August 14, 2026

Cybersecurity Maturity Model Certification Reform Task Force
U.S. Department of War

Re: Comments Regarding Reform of the Cybersecurity Maturity Model Certification (CMMC) Program

Dear Members of the CMMC Reform Task Force:

On behalf of the American metalcasting industry, we appreciate the opportunity to submit the enclosed comments regarding reform of the Cybersecurity Maturity Model Certification (CMMC) program.

U.S. metalcasters are an essential part of the nation's manufacturing and defense industrial base, producing highly engineered iron, steel, aluminum, and other non-ferrous castings used in thousands of defense applications. The industry includes more than 1,600 facilities across the United States and supports nearly 500,000 direct and indirect American jobs.

Our industry strongly supports the Department's responsibility to protect Federal Contract Information, Controlled Unclassified Information, and other sensitive defense information from cybersecurity threats. Effective cybersecurity is essential to national security and the resilience of the Defense Industrial Base.

At the same time, the experience of small and medium-sized manufacturers working to comply with CMMC and NIST SP 800-171 has demonstrated that the cost, complexity, and administrative burden associated with the current approach can become a significant barrier to defense contracting. For many smaller manufacturers, defense-related work represents only a portion of their overall business. When cybersecurity compliance costs become disproportionate to the value or risk of that work, companies may elect not to participate in the defense market at all.

The Department's decision to suspend implementation of CMMC Phase II creates an important opportunity to evaluate these challenges and establish a more scalable, risk-based, and practical cybersecurity framework. We encourage the Department to pursue reforms that maintain appropriate protections for sensitive defense information while recognizing the operational realities and limited resources of small manufacturers.

The enclosed comments provide the metalcasting industry's perspective on the burdens experienced under the current framework and offer recommendations intended to improve cybersecurity outcomes while preserving and expanding the domestic manufacturing base available to support national defense.

A cybersecurity program intended to protect the Defense Industrial Base should strengthen that industrial base—not create unnecessary barriers that cause capable domestic manufacturers to leave, or never enter, the defense marketplace.

We appreciate the Department's consideration of these comments and its willingness to engage with industry as it evaluates potential reforms to the CMMC program. We welcome the opportunity to provide additional information or participate in further discussions regarding these important issues.

Sincerely,

Justin Scott
Chief Executive Officer/American Foundry Society

Michael Meyer
President/North American Die Casting Association

Jerrod A. Weaver
Executive Director/Non-Ferrous Founders' Society

Ryan Moore
VP of Operations/Steel Founders' Society of America

U.S. Metalcasting Industry Comments on Reforming CMMC and Reducing Compliance Burden for the Defense Industrial Base

The American metalcasting industry appreciates the opportunity to provide comments to the Department of War regarding reform of the Cybersecurity Maturity Model Certification (CMMC) program.

These comments represent the perspective of U.S. metalcasters, including many small and medium-sized manufacturers that currently support, or have the technical capabilities to support, Department of War programs and the broader Defense Industrial Base (DIB).

The U.S. metalcasting industry is a strategic asset and serves as the backbone of virtually all U.S. manufacturing activities, including our national defense, energy, and infrastructure systems. U.S. metalcasters produce highly engineered, 100% made-in-USA castings made from iron, steel, aluminum, copper, and other non-ferrous alloys that have thousands of defense applications. The industry includes more than 1,615 facilities operating nationwide, supports nearly 500,000 direct and indirect jobs in every state, and generates tens of billions of dollars in economic impact.

Although domestic casting capability is critical to national defense, defense work represents a relatively small portion of the industry's overall production. At the same time, serving the defense market can impose substantially greater cybersecurity costs, administrative requirements, and compliance complexity than serving commercial customers. For small manufacturers, these added costs can make defense work economically unattractive, creating an incentive to prioritize commercial markets and potentially further reducing the supplier base available to DoW.

Our industry strongly supports the Department's objective of protecting Federal Contract Information (FCI), Controlled Unclassified Information (CUI), and other sensitive defense information from cybersecurity threats. Cybersecurity is an important component of defense readiness and supply-chain resilience.

At the same time, the experience of small manufacturers attempting to comply with CMMC and NIST SP 800-171 demonstrates the need for a more scalable, risk-based, and practical approach to cybersecurity compliance. For many small metalcasters, cybersecurity compliance is not simply an information technology issue; it has become a significant business decision affecting whether a company is willing or financially able to participate in defense contracting at all. The challenge, therefore, is not whether cybersecurity protections are necessary, but how those protections are structured and applied to small manufacturers.

The Department's suspension of CMMC Phase II provides an important opportunity to redesign the program so that it improves actual cybersecurity outcomes without unnecessarily discouraging capable domestic manufacturers from participating in the defense supply chain. A cybersecurity program designed to protect the Defense Industrial Base should not unnecessarily shrink that industrial base by causing capable domestic suppliers to leave, or never enter, the defense market.

The Small Manufacturing Perspective

The typical small metalcasting operation is fundamentally different from a large defense prime contractor or major technology company.

Eighty percent of U.S. metalcasters employ fewer than 100 people and operate with very small administrative and information technology staff - reflecting true main street businesses.

In many cases, these companies do not employ dedicated cybersecurity professionals. Their core expertise and investment are concentrated in manufacturing equipment, metallurgy, tooling, quality systems, workforce development, and production.

Yet these companies manufacture cast components that may be critical to weapons systems, ships, aircraft, vehicles, ground equipment, small arms, electronics, radar systems, infrastructure, and sustainment programs for all branches of the military.

When cybersecurity requirements impose substantial fixed costs regardless of company size, contract value, amount of sensitive information handled, or actual cybersecurity risk, the burden falls disproportionately on these smaller manufacturers.

The practical result can be counterproductive to the Department's broader industrial-base objectives. Companies capable of producing needed defense components may decide that the cost and administrative burden associated with entering the defense market exceeds the economic opportunity available to them.

CMMC reform should therefore seek to accomplish two objectives simultaneously:

1. Meaningfully improve the cybersecurity and operational resilience of the Defense Industrial Base; and
2. Reduce unnecessary barriers that prevent capable small and nontraditional manufacturers from participating in defense production.

These objectives are not mutually exclusive.

Most Prohibitive Cost Drivers and Administrative Burdens

The metalcasting industry believes the most significant barriers for small manufacturers generally fall into five areas.

1. Third-Party Consulting and Cybersecurity Expertise

Small manufacturers frequently lack the internal cybersecurity expertise necessary to independently interpret and implement CMMC and NIST SP 800-171 requirements.

As a result, companies must often times retain outside consultants simply to understand what is required, perform gap assessments, develop policies and procedures, prepare System Security Plans, establish Plans of Action and Milestones, configure systems, and prepare for certification.

These consulting costs occur before a manufacturer receives any guarantee of defense business.

For a small metalcaster evaluating whether to pursue a limited number of defense opportunities, the cost of establishing compliance can therefore become a significant barrier to market entry.

2. Technology and Infrastructure Costs

Compliance can require investments in information technology infrastructure, security software, identity and access management, endpoint protection, logging and monitoring systems, data storage, network segmentation, secure communications, and other cybersecurity capabilities.

Some of these investments provide substantial cybersecurity benefits and should be encouraged.

The concern arises when companies must redesign otherwise functional information systems or purchase specialized technologies primarily to demonstrate compliance with prescriptive requirements rather than to address a material cybersecurity risk.

3. Certification and Assessment Costs

Independent certification creates another significant fixed cost for small manufacturers.

Third-party certification expenses must be evaluated in relation to the value and frequency of defense contracts available to the company.

A large defense contractor may distribute certification costs across hundreds of millions or billions of dollars in government business. A small metalcaster may be considering defense contracts representing only a small fraction of its annual revenue.

A compliance framework that applies similar certification costs to both companies can create a strong economic disincentive for small manufacturers to enter the defense market.

4. Staff Time and Documentation

The administrative burden associated with CMMC extends well beyond the direct cost of technology.

Small companies must dedicate management, IT, quality, and administrative personnel to interpreting requirements, documenting processes, collecting evidence, maintaining policies, responding to assessments, tracking corrective actions, and periodically updating documentation.

For a small manufacturer, these individuals frequently perform multiple operational roles. Hours devoted to compliance activities are therefore hours unavailable for production management, quality improvement, customer service, workforce development, engineering, and other activities directly related to manufacturing.

The Department should recognize staff time and opportunity cost as significant components of the true cost of cybersecurity compliance.

5. Lost or Avoided Defense Opportunities

Perhaps the most consequential cost is difficult to measure: companies deciding not to pursue defense work at all.

Our associations have encountered manufacturers that are interested in supporting the Department but question whether anticipated defense revenue justifies the investment required to become CMMC compliant and certified. This creates a potential unintended consequence.

A cybersecurity program designed to protect the Defense Industrial Base should not unnecessarily shrink that industrial base by causing capable domestic suppliers to leave, or never enter, the defense market.

CMMC reform should specifically evaluate the number of otherwise capable suppliers that have declined defense opportunities because of cybersecurity compliance requirements.

Security Controls Providing the Greatest Cybersecurity Benefit

The metalcasting industry supports cybersecurity requirements that result in measurable reductions in actual cyber risk.

From a small-manufacturer perspective, the Department should place greater emphasis on foundational controls that directly reduce the probability or impact of common cybersecurity incidents.

Examples include:

- Multi-factor authentication;
- Strong identity and access management;
- Timely security patching and vulnerability remediation;
- Endpoint protection;
- Network segmentation;
- Secure and tested data backups;
- Email and phishing protection;
- Employee cybersecurity awareness training;
- Controlled administrative privileges;
- Incident detection and response capabilities; and
- Tested business continuity and disaster recovery procedures.

These types of controls are generally understandable to small businesses, address recognizable threats, and can provide measurable improvements in cybersecurity and operational resilience.

Future cybersecurity requirements should prioritize these demonstrably effective controls rather than treating every administrative and technical requirement as having equal cybersecurity value.

Requirements Creating High Burden With Limited Risk Reduction

The Department should review CMMC requirements through a simple test:

Does this requirement materially reduce cybersecurity risk, or does it primarily demonstrate that a company has documented compliance?

Documentation is necessary to establish accountability, but documentation itself should not become the objective of the cybersecurity program.

Small businesses can devote substantial resources to preparing policies, procedures, evidence packages, screenshots, inventories, narratives, and other materials necessary to demonstrate compliance.

Where these requirements duplicate other records or provide little incremental security benefit, they should be reduced or eliminated.

The Department should particularly review requirements that:

- Require extensive documentation disproportionate to the underlying cybersecurity risk;
- Require substantially similar information to be maintained in multiple formats;
- Require highly technical compliance activities with limited practical relevance to a small manufacturing environment;
- Create significant assessment preparation requirements without improving cybersecurity;
- Require expensive technological solutions where equivalent commercial solutions provide comparable protection; or
- Apply identically regardless of the quantity or sensitivity of government information actually handled by the contractor.

The goal should be to move CMMC from a documentation-centered compliance exercise toward a measurable cybersecurity risk-management program.

Recognition of Commercial Cybersecurity Solutions

Small manufacturers overwhelmingly rely upon commercially available information technology and cybersecurity products and outside service providers.

The Department should design CMMC around this reality rather than expecting every small contractor to independently construct and maintain enterprise-level cybersecurity infrastructure.

Commercial cloud environments, managed service providers, managed security service providers, endpoint security platforms, identity management services, secure collaboration platforms, backup services, email security tools, and other commercially available solutions can provide cybersecurity capabilities that would otherwise be beyond the resources of a small manufacturer.

DoW should establish clear mechanisms for recognizing compliant commercial cybersecurity platforms and configurations.

Where a widely used commercial platform has been independently evaluated and provides defined cybersecurity capabilities, individual small businesses should not repeatedly be required to prove the underlying effectiveness of the same technology.

The Department should consider creating standardized reference architectures or approved technology configurations specifically designed for small businesses.

For example, DoW could publish several scalable cybersecurity architectures based upon commonly available commercial platforms. A small manufacturer implementing one of these configurations could then concentrate its resources on properly operating the system rather than independently designing and documenting an entire cybersecurity architecture.

This approach could simultaneously improve cybersecurity, increase consistency, and substantially reduce compliance costs.

Reform of Phase I Self-Assessments

U.S. metalcasters support the continued use of self-assessment where appropriate.

However, the self-assessment process should be simplified and structured to help companies improve cybersecurity rather than merely produce a compliance score.

For a small manufacturer, determining exactly how individual requirements apply to its environment can itself require outside consulting assistance.

The Department should consider developing:

- A simplified small-business self-assessment tool;
- Plain-language explanations of requirements;
- Manufacturing-specific implementation guidance;
- Examples of acceptable evidence;
- Automated assessment tools;
- Standard templates for required policies and documentation;
- Clearly defined remediation pathways; and
- Technical assistance programs for small businesses.

Companies should also be able to identify deficiencies and correct them without immediately becoming ineligible for defense work when those deficiencies do not create an unacceptable risk to government information.

A mature cybersecurity framework should encourage companies to identify weaknesses and continuously improve them rather than creating incentives to treat cybersecurity as a periodic compliance exercise.

Recommended CMMC Policy Reforms

The domestic metalcasting industry recommends that the CMMC Reform Task Force consider the following principles.

1. Establish a Tiered, Risk-Based Compliance Model

Compliance requirements should reflect the sensitivity and quantity of information actually handled by the contractor.

A small foundry receiving limited technical information should not necessarily face the same cybersecurity architecture and certification burden as a contractor maintaining extensive repositories of highly sensitive defense information.

2. Simplify Requirements for Small Businesses

DoW should develop a defined small-business compliance pathway that focuses on the cybersecurity controls providing the greatest measurable risk reduction.

This pathway should reduce duplicative documentation and provide standardized tools, templates, architectures, and implementation guidance.

3. Reduce Reliance on Mandatory Third-Party Certification

Third-party certification should be reserved for situations where the sensitivity of the information or risk associated with the contract justifies the additional expense.

Self-attestation combined with targeted government verification, automated validation, or risk-based audits may provide an appropriate alternative for many smaller suppliers.

4. Recognize Existing Commercial Cybersecurity Capabilities

DoW should establish safe harbors or presumptions of compliance for properly configured commercial cybersecurity technologies and managed services that satisfy defined security outcomes.

Small companies should not be required to repeatedly demonstrate the effectiveness of widely accepted commercial security technologies.

5. Separate Cybersecurity Improvement From Documentation Burden

Program success should be evaluated primarily through measurable improvements in cybersecurity posture and operational resilience rather than the quantity of compliance documentation produced.

6. Allow Reasonable Remediation

Companies demonstrating substantial compliance should have reasonable opportunities to remediate lower-risk deficiencies through Plans of Action and Milestones without immediately losing eligibility for defense work.

7. Provide a Practical On-Ramp for New Defense Suppliers

A company interested in entering the defense market should not need to make a substantial cybersecurity investment before it knows whether meaningful business opportunities exist.

DoW should establish an onboarding pathway allowing prospective suppliers to progressively increase cybersecurity capabilities as the sensitivity of information and level of defense participation increases.

8. Consider Contract Value and Compliance Economics

The Department should examine whether cybersecurity compliance costs are reasonable relative to the anticipated value of the defense work.

Fixed certification and compliance costs can make small-dollar contracts economically unattractive to small manufacturers even when those companies possess exactly the manufacturing capabilities DoW needs.

Improving Operational Resilience Against Cyberattacks

CMMC reform should expand its focus from compliance toward operational resilience.

For a metalcasting company, the consequences of a cyberattack extend beyond loss of information. An attack can interrupt production, disable equipment, disrupt scheduling and logistics systems, prevent access to engineering information, and delay delivery of components required by defense customers.

The Department should therefore emphasize practical resilience capabilities including:

- Secure and recoverable backups;
- Incident-response planning;
- Business continuity planning;
- Network and system segmentation;
- Recovery testing;
- Employee cyber awareness;
- Rapid vulnerability remediation;
- Protection of operational technology environments; and
- Access to cybersecurity technical assistance following an incident.

DoW should consider providing small DIB manufacturers with shared cybersecurity resources, technical assistance, threat information, vulnerability alerts, and incident-response support.

Investing in these capabilities may produce substantially greater improvements in defense supply-chain resilience than increasing documentation or assessment requirements.

Cybersecurity Should Be an Enabler of the Industrial Base

The American metalcasting industry supports the Department's objective of maintaining a secure and resilient Defense Industrial Base.

However, the country's cybersecurity policy must also recognize an equally important national security reality: the United States needs a sufficiently large, diverse, competitive, and capable domestic manufacturing base to produce the components required by the warfighter.

Cybersecurity requirements that unintentionally discourage small manufacturers from participating in defense procurement can work against that objective.

For a small foundry owner, the decision is straightforward. If entering the defense market requires substantial consulting expenses, new information technology infrastructure, extensive documentation, recurring staff

commitments, and expensive third-party certification before the company can determine whether sufficient defense business exists to recover those costs, many businesses will simply decline to participate.

The Department should not interpret that decision as opposition to cybersecurity, rather it is an economic decision resulting from the disproportionate cost of entry.

CMMC reform provides an opportunity to establish a different model: one that holds contractors accountable for protecting government information while providing small manufacturers with a clear, affordable, scalable path to achieve that objective.

The American metalcasting industry encourages the Department to adopt a cybersecurity framework based upon measurable risk reduction, commercial technology, simplified small-business requirements, appropriate use of self-attestation, targeted verification, reasonable remediation, and continuous improvement.

Such an approach would strengthen cybersecurity while simultaneously expanding the pool of qualified domestic manufacturers available to support the warfighter. That combination — a more secure Defense Industrial Base and a larger, stronger domestic manufacturing base — should be the ultimate measure of successful CMMC reform.

Respectfully submitted,

Justin Scott
Chief Executive Officer/American Foundry Society

Michael Meyer
President/North American Die Casting Association

Jerrod A. Weaver
Executive Director/Non-Ferrous Founders' Society

Ryan Moore
VP of Operations/Steel Founders' Society of America