CMMC 2.0 AND WHAT HEAT TREATERS SHOULD BE DOING NOW

The transition to CMMC 2.0 represents a significant shift in how heat-treating companies must operate. (Courtesy: Shutterstock)

Some current and future business depends on CMMC 2.0 certification.

By JOE COLEMAN

The heat-treating industry, while traditionally focused on metallurgical and heat-treating processes, has increasingly become integrated with the digital world. As a critical component in the supply chains of defense, aerospace, and other high-tech industries, heat treaters have now become custodians of sensitive and controlled unclassified information (CUI). With the Cybersecurity Maturity Model Certification (CMMC) 2.0 coming by the end of 2024 or early 2025, the U.S. Department of Defense (DoD) has made it clear cybersecurity is no longer optional but a mandated standard for anyone involved in the defense industrial base (DIB). For heat treaters, achieving and maintaining CMMC 2.0 certification is not just about compliance; it is about securing their place in future business opportunities and protecting their current operations from potentially catastrophic cyber threats.

UNDERSTANDING CMMC 2.0: THE BASICS

The CMMC 2.0 framework was developed by the DoD to create a unified cybersecurity standard across its contractors and subcontractors. The original CMMC 1.0 model, introduced in 2020, had five cybersecurity maturity levels, ranging from basic cyber hygiene to advanced and progressive practices. However, recognizing the complexities and challenges faced by small- and medium-sized businesses (SMBs), the DoD revised the model, resulting in CMMC 2.0.

This updated version simplifies the certification process by reducing the levels from five to three, making it more accessible, while ensuring robust cybersecurity practices.

THE THREE LEVELS OF CMMC 2.0

›› **Level 1 (Foundational):** This level is designed for companies that handle federal contract information (FCI). It requires 17 basic cybersecurity practices, which are derived from the Federal Acquisition Regulation (FAR) 52.204-21. This level represents the minimum level of protection and is self-assessed annually.

›› **Level 2 (Advanced):** This level applies to companies that handle CUI. It is closely aligned with the 110 security controls in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. Most heat-treating companies dealing with defense contracts will need to meet Level 2 requirements, which involve a certified third-party assessment every three years for certain contracts.

›› **Level 3 (Expert):** Aimed at the highest-risk contracts involving critical national security information, Level 3 is based on a subset of NIST SP 800-172 standards and all 110 controls of NIST SP 800-171 R2. This level involves government-led assessments and is relevant for only a small percentage of defense contractors.

CMMC 2.0 ensures companies across the defense supply chain and defense industrial base (DIB) have the safeguards to protect against increasingly common and sophisticated data breaches and cyber espionage.

WHY CMMC 2.0 MATTERS TO THE HEAT-TREATING INDUSTRY

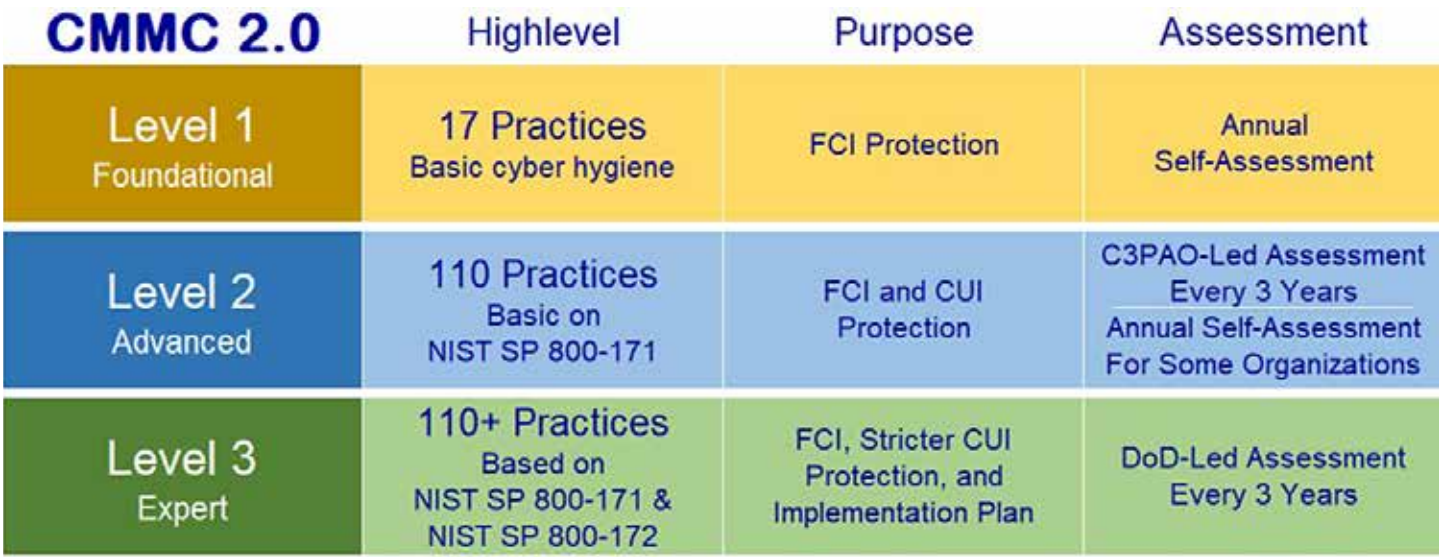
Heat-treating companies, especially those in the defense and aerospace sectors, are critical links in the DoD supply chain. The parts and components they process often require adherence to stringent specifications and standards, including cybersecurity-related ones. So, CMMC 2.0 is not just a regulatory hurdle but a business imperative.

The CMMC 2.0 framework was developed by the DoD to create a unified cybersecurity standard across its contractors and subcontractors. (Courtesy: Bluestreak Consulting)

KEY REASONS WHY CMMC 2.0 IS CRUCIAL FOR HEAT TREATERS

›› **Supply chain security:** The nature of modern cyber threats means hackers looking to penetrate larger, more secure systems can target even small subcontractors to "get a foot in the door." Heat treaters, who may possess detailed specifications for defense-related parts, are prime targets for these attacks. CMMC 2.0 certification ensures all companies in the supply chain adhere to a baseline level of cybersecurity, reducing the overall risk of a data breach.

›› **Compliance and contractual requirements:** Without CMMC 2.0 certification, heat-treating companies could find themselves ineligible to bid on or renew contracts with the DoD and other defense-related entities. As the DoD begins to enforce CMMC 2.0 requirements,



CMMC 2.0 is expected to be placed in DoD contract, RFPs, and PFIs starting in Q1 2025. (Courtesy: Bluestreak Consulting)

compliance will become a prerequisite for doing business with the DoD or providing downstream services. This is particularly important for heat treaters, who often serve as subcontractors to larger companies that will require proof of certification from their entire supply chain.

» **Protection of intellectual property (IP):** Many heat-treating companies work with proprietary processes or handle parts subject to IP protections. A cybersecurity breach could lead to the theft of this IP, resulting in significant financial and reputational damage. CMMC 2.0 helps ensure robust cybersecurity measures are in place to protect this valuable information.

» **Customer trust and competitive advantage:** Certification under CMMC 2.0 signals to customers and partners that a company takes cybersecurity seriously. This can be a significant competitive advantage, especially in an industry where trust and reliability are paramount. Companies that achieve certification may find themselves better positioned to win contracts and attract new business.

» **Financial and legal implications:** A cyberattack can have severe financial repercussions, including ransom payments, legal fees, and lost business. Additionally, non-compliance with CMMC 2.0 could lead to penalties, contract termination, and potential litigation. Investing in compliance is far less costly than dealing with the fallout from a breach.

PREPARING FOR CMMC 2.0 COMPLIANCE: A STEP-BY-STEP GUIDE FOR HEAT TREATERS

Achieving CMMC 2.0 compliance is a significant undertaking, particularly for SMBs that may not have extensive cybersecurity resources. However, with careful planning and execution, it is possible to meet the necessary requirements. The following steps outline a strategic approach for heat-treating companies seeking CMMC 2.0 certification.

1. Conduct a Preliminary Assessment

The first step in preparing for CMMC 2.0 is to conduct a thorough assessment of current cybersecurity practices. This should include a gap analysis comparing existing measures against the requirements of the relevant CMMC 2.0 Level 2 for heat treaters. Key areas to evaluate include:

» **Access control:** Who has access to sensitive information and systems? Are there measures to ensure that only authorized personnel can access this data?

» **Physical security:** How is access to physical locations, such as production facilities and data centers, controlled and monitored?

» **Network security:** Are firewalls, encryption, and other network security measures in place to protect against unauthorized access and cyberattacks?

» **Incident response:** Does your company have a plan to respond to a cybersecurity incident? Are employees trained in how to handle potential breaches?

2. Develop a Remediation Plan

Once the assessment is complete, the next step is to develop a remediation plan to address any gaps identified. This plan should include:

» **Prioritization:** Identify the most critical vulnerabilities and prioritize them for remediation. This ensures the most significant risks are addressed first.

» **Timeline:** Establish a timeline for implementing the necessary changes. This should include milestones and deadlines to keep the project on track.

» **Resources:** Determine the needed resources, including personnel, technology, and budget. This may involve hiring cybersecurity professionals or investing in new tools and systems.

» **Policies and procedures:** Update or create cybersecurity policies and procedures to align with CMMC 2.0 requirements. This includes documentation of all practices and controls.

3. Implement Necessary Changes

With a plan in place, it's time to begin implementing the necessary changes to your cybersecurity infrastructure. This may include:

» **Upgrading technology:** Implementing or upgrading firewalls, encryption tools, multi-factor authentication (MFA), and other cybersecurity technologies.

» **Training employees:** Conduct regular training sessions to ensure they understand the importance of cybersecurity and are familiar with the newly adopted policies and procedures.

» **Strengthening physical security:** Enhance physical security measures, such as access controls, surveillance systems, and secure storage for sensitive materials.

» **Testing and validation:** Once changes are implemented, conduct thorough testing to ensure they work as intended and that all vulnerabilities have been addressed.

While CMMC 2.0 presents challenges, it also offers growth opportunities. Companies that achieve certification will have a competitive edge as customers increasingly prioritize security in their supply chain partners.

4. Engage a Third-Party Assessor

A third-party assessment is required for Level 2 and Level 3 certifications. These assessors, known as certified third-party assessment organizations (C3PAOs), will evaluate your company's compliance with CMMC 2.0. It is essential to choose a reputable C3PAO and schedule your assessment well in advance, as demand for these services is expected to be high.

It is also highly recommended you hire a CMMC registered practitioner organization (RPO), a CMMC-registered practitioner (RP), or a registered practitioner advanced (RPA) to guide or lead you through this complicated process and to help you be prepared for your CMMC assessment by a C3POA.

During the assessment, the C3PAO will review your documentation, interview key personnel, and assess your systems to ensure they meet the required standards. It is crucial to be well prepared for this process, as any deficiencies identified during the assessment will need to be addressed before certification can be granted.

5. Maintain and Monitor Compliance

Achieving CMMC 2.0 certification is not a one-time event. Continuous monitoring and maintenance are required to ensure ongoing compliance. This includes:

- **Regular audits:** Conduct internal audits to verify all cybersecurity practices and controls function as intended.
- **Monitoring systems:** Implement continuous monitoring tools to detect and respond to potential threats in real time.
- **Staying informed:** Stay current with the latest developments in cybersecurity and CMMC standards to ensure your company remains compliant with any changes.
- **Re-certification:** For Level 2, a re-certification assessment is required every three years. It is important to maintain all documentation and continue best practices to ensure a smooth re-certification process.

6. Consider the Broader Implications

Beyond meeting CMMC 2.0 requirements, heat treaters should consider the broader implications of cybersecurity on their business. This includes:

- **Supply chain relationships:** Work closely with your supply chain partners to ensure they are also compliant with CMMC 2.0. A weak link in the supply chain can compromise your security, even if your own practices are robust.
- **Customer communications:** Be transparent with your customers about your cybersecurity practices and CMMC 2.0 certification. This can help build trust and potentially lead to new business opportunities.
- **Cyber insurance:** Consider investing in cyber insurance to mitigate the monetary impact of a potential breach. This can provide additional protection and peace of mind.

THE FUTURE OF HEAT TREATING IN A CYBERSECURITY-DRIVEN WORLD

As the heat-treating industry continues to evolve in the way they do business, cybersecurity's importance will only increase. With the implementation of CMMC 2.0, the DoD has made it clear that cybersecurity concerns not just large defense contractors, but every company involved in the supply chain. For heat treaters, cybersecurity must become a core component of their business strategy.

ADAPTING TO A NEW BUSINESS REALITY

The transition to CMMC 2.0 represents a significant shift in how heat-treating companies must operate. No longer can cybersecurity be seen as an afterthought or a secondary concern. Instead, it must be integrated into every aspect of the business, from production processes to customer communications. This shift requires not only technical upgrades but also a cultural change within organizations. Employees at all levels must understand the importance of cybersecurity and be trained to follow best practices.

OPPORTUNITIES FOR GROWTH

While CMMC 2.0 presents challenges, it also offers growth opportunities. Companies that achieve certification will have a competitive edge as customers increasingly prioritize security in their supply chain partners. Additionally, as cybersecurity standards continue to evolve globally, CMMC 2.0 compliance could open doors to international markets where similar standards are being adopted.

The future looks promising for heat-treating companies that are proactive in achieving CMMC 2.0 certification. By securing their operations against cyber threats, these companies cannot only protect their current business but also position themselves for future growth in a cybersecurity-conscious market.

THE COST OF INACTION

The cost of failing to achieve CMMC 2.0 compliance is high. Companies that do not meet the required standards may find themselves excluded from defense contracts and other critical business opportunities. Moreover, the financial and reputational damage caused by a cybersecurity breach can be devastating, particularly for SMBs. Investing in CMMC 2.0 compliance is not just a regulatory requirement; it is a necessary step to ensure the long-term viability of your business.

CONCLUSION

CMMC 2.0 represents a significant development in the way cybersecurity is managed across the defense industrial base. For heat treaters, achieving certification is critical to maintaining current business relationships and securing future opportunities. By understanding the requirements, conducting a thorough assessment, and implementing necessary changes, heat-treating companies can position themselves as trusted and secure partners in the defense and aerospace industries.

As the global landscape of cybersecurity continues to evolve, the importance of CMMC 2.0 will only grow. Heat-treating companies that take proactive steps to achieve and maintain certification will not only protect their operations but also gain a competitive edge in an increasingly security-conscious market.

ABOUT THE AUTHOR

Joe Coleman, the Cyber Security Officer and CMMC RPA (Registered Practitioner Advanced) for Bluestreak Compliance™ and Bluestreak | Bright AM™, an RPO (Registered Practitioner Organization), has more than 35 years of manufacturing, management, and engineering experience. He holds extensive cybersecurity training, DFARS, NIST SP 800-171, and CMMC.