

Commitment to CMMC 2.0 Level 2 Compliance

Protecting Our Customers' Data is a Top Priority

We are committed to upholding the highest standards of cybersecurity to support our customers—many of whom handle sensitive data such as Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). As part of this commitment, we are actively pursuing CMMC 2.0 Level 2 certification, with the support of specialized consultants, and are on track to achieve compliance by the first half of 2026. This milestone will reinforce our alignment with the stringent security requirements of the U.S. Department of Defense and further strengthen our customers' trust.

Key Milestones in Our CMMC Compliance Journey:

1. Gap Analysis and Remediation Planning (Completed by Q3 2024):

- Contracted an accredited C3PAO (CMMC Third-Party Assessment Organization) to provide a readiness assessment of the CIS controls framework v8 NIST800-171 v2 (CMMC)
- The C3PAO conducted a thorough gap analysis to identify areas where our current security policies, practices, and controls align with, and where they need to be enhanced for compliance.
- Based on this analysis, we have developed a comprehensive plan to address any identified gaps.

2. Implementation of Required Controls (Estimated Completion Q3 2025):

- Implementing a formal cybersecurity risk management and governance program.
- Training per our security awareness program schedule.
- Testing and monitoring the physical and technical controls.
- Updating organizational policies and procedures.
- Enhancing incident response workflows.

3. Pre-Assessment of Center for Internet Security (CIS) Controls (Estimated Completion for Q3 2025):

- Contracted a leading cybersecurity firm to:
 - Conduct a CIS controls-based and security posture analysis.
 - Document a threat focused risk register.
 - Create a risk treatment roadmap.
 - Create a governance program for sustainability of our security program.

4. Official CMMC 2.0 Level 2 Assessment:

- We plan to schedule our formal CMMC 2.0 Level 2 assessment with an accredited C3PAO (CMMC Third-Party Assessment Organization) based on current government timeline guidance.



What This Means for Our Customers

Achieving CMMC 2.0 Level 2 compliance will provide our customers with the assurance that their data is protected by industry-leading security practices. Our certification will also facilitate compliance for customers who are involved in DoD contracts and other government projects (when CMMC 2.0 is required), ensuring that their supply chain is secure and resilient.

Why Work with Scot Forge?

When you collaborate with Scot Forge, you're teaming up with a company that prioritizes both manufacturing excellence and cybersecurity. Our commitment to achieving CMMC 2.0 Level 2 certification reflects our dedication to protecting your sensitive data and ensuring compliance with industry standards.

We invite you to join us on this journey and experience the confidence that comes with working with a CMMC 2.0-certified partner.

If you have any questions, please contact us at secops@scotforge.com.

