1 Bethany Rd., Suite 26
Hazlet, NJ 07730
+1 (888) 727-1266
www.HighQA.com

High QA, Inc. Commitment to CMMC 2.0 Level 2 Compliance

Securing the Defense Manufacturing Quality Supply Chain Through Proactive Cybersecurity Excellence

Published: November 2025
Contact: security@highqa.com

Executive Summary

High QA, Inc. is committed to achieving Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2 compliance by Q1 2026, demonstrating our dedication to protecting the Defense Industrial Base (DIB) and enabling our customers to meet their critical national security obligations.

As a leading provider of on-premises manufacturing quality platform software for defense manufacturing, we recognize that our customers, DoD prime contractors and subcontractors, depend on secure, compliant technology solutions to protect Controlled Unclassified Information (CUI) and maintain their own CMMC certification requirements.

Our commitment represents more than regulatory compliance, reflects our responsibility as a trusted partner in the defense manufacturing quality supply chain.

Understanding CMMC 2.0: The Current Landscape

Official Implementation Timeline

The Department of Defense has established a clear, phased approach to CMMC 2.0 enforcement:

Regulatory Foundation:

1 Bethany Rd., Suite 26
Hazlet, NJ 07730
+1 (888) 727-1266
www.HighQA.com

- **December 16, 2024:** 32 CFR Part 170 (CMMC Program Rule) became effective
- **September 10, 2025:** 48 CFR DFARS rule published in Federal Register
- **November 10, 2025:** CMMC requirements begin appearing in DoD contracts

Four-Phase Rollout (32 CFR § 170.3(e)):

- **Phase 1 (November 10, 2025):** CMMC Level 1 and Level 2 self-assessments required; C3PAO assessments at DoD discretion
- **Phase 2 (November 10, 2026):** Level 2 C3PAO certifications required for new CUI contracts
- **Phase 3 (November 10, 2027):** Level 2 certifications required for option period exercises; Level 3 introduced
- **Phase 4 (November 10, 2028):** Full implementation across all applicable DoD contracts

What This Means for Defense Manufacturers

DoD contractors handling CUI must achieve and maintain CMMC 2.0 Level 2 certification, which requires:

- Implementation of all 110 security requirements from NIST SP 800-171 Revision 2
- Third-party assessment by a CMMC Third-Party Assessment Organization (C3PAO) or annual self-assessment
- Current certification status posted in the Supplier Performance Risk System (SPRS)
- FedRAMP Moderate authorized cloud services for any CUI in cloud environments

Critical compliance requirement: Contractors cannot be awarded new DoD contracts without current CMMC certification status in SPRS at the required level.

High QA's CMMC Journey: A Proactive Commitment

Our Strategic Approach

High QA identified CMMC 2.0 Level 2 as a critical strategic initiative in 2024, recognizing our responsibility to the defense manufacturing community we serve. Our approach has been methodical and comprehensive:

2024 Actions Completed:

1 Bethany Rd., Suite 26
Hazlet, NJ 07730
+1 (888) 727-1266
www.HighQA.com

- Designated CMMC 2.0 Level 2 as a strategic business priority
- June 2024, engaged with certified third-party cybersecurity consultants (COMMIT-US) to assess our security posture
- October 2024, completed comprehensive gap analysis against NIST SP 800-171 requirements
- Identified remediation priorities and developed implementation roadmap
- Initiated security control implementation and documentation

2025 Progress:

- Implemented Vanta (www.vanta.com) – GRC platform with CMMC 2.0 module for automated evidence collection and control tracking
- Ongoing implementation of technical and administrative security controls
- Development of System Security Plan (SSP) and supporting documentation
- Security awareness training for all personnel
- Establishment of continuous monitoring and compliance validation processes

Q1 2026 Target Completion:

- Finalization of all 110 NIST SP 800-171 security requirements
- Completion of comprehensive CMMC 2.0 Level 2 self-assessment
- Submission of assessment results to SPRS
- Preparation for potential C3PAO assessment as market demands evolve

Why Our Compliance Matters to Your Organization

As an **on-premises software provider**, High QA's quality management solutions are deployed directly within your secure environment. When your organization processes CUI using our software, **our security posture becomes part of your CMMC assessment scope.**

Our CMMC 2.0 Level 2 compliance provides:

1. **Supply Chain Assurance:** Demonstrates that High QA employs the same rigorous cybersecurity controls required of DoD contractors
2. **Reduced Assessment Burden:** Minimizes questions and concerns during your CMMC assessments about vendor security practices
3. **Secure Software Development:** Validates our commitment to security-by-design principles throughout our development lifecycle
4. **Vulnerability Management:** Ensures we maintain robust processes for identifying and remediating security vulnerabilities

1 Bethany Rd., Suite 26
Hazlet, NJ 07730
+1 (888) 727-1266
www.HighQA.com

5. **Long-term Partnership Viability:** Confirms High QA's commitment to remaining a compliant, trusted partner as CMMC requirements evolve

---

What Sets High QA Apart

1. Proactive Leadership in Software Security

While many software vendors wait for customer demands or contractual requirements, High QA has taken a proactive stance on CMMC compliance. Our early commitment demonstrates:

- **Strategic foresight:** Understanding the critical importance of cybersecurity in defense manufacturing
- **Customer-centric approach:** Anticipating our customers' needs before they become urgent requirements
- **Cultural commitment:** Embedding security practices throughout our organization, not treating compliance as a checkbox exercise

2. On-Premises Architecture Advantage

Our fully on-premises deployment model provides inherent security benefits for defense contractors:

- **No cloud dependencies:** Your CUI remains within your controlled environment
- **No external data transmission:** Our software doesn't send telemetry, diagnostics, or data to High QA systems
- **No remote access requirements:** We don't maintain administrative access to your production systems
- **Customer-controlled updates:** You manage patching and updates on your schedule
- **Air-gap compatible:** Can operate in completely isolated networks when required

3. Secure Software Development Lifecycle

High QA applies security best practices throughout our development process:

- **Security requirements analysis:** Security considerations integrated from initial design
- **Secure coding standards:** Adherence to OWASP and industry best practices
- **Code review and testing:** Security-focused peer reviews and automated scanning
- **Vulnerability management:** Structured process for identifying and remediating vulnerabilities
- **Supply chain risk management:** Vetting of third-party components and dependencies
- **Software Bill of Materials (SBOM):** Comprehensive tracking of software components

4. Transparency and Partnership

We believe in open communication with our customers about our security posture:

- **Documentation availability:** Security documentation provided during procurement processes
- **Assessment coordination:** Support during your CMMC assessments regarding our software
- **Vulnerability disclosure:** Timely notification of any security issues affecting our products
- **Security roadmap sharing:** Regular updates on our compliance journey and security enhancements

---

Benefits to Our Defense Manufacturing Customers

Streamlined CMMC Assessment Process

When you use High QA's quality management software in your CMMC assessment:

✓ **Reduced vendor risk questions:** Our CMMC compliance documentation addresses common assessor concerns about third-party software

✓ **Clear security boundaries:** Our on-premises architecture simplifies scope definition for your assessment

✓ **Documented security controls:** Our SSP and security documentation support your own compliance evidence

1 Bethany Rd., Suite 26
Hazlet, NJ 07730
+1 (888) 727-1266
www.HighQA.com

✓ **No cloud service complications:** No need to validate FedRAMP equivalency for High QA systems

Competitive Advantage

High QA's CMMC commitment provides your organization:

✓ **Faster contract qualification:** Reduced delays in vendor security validation processes

✓ **Prime contractor confidence:** Demonstrates your supply chain security to prime contractors

✓ **Reduced audit findings:** Minimizes potential non-conformances related to vendor management

✓ **Future-proof partnership:** Assurance that High QA will meet evolving DoD cybersecurity requirements

Operational Excellence

Beyond compliance, our security program delivers:

✓ **Enhanced product security:** Reduced vulnerability risk in our software protecting your operations

✓ **Reliable support:** Security-trained personnel supporting your critical manufacturing systems

✓ **Business continuity:** Robust incident response ensuring minimal disruption

✓ **Continuous improvement:** Ongoing security enhancements aligned with emerging threats

---

1 Bethany Rd., Suite 26
Hazlet, NJ 07730
+1 (888) 727-1266
www.HighQA.com

Our Commitment Moving Forward

High QA's pursuit of CMMC 2.0 Level 2 compliance is not a one-time project—it represents our ongoing commitment to cybersecurity excellence and support for the Defense Industrial Base.

Continuous Improvement

- **Regular security assessments:** Periodic third-party security testing and vulnerability assessments
- **Threat intelligence monitoring:** Staying informed of emerging threats affecting manufacturing systems
- **Control effectiveness validation:** Ongoing monitoring to ensure security controls remain effective
- **Industry engagement:** Active participation in defense cybersecurity forums and working groups

Long-term Partnership

- **Regulatory monitoring:** Tracking DoD policy changes and CMMC program evolution
- **Customer support:** Assisting customers with security documentation and assessment preparation
- **Security enhancements:** Continuously improving product security features and controls
- **Transparent communication:** Proactive updates on our compliance status and security posture

Organizational Culture

- **Security awareness:** All-hands training and security-first mindset across the organization
- **Accountability:** Clear roles and responsibilities for security program management
- **Resource commitment:** Dedicated budget and personnel for cybersecurity initiatives
- **Executive sponsorship:** Board-level oversight of cybersecurity risk and compliance

1 Bethany Rd., Suite 26
Hazlet, NJ 07730
+1 (888) 727-1266
www.HighQA.com

Conclusion

The defense manufacturing sector faces unprecedented cybersecurity challenges. Nation-state adversaries actively target the Defense Industrial Base, seeking to steal sensitive technology, disrupt critical operations, and compromise national security.

High QA recognizes that protecting CUI is not merely a compliance requirement, it is a patriotic duty and a business imperative.

By pursuing CMMC 2.0 Level 2 compliance, we are:

- **Protecting our customers' ability to compete** for and maintain DoD contracts
- **Strengthening the security** of the defense supply chain
- **Supporting national security** through responsible technology practices
- **Building trust** through transparency and proactive action

We are proud to serve the defense manufacturing community and honored to contribute to the protection of sensitive defense information. Our CMMC journey reflects our values: integrity, excellence, and unwavering commitment to our customers' success.

Contact Information

For questions about High QA's CMMC compliance program, security practices, or to request supporting documentation:

Email: security@highqa.com
Subject Line: CMMC Compliance Inquiry

We welcome inquiries from current and prospective customers, prime contractors conducting vendor assessments, and CMMC assessors requiring documentation to support customer assessments.

---

1 Bethany Rd., Suite 26
Hazlet, NJ 07730
+1 (888) 727-1266
www.HighQA.com

Additional Resources

Department of Defense CMMC Resources:

- DoD CIO CMMC Website: https://dodcio.defense.gov/CMMC/
- CMMC Accreditation Body (Cyber AB): https://cyberab.org/
- CMMC Model Overview: https://dodcio.defense.gov/CMMC/Model/

NIST Cybersecurity Resources:

- NIST SP 800-171 Rev 2: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

---

This Compliance Statement is current as of November 2025. CMMC 2.0 Level 2 requirements and timelines are subject to change based on DoD policy updates. High QA commits to maintaining current information and updating this document as our compliance journey progresses.

Document Version: 3.0
Last Updated: November 2025
Next Review: January 2026

1 Bethany Rd., Suite 26
Hazlet, NJ 07730
+1 (888) 727-1266
www.HighQA.com

Exhibit 1

Our Security Framework: NIST 800-171 Implementation

High QA's security program is built on the 110 security requirements outlined in NIST Special Publication 800-171, organized across 14 security domains:

Core Security Domains

Access Control (22 requirements)

- Role-based access controls and least privilege principles
- Multi-factor authentication for privileged access
- Session management and account lifecycle controls

Awareness and Training (8 requirements)

- Comprehensive security awareness program for all personnel
- Role-based training for developers and administrators
- Insider threat awareness and reporting mechanisms

Audit and Accountability (9 requirements)

- Comprehensive logging and monitoring across all systems
- Protected audit records with integrity verification
- Regular audit log review and analysis

Configuration Management (9 requirements)

- Baseline configurations and change control processes
- Software inventory and license management
- Least functionality principles applied across systems

Identification and Authentication (11 requirements)

- Strong authentication mechanisms and password policies
- Cryptographic protection of authentication credentials
- Device identification and authorization

Incident Response (4 requirements)

1 Bethany Rd., Suite 26
Hazlet, NJ 07730
+1 (888) 727-1266
www.HighQA.com

- Documented incident response plan and procedures
- 72-hour cyber incident reporting capability (DFARS 252.204-7012)
- Incident tracking and lessons learned processes

Maintenance (6 requirements)

- Controlled maintenance activities with audit trails
- Sanitization of equipment before maintenance
- Remote maintenance authorization and monitoring

Media Protection (8 requirements)

- Media marking, storage, and sanitization procedures
- CUI data protection throughout the information lifecycle
- Secure disposal and destruction processes

Personnel Security (2 requirements)

- Personnel screening appropriate to risk level
- Termination procedures ensuring access revocation

Physical Protection (6 requirements)

- Controlled facility access with visitor management
- Physical safeguards for information systems and media
- Monitoring and escort procedures

Risk Assessment (3 requirements)

- Regular vulnerability assessments and penetration testing
- Risk-based approach to security control implementation
- Continuous threat intelligence monitoring

Security Assessment (4 requirements)

- Regular security control assessments
- Plan of Action and Milestones (POA&M) for identified gaps
- Continuous monitoring and security posture improvement

System and Communications Protection (16 requirements)

- Encryption of CUI at rest and in transit

- Boundary protection and network segmentation
- Secure communications protocols and cryptographic key management

System and Information Integrity (12 requirements)

- Malware protection with real-time monitoring
- Timely security patch management
- Information input validation and error handling

1 Bethany Rd., Suite 26
Hazlet, NJ 07730
+1 (888) 727-1266
www.HighQA.com

Exhibit 2

Frequently Asked Questions

Q: When will High QA's CMMC Level 2 assessment be complete?

A: We are targeting completion of our CMMC Level 2 self-assessment and SPRS registration by Q1 2026. We are implementing all 110 NIST 800-171 requirements and developing comprehensive documentation to support either self-assessment or third-party C3PAO assessment as requirements evolve.

Q: Can we use High QA software before your CMMC certification is complete?

A: Yes. Our on-premises software is deployed and operated entirely within your controlled environment. Your CMMC assessor will evaluate how you've secured and configured our software within your system, but our pending certification demonstrates our commitment to security best practices that align with NIST 800-171 requirements. Many customers choose to include our compliance documentation as supporting evidence during their assessments.

Q: Does High QA handle or access our CUI?

A: No. Our software runs entirely on-premises in your environment. We do not maintain remote access to your systems, and we do not host any components of your solution. License activation and optional diagnostic features can be disabled for air-gapped deployments. Your CUI remains entirely under your control within your CMMC-assessed boundary.

Q: What happens if you identify security vulnerabilities in your software?

A: We maintain a comprehensive vulnerability management program aligned with NIST 800-171 requirements. If we identify security vulnerabilities, we follow a structured process: immediate risk assessment, development of patches or mitigations, notification to affected customers, and coordinated remediation. Our incident response procedures ensure rapid communication and resolution.

Q: Will you pursue C3PAO certification in the future?

A: We are monitoring market requirements and customer needs. While our initial focus is completing our Level 2 self-assessment, we are prepared to pursue C3PAO certification if

1 Bethany Rd., Suite 26
Hazlet, NJ 07730
+1 (888) 727-1266
www.HighQA.com

it becomes necessary to serve our customers' evolving compliance requirements or if DoD policy shifts toward requiring third-party assessments for software vendors.

Q: How does your CMMC compliance affect our subcontractor flow-down requirements?

A: As a commercial software vendor providing an off-the-shelf product deployed on-premises, High QA would not typically be considered a subcontractor requiring CMMC flow-down. However, our voluntary pursuit of CMMC Level 2 compliance demonstrates that we meet or exceed the security standards that would apply to entities in your supply chain, simplifying vendor risk management.

Q: What documentation can High QA provide to support our CMMC assessment?

A: Upon request and under appropriate non-disclosure agreements, we can provide: System Security Plan (SSP) excerpts relevant to our software, secure development lifecycle documentation, vulnerability management procedures, security test results, and software security architecture documentation. We work collaboratively with customers and their assessors to provide appropriate evidence.