name of the assessment organization;
    b. the names of all assessors who participated in the assessment;
    c. a brief description of each assessor's qualifications, certifications, and relevant assessment experience;
    d. a description of the assessment scope and boundary, including the systems, facilities, and organizational components included within the assessment;
    e. the assessment period, including the dates on which the assessment concluded;
    f. an attestation signed by the lead assessor stating whether, in the assessor's professional opinion, the assessed organization conforms to the applicable requirements of NIST 800-171 as of the date of the assessment;
    g. If the assessment is performed by an assessment organization whose assessors are not subject to professional licensure or regulation as attorneys, Certified Public Accountants (CPAs), or CMMC Certified Assessors acting on behalf of an authorized CMMC Third-Party Assessment Organization (C3PAO), the assessment report shall include the following statement, signed by the lead assessor:

    I understand that this report is being prepared for use by the assessed organization and the United States Department of Defense in connection with federal contracting activities. I further understand that knowingly making or causing to be made any materially false, fictitious, or fraudulent statement or representation in this report, or causing another person to submit a false or fraudulent claim or statement to the United States Government, may subject me to civil and criminal liability under applicable federal law, including but not limited to 18 U.S.C. § 1001 and the False Claims Act, 31 U.S.C. §§ 3729–3733.

(c) Notwithstanding any other provision of this part, the Department shall accept a written assessment report that complies with the requirements of this section as satisfying any requirement for an independent third-party assessment of compliance with NIST SP 800-171, in lieu of a CMMC C3PAO assessment.

II. Expand Government-Sponsored Cybersecurity Assistance for Small Businesses and New Defense Industrial Base Entrants

Proposed Policy Language - § 170.XX Government-Sponsored Cybersecurity Assistance for Small Businesses and New Entrants.

(a) A contractor that qualifies as a small business concern under applicable Small Business Administration (SBA) regulations and has not previously obtained an independent third-party cybersecurity assessment recognized by the Department shall satisfy the Department's third-party cybersecurity assessment requirement by demonstrating active participation in one or more Department-approved government-sponsored cybersecurity assistance programs.

(b) Approved programs shall include, at a minimum:

1. The National Security Agency (NSA) Cybersecurity Collaboration Center (CCC);
2. The Department of Defense Defense Industrial Base Cybersecurity (DIB CS) Program; and
3. Any successor or substantially similar government-sponsored cybersecurity assistance program designated by the Department.

(c) Contractors that are entering the Defense Industrial Base for the first time and are not eligible to participate in an approved program prior to contract award shall enroll in at least one approved program within thirty (30) calendar days after contract award and shall actively participate in that program throughout contract performance.

(d) Contractors shall provide documentation demonstrating enrollment and meaningful participation upon request by the Contracting Officer.

(e) Nothing in this section shall preclude a contractor from voluntarily obtaining an independent third-party cybersecurity assessment.

Proposed Policy Language - DFARS 252.204-70XX – Government-Sponsored Cybersecurity Assistance Program Participation [for new entrants only]

(a) **Applicability**. This clause applies only to a Contractor that, as of the date of contract award:
1. Qualifies as a small business concern under applicable Small Business Administration regulations;
2. Does not hold any active Department of Defense prime contract or subcontract;
3. Has not previously obtained an independent third-party cybersecurity assessment recognized by the Department; and
4. Is awarded a Department of Defense contract requiring implementation of NIST Special Publication 800-171 or any successor cybersecurity requirements established by the Department.

(b) **Enrollment Requirement.** The Contractor shall initiate enrollment in at least one Department-approved government-sponsored cybersecurity assistance program within thirty (30) calendar days after contract award. Approved programs shall include, at a minimum:
1. The National Security Agency (NSA) Cybersecurity Collaboration Center (CCC);
2. The DoD Defense Industrial Base Cybersecurity (DIB CS) Program; or
3. Any successor or substantially similar government-sponsored cybersecurity assistance program designated by the Department.

(c) **Participation Requirement**. Throughout contract performance, the Contractor shall actively participate in the selected program by utilizing, as applicable, the cybersecurity services, technical assistance, threat intelligence, assessments, vulnerability information, incident response support, and other cybersecurity resources made available through the program.

(d) **Documentation**. Upon request of the Contracting Officer, the Contractor shall provide documentation demonstrating timely enrollment and meaningful participation in the approved program.

(e) **Satisfaction of Initial Third-Party Assessment Requirement**. For Contractors meeting the applicability requirements of paragraph (a), compliance with this clause shall satisfy any Department requirement for an initial independent third-party cybersecurity assessment during the period in which the Contractor actively participates in an approved government-sponsored cybersecurity assistance program.

(f) **Transition to Standard Assessment Requirements.** Upon completion of the Contractor's first Department of Defense contract, or upon no longer qualifying under paragraph (a), the Contractor shall become subject to any otherwise applicable Department cybersecurity assessment requirements for future contract awards.

III. Expand DIBCAC's Assessment Capability Through Strategic Use of C3PAOs

The Department should expand the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)'s capacity to conduct no-cost NIST SP 800-171 assessments by contracting with accredited CMMC C3PAOs to perform assessments on behalf of the Department. Rather than requiring contractors to independently procure and fund third-party assessments, the Department should leverage the existing C3PAO ecosystem as an extension of DIBCAC's assessment capability, particularly for small businesses and other resource-constrained members of the Defense Industrial Base.

By contracting directly with C3PAOs, the Department could also establish assessment priorities based on mission need, operational risk, critical technologies, supply chain importance, contractor size, or other acquisition priorities, rather than allowing assessment capacity to be driven solely by a contractor's ability to pay. This approach would enable the Department to direct limited assessment resources where they provide the greatest benefit to the Defense Industrial Base while reducing barriers to entry for innovative small businesses.

To maximize competition and expand assessment capacity, the Department should establish an open, multiple-award contract vehicle under which qualified C3PAOs may apply for inclusion at any time upon satisfying the Department's qualification requirements. Similar to the General Services Administration's Multiple Award Schedule program, this approach would allow newly authorized C3PAOs to become eligible to perform government-funded assessments without waiting for a new procurement cycle, ensuring the assessment marketplace continues to expand while maintaining rigorous qualification and oversight standards.

This model would substantially increase the Department's assessment capacity, reduce costs for contractors, shorten assessment wait times, improve competition among assessment providers, and allow DIBCAC to focus its government expertise on quality assurance, assessor oversight, and continuous improvement of the assessment program rather than performing the majority of assessments itself.

And because the Department—not individual contractors—would control the ordering process, assessments could be prioritized to support major weapon systems, critical supply chains, emerging technologies, and other acquisition priorities, ensuring that limited assessment resources are allocated where they most directly contribute to national security.

IV. Require CUI Mitigation Plans for Prime Contractors

The Department should require offerors to submit a CUI Mitigation Plan as part of every solicitation involving CUI. The purpose of the plan is to minimize the unnecessary distribution of CUI throughout the supply chain, thereby reducing cybersecurity costs, limiting compliance burdens, and decreasing the number of organizations required to implement CMMC requirements.

The CUI Mitigation Plan should include, at a minimum:

1. **Identification of Anticipated CUI Categories.** The prime contractor shall identify the specific CUI categories it reasonably anticipates will generate, receive from the Government, or receive from subcontractors during contract performance. Rather than broadly asserting that CUI "may be involved," offerors should identify the expected CUI categories associated with contract performance.
2. **Controlled Distribution Strategy.** The prime contractor shall identify which subcontractors, suppliers, consultants, and teaming partners require access to each category of CUI and describe the technical, contractual, and operational measures that will be implemented to prevent unnecessary dissemination of CUI to organizations that do not require access to perform their contractual responsibilities.
3. **Subcontractor CUI Assurance Strategy.** For each subcontractor identified as requiring CUI, the prime contractor shall describe how it has verified or will verify that the subcontractor is capable of protecting CUI commensurate with applicable DoD requirements. The plan should identify the assurance mechanism used, which may include:
    - Providing access through a prime contractor-managed secure enclave or other controlled computing environment;
    - Reviewing a NIST SP 800-171 self-assessment or other recognized third-party assessment;
    - Conducting a cybersecurity due diligence review or security questionnaire;
    - Performing contractual or technical validation of the subcontractor's security controls; or

- Another documented risk-based assurance process appropriate for the sensitivity of the information being shared.

4. **Small Business Burden Reduction Strategy.** Where the proposal includes small business subcontractors, the prime contractor shall identify the specific measures it has taken to reduce cybersecurity compliance costs and administrative burdens on those businesses while maintaining adequate protection of CUI. Examples may include limiting CUI access to only those entities with a demonstrated need-to-know, furnishing prime-managed CUI enclaves or shared secure environments, providing secure collaboration platforms, segregating work to avoid unnecessary CUI handling, leveraging existing compliant infrastructure, or otherwise reducing the need for individual small businesses to independently implement costly CMMC compliance capabilities.

By requiring contractors to deliberately identify anticipated CUI, limit its distribution, document how downstream recipients will protect it, and explain how they have minimized compliance burdens on small business subcontractors before contract award, DoD can significantly reduce the number of organizations required to implement costly CMMC compliance programs. Many subcontractors perform work that does not require access to CUI but nevertheless become part of the CUI boundary because no information-sharing strategy exists. Requiring CUI Mitigation Plans would promote least-privilege information sharing, encourage primes to adopt secure collaboration models such as shared CUI enclaves, improve supply chain security, reduce the attack surface available to adversaries, and lower compliance costs for thousands of small businesses without diminishing protections for CUI. DoD should consider the quality of the CUI Mitigation Plan as an evaluation factor during source selection. Offerors that demonstrate thoughtful CUI minimization, effective supply chain security, and meaningful burden reduction for small business partners should receive favorable evaluation consideration. This would create an incentive for primes to treat CUI minimization as a core acquisition objective rather than simply flowing CMMC requirements indiscriminately to every subcontractor.

7) Recommendations for Improving the Cybersecurity Posture of the DIB While Reducing Risk

V. Expand Government-Sponsored Cybersecurity Assistance Programs

The Department should significantly expand the funding, scope, and capabilities of approved government-sponsored cybersecurity assistance programs, including the National Security Agency (NSA) Cybersecurity Collaboration Center (CCC), the DoD Defense Industrial Base Cybersecurity (DIB CS) Program, and any other or substantially similar government-sponsored cybersecurity assistance program.

Rather than limiting these programs to information sharing and technical assistance, the Department should authorize approved programs to provide a broader range of government-funded cybersecurity services that directly improve the cybersecurity posture of Defense Industrial Base contractors. Such services may include:

- NIST SP 800-171 assessments and readiness assessments;
- Managed Security Service Provider (MSSP) services;
- Managed Service Provider (MSP) services;
- Secure enclave and managed hosted environment solutions;
- Continuous security monitoring and managed detection and response (MDR);
- Vulnerability assessments and penetration testing;
- Incident response and recovery assistance;
- Identity, access management, and multifactor authentication implementation;
- Encryption and data protection services;
- Governance, risk, and compliance (GRC) support;
- Cybersecurity engineering, architecture, and remediation services; and
- Other cybersecurity services designated by the Department.

To efficiently deliver these services, the Department should establish one or more open, multiple-award contract vehicles that permit qualified commercial cybersecurity providers to apply for inclusion at any time upon satisfying established qualification requirements. Similar to the GSA's Multiple Award Schedule (MAS) program, this approach would allow the Department to continuously expand the pool of qualified providers without requiring a new procurement each time additional capacity is needed.

The Department should establish standardized labor categories, service offerings, and funding ceilings tied to measurable cybersecurity outcomes and the implementation of foundational security capabilities. Funding priorities should emphasize services that implement or strengthen the security controls demonstrated to provide the greatest reduction in cybersecurity risk, including multifactor authentication, encryption, secure enclaves, external service providers, identity and access management, continuous monitoring, privileged access management, and other high-impact cybersecurity capabilities identified by the Department.

This approach would enable the Department to leverage commercial cybersecurity expertise at scale, reduce barriers to entry for small businesses, accelerate implementation of effective cybersecurity safeguards, and direct government funding toward activities that measurably improve the cybersecurity posture of the Defense Industrial Base rather than solely validating compliance.

VI. Expand Government-Sponsored Secure CUI Environments Through Secure Cloud Enclaves and Fully Managed Operating Environment (FMOE) Solutions

The Department should expand the availability of government-sponsored secure computing environments that enable Defense Industrial Base contractors, particularly small businesses, to securely process, store, and transmit CUI without independently building and operating a complete NIST SP 800-171 cybersecurity program. At a minimum, the Department should support the following deployment models:

1. **Secure Cloud Enclaves.** A dedicated cloud-based environment designed to securely process, store, and transmit CUI through standardized infrastructure, centralized cybersecurity management, and controlled user access. Secure cloud enclaves provide contractors with a cost-effective means of satisfying many NIST SP 800-171 technical requirements while reducing the complexity of designing, implementing, and maintaining an independent cybersecurity environment.

2. **Fully Managed Operating Environment (FMOE).** A dedicated hosted environment in which the contractor owns or leases the underlying computing infrastructure, while a qualified External Services Provider (ESP) houses, operates, manages, monitors, secures, and maintains the environment on the contractor's behalf. Contractor personnel access CUI through Virtual Desktop Infrastructure (VDI) or similar secure remote access technologies. Under a documented shared responsibility model, responsibility for implementing and maintaining many of the NIST SP 800-171 security requirements is contractually allocated to the qualified ESP, including system administration, security monitoring, vulnerability management, patch management, identity and access management, logging, configuration management, backup and recovery, infrastructure maintenance, and other operational cybersecurity functions. While both deployment models are generally available at comparable cost, the FMOE model permits a substantially greater portion of the NIST SP 800-171 security requirements to be performed by qualified cybersecurity professionals, significantly reducing the contractor's implementation and compliance burden while maintaining the required protection of CUI.

The Army's NCODE pilot program is a strong example of how the Department can partner with qualified commercial providers to deliver secure enclave capabilities to Defense Industrial Base contractors. The Department should expand this concept beyond the current pilot by making similar secure environment offerings available across the Department and extending eligibility to all businesses that qualify as small business concerns under the Small Business Administration's size standards, rather than limiting participation to micro-sized businesses.

To accelerate adoption, the Department should establish one or more open, multiple-award contract vehicles that permit qualified providers of secure cloud enclave and FMOE services to qualify for participation on a rolling basis, similar to the General Services Administration's Multiple Award Schedule (MAS) program. This approach would continuously expand provider capacity, promote competition, and provide contracting activities with a readily available source of vetted cybersecurity service providers.

Expanding these managed cybersecurity service models would improve protection of CUI, reduce barriers to participation in the DIB, leverage economies of scale, increase consistency in the implementation of cybersecurity safeguards, and allow contractors to focus on delivering mission capabilities while relying on qualified cybersecurity providers to operate and secure the environments in which CUI resides.

VII. Replace the Binary CMMC Certification Model with a Standardized Independent Cybersecurity Assessment Report

The Department should replace the current binary pass/fail CMMC certification model with a standardized independent cybersecurity assessment report that provides contracting officers and prime contractors with meaningful information regarding a contractor's cybersecurity posture while avoiding disclosure of sensitive technical information that could increase cybersecurity risk if compromised.

The current CMMC model communicates only whether a contractor satisfied the requirements of a particular assessment on a specific date. While this approach may simplify acquisition administration, it provides little meaningful information regarding the contractor's overall cybersecurity environment, governance structure, implementation approach, or residual cybersecurity risk. As a result, contracting officers and prime contractors are left to make supply chain risk decisions based upon little more than a binary certification status.

This approach is inconsistent with mature third-party cybersecurity and assurance programs used throughout government and industry. Assessment frameworks including SOC 2, ISO/IEC 27001, HITRUST, FedRAMP, and PCI DSS all rely upon standardized independent assessment reports prepared by qualified assessors. Those reports describe the assessment scope, environment, methodology, governance, and assessor's professional opinion, enabling customers, regulators, and other stakeholders to make informed, risk-based decisions. None relies solely upon a binary certification status as the primary assessment deliverable.

The Department should adopt a similar reporting model for CMMC by requiring independent assessors to prepare a standardized cybersecurity assessment report that provides meaningful decision support while protecting sensitive security information.

At a minimum, the assessment report should include:

1. The legal name of the assessment organization.
2. The names of all assessors who participated in the assessment and a brief summary of their qualifications.
3. The assessment period.
4. A description of the assessment boundary, including the general nature of the environment, such as:
    - Company-managed enterprise;
    - Secure cloud enclave;
    - Managed External Service Provider (ESP);
    - Managed Security Service Provider (MSSP);
    - Hybrid environment; or
    - Other comparable operating model.
5. A high-level description of the assessed environment, including the approximate number of users, the general scope of systems included within the assessment boundary, and whether CUI is processed within a dedicated enclave or enterprise-wide environment.
6. A narrative summary, organized by each NIST SP 800-171 control family, describing at a high level how the contractor governs, implements, and manages the applicable security requirements. These summaries should describe the contractor's governance model, implementation approach, and operational management without identifying specific technologies, configurations, vulnerabilities, or other sensitive implementation details.
7. An independent assessor opinion regarding the organization's overall conformance with NIST Special Publication 800-171.
8. An attestation signed by the lead assessor.

To reduce the risk of unauthorized disclosure, the assessment report should not include detailed technical information that could reasonably assist an adversary, including network diagrams, system configurations, IP addresses, hardware inventories, software versions, vulnerabilities, evidence reviewed during the assessment, or other sensitive implementation details.

The standardized assessment report should be submitted to the Contracting Officer as part of any proposal, offer, or other acquisition submission requiring demonstration of NIST SP 800-171 compliance and should satisfy the Department's requirement for an independent third-party cybersecurity assessment. Prime contractors should likewise

be permitted to rely upon the report when evaluating subcontractor cybersecurity as part of supply chain risk management.

Replacing the current binary certification model with a standardized independent assessment report would align the Department with established industry assurance practices, provide contracting officers and prime contractors with substantially more meaningful information for evaluating cybersecurity risk, encourage continuous cybersecurity improvement, and preserve the confidentiality of information that could otherwise increase the risk of compromise if disclosed.

Consistent with the recommendations above, the Department should permit standardized cybersecurity assessment reports to be prepared by any Department-recognized independent assessment organization, including C3PAOs, CPA firms, law firms, HITRUST Authorized External Assessors, FedRAMP Third Party Assessment Organizations (3PAOs), and other qualified assessment organizations approved by the Department. Expanding the pool of qualified assessors will increase competition, leverage existing assessment expertise, reduce costs, and provide contractors with greater access to independent cybersecurity assessments while maintaining consistent reporting standards and assessment quality.

Proposed Policy Language - § 170.XX Independent Cybersecurity Assessment Reports

(a) Purpose. In lieu of issuing a binary certification determination, each independent cybersecurity assessment conducted pursuant to this part shall result in a standardized Independent Cybersecurity Assessment Report prepared by a Department-recognized independent assessment organization. The report shall provide the Department, contracting officers, and authorized prime contractors with sufficient information to evaluate the contractor's cybersecurity posture and overall conformance with NIST Special Publication 800-171 while protecting sensitive security information from unnecessary disclosure.

(b) Authorized Assessment Organizations. Independent Cybersecurity Assessment Reports may be prepared by any Department-recognized independent assessment organization meeting the requirements of this part, including CMMC Third-Party Assessment Organizations (C3PAOs), Certified Public Accounting firms, law firms, HITRUST Authorized External Assessors, FedRAMP Third Party Assessment Organizations (3PAOs), and other qualified assessment organizations recognized by the Department.

(c) Minimum Report Contents. At a minimum, each Independent Cybersecurity Assessment Report shall include:

1. The legal name of the assessment organization.
2. The names of all assessors who participated in the assessment and a brief description of their qualifications.
3. The assessment period.
4. A description of the assessment boundary, including the general operating model of the assessed environment, such as:
    - Company-managed enterprise;
    - Secure cloud enclave;
    - Fully Managed Operational Environment (FMOE);
    - Managed Security Service Provider (MSSP);
    - Hybrid environment; or
    - Another comparable operating model.
5. A high-level description of the assessed environment, including the approximate number of users, the general scope of systems included within the assessment boundary, and whether CUI is processed within a dedicated enclave or enterprise-wide environment.
6. A narrative summary, organized by each NIST 800-171 control family, describing at a high level how the organization governs, implements, and manages the applicable security requirements.
7. An independent assessor opinion regarding the organization's overall conformance with NIST SP 800-171.
8. An attestation signed by the lead assessor.

(d) Protection of Sensitive Information. The assessment report shall not include technical information that could reasonably assist an unauthorized person in compromising the assessed environment, including network diagrams,

system configurations, IP addresses, hardware inventories, software versions, vulnerabilities, detailed evidence reviewed during the assessment, or other sensitive implementation information.

(e) Assessment Opinion. The lead assessor shall express an independent professional opinion regarding whether the assessed organization conforms to the applicable requirements of NIST 800-171 based upon the evidence obtained during the assessment.

(f) Department Acceptance. An Independent Cybersecurity Assessment Report prepared in accordance with this section shall satisfy any Department requirement for an independent third-party cybersecurity assessment and shall be accepted by the Department in lieu of a binary CMMC certification.

(g) Use of Assessment Reports. An Independent Cybersecurity Assessment Report may be submitted in response to any solicitation, proposal, offer, contract administration requirement, or other Department requirement demonstrating compliance with NIST Special Publication 800-171. Prime contractors may rely upon such reports when evaluating subcontractor cybersecurity as part of supply chain risk management.

VIII. Adopt a Risk-Based Assessment Methodology That Prioritizes the Most Impactful Cybersecurity Controls

The Department should reevaluate the current Supplier Performance Risk System (SPRS) scoring methodology and adopt a risk-based weighting framework that more accurately reflects the relative cybersecurity value of individual NIST SP 800-171 security requirements. If the Department elects to retain a scoring methodology as part of CMMC or future cybersecurity assessment programs, greater weight should be assigned to those technical safeguards that demonstrably provide the greatest reduction in the likelihood and impact of unauthorized access to CUI.

The current SPRS methodology assigns the lowest point deductions (1 point) to several foundational technical controls that directly protect CUI, while assigning the highest point deductions (5 points) to governance and program management controls. Although all NIST SP 800-171 security requirements are important components of a comprehensive cybersecurity program, the current weighting methodology does not accurately reflect the relative effectiveness of individual controls in preventing the compromise of CUI.

The Department should revise the scoring methodology to more closely align assessment weighting with the demonstrated cybersecurity impact of individual security requirements. Controls that directly prevent unauthorized access to CUI—such as multifactor authentication, encryption of data at rest and in transit, identity and access management, least privilege, audit integrity, and other foundational technical safeguards—should receive proportionally greater weight than controls whose primary purpose is governance, documentation, or post-incident management. A risk-based weighting methodology would better incentivize implementation of the most effective cybersecurity safeguards and produce assessment results that more accurately reflect an organization's overall cybersecurity posture and residual risk.

IX. Align Department Cybersecurity Requirements with the Current Version of NIST SP 800-171

The Department should discontinue its practice of permanently incorporating specific versions of NIST SP 800-171 into DFARS clauses and the CMMC program. Instead, the Department should adopt a policy of aligning cybersecurity requirements with the current version of NIST SP 800-171 in accordance with NIST's published implementation and transition timelines. Historically, the Department has continued to require compliance with outdated versions of NIST SP 800-171 long after NIST issued revised guidance, resulting in unnecessary divergence between Department requirements, commercial cybersecurity practices, and other federal cybersecurity initiatives. This approach delays adoption of improved cybersecurity practices and places the DIB behind the broader cybersecurity community. Beginning with future revisions of NIST SP 800-171, the Department should publicly communicate its intent to adopt updated requirements consistent with NIST's published transition schedule. This policy would provide contractors with predictable implementation timelines, encourage earlier planning and investment, and reduce uncertainty regarding future compliance obligations.