DOMINUS GRAY, LLC

Securing Access to Opportunity

CMMC Level 2
Gap Assessment Report

NIST SP 800-171 Rev 2 Compliance Assessment

PREPARED FOR

Meridian Defense Systems, Inc.

February 2026

Document ID: DG-CMMC-GA-2026-001

CONFIDENTIAL — DO NOT DISTRIBUTE

SDVOSB | MBE | NaBOVA | VetHUB | SAM.gov Registered

Service-Disabled Veteran-Owned Small Business

Table of Contents

1. Executive Summary

SPRS SCORE	CONTROLS MET	CRITICAL FINDINGS	HIGH FINDINGS
53	64/110	4	10
of 110 (48%)	58% compliant	Require immediate action	Address within 90 days

CONDITIONAL CERTIFICATION: NOT YET ELIGIBLE

A minimum score of 88/110 is required for CMMC 2.0 conditional certification. Meridian Defense Systems, Inc.'s current score of 53/110 requires remediation of 35 additional points before conditional status can be achieved. All 5-point and 3-point control deficiencies must be addressed first — POA&Ms are only permitted for 1-point controls.

Dominus Gray, LLC conducted a comprehensive CMMC Level 2 gap assessment of Meridian Defense Systems, Inc.'s information systems and security controls against all 110 NIST SP 800-171 Rev 2 requirements. This assessment evaluates Meridian Defense Systems, Inc.'s readiness for formal C3PAO certification assessment.

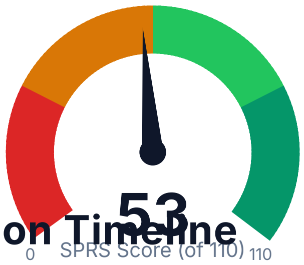
Key Findings

- 64 of 110 controls fully implemented (58% compliant)
- 30 controls partially implemented — require targeted remediation
- 16 controls not met — including 4 critical deficiencies that will block certification
- Current SPRS score: 53/110 — 35 points below conditional certification threshold
- Estimated remediation timeline: 10–14 months to assessment-ready status
- Primary gaps: Network segmentation (CUI boundary), MFA enforcement, FIPS-validated cryptography, SIEM deployment

Critical Path Items

These 4 items must be resolved before C3PAO engagement:

1. CUI Network Boundary & Segmentation (AC.L2-3.1.3, SC.L2-3.13.1)
2. FIPS 140-2 Validated Cryptography (SC.L2-3.13.11)
3. Multi-Factor Authentication on all CUI access (IA.L2-3.5.3)
4. Centralized Audit Logging & SIEM (AU.L2-3.3.1)



CMMC 2.0 Implementation Timeline

PHASE	DATE	MILESTONE
Phase 1	**Nov 2025**	Self-assessments begin for CMMC Level 1 & Level 2
Phase 2	**Nov 2026**	Mandatory C3PAO assessments required for Level 2 contracts
Phase 3	**Nov 2027**	Level 3 requirements take effect (DIBCAC-led assessments)
Phase 4	**Nov 2028**	Universal mandatory compliance across all DoD contracts

⚠ CRITICAL DEADLINE

Meridian Defense Systems, Inc. must complete C3PAO certification by November 2026 to maintain eligibility for CUI contracts.

2. Assessment Overview & Methodology

ASSESSMENT SCOPE

Client: Meridian Defense Systems, Inc.

Industry: Defense Contractor (DoD)

Employees: 200–500

Facilities: 3 locations (HQ + 2 field offices)

CUI Systems: 12 servers, 180 endpoints, 3 network segments

Assessment Level: CMMC Level 2 (110 controls)

Framework: NIST SP 800-171 Rev 2

ASSESSMENT TEAM

Lead Assessor: Certified CMMC Professional (CCP)

Assessment Type: Readiness / Gap Assessment

Duration: 4 weeks (on-site + remote)

Methods: Document review, interviews, technical testing, observation

Date Range: January 13 – February 7, 2026

Organization: Dominus Gray, LLC (RPO)

Report Date: February 9, 2026

Methodology

This assessment was conducted in accordance with NIST SP 800-171A assessment procedures and the CMMC Assessment Process (CAP). Each of the 110 security requirements was evaluated against the corresponding assessment objectives (320 total procedures) using a combination of:

- Document Review — Policies, procedures, system documentation, network diagrams, prior audit reports
- Personnel Interviews — IT staff, security personnel, system administrators, management, end users
- Technical Testing — Configuration reviews, vulnerability scanning, access control validation, log analysis
- Physical Observation — Facility walkthroughs, server room inspections, media handling practices

> **Important Distinction**
>
> This is a readiness assessment, not a formal CMMC certification assessment. Formal certification assessments are conducted exclusively by accredited C3PAOs (CMMC Third-Party Assessment Organizations). This report identifies gaps and provides a remediation roadmap to prepare for successful C3PAO assessment.

3. SPRS Score Dashboard

CURRENT SPRS SCORE

53 / 110

Conditional Certification ThresholdFull Compliance Target

88

Gap: 35 points

110

Gap: 57 points

Score Breakdown by Control Family

AC	Access Control	**64%**	14/22	3 GAPS
AT	Awareness & Training	**33%**	1/3	2 PARTIAL
AU	Audit & Accountability	**56%**	5/9	2 GAPS
CM	Configuration Management	**56%**	5/9	1 GAP
IA	Identification & Authentication	**64%**	7/11	1 GAP
IR	Incident Response	**33%**	1/3	1 GAP
MA	Maintenance	**67%**	4/6	2 PARTIAL

MP	Media Protection	67%	6/9	1 GAP
PS	Personnel Security	100%	2/2	COMPLIANT
PE	Physical Protection	83%	5/6	1 PARTIAL
RA	Risk Assessment	33%	1/3	1 GAP
CA	Security Assessment	25%	1/4	1 GAP
SC	System & Communications Protection	56%	9/16	3 GAPS
SI	System & Information Integrity	43%	3/7	2 GAPS

SPRS Scoring Methodology

Scoring starts at 110 and deducts points for each unmet control: 5 points for critical controls, 3 points for significant controls, and 1 point for standard controls. Partially implemented controls receive half-point deductions (rounded up). Under CMMC 2.0,

4. Risk Heat Map — Control Family Analysis

The following heat map visualizes risk exposure across all 14 NIST 800-171 control families. Colors indicate the highest-severity finding within each family. Families with critical findings must be prioritized for remediation.

AC Access Control **CRITICAL**	**AT** Awareness & Training **MEDIUM**	**AU** Audit & Accountability **HIGH**	**CM** Configuration Management **HIGH**	**IA** Identification & Authentication **CRITICAL**
IR Incident Response **HIGH**	**MA** Maintenance **MEDIUM**	**MP** Media Protection **HIGH**	**PS** Personnel Security **MET**	**PE** Physical Protection **LOW**
RA Risk Assessment **HIGH**	**CA** Security Assessment **HIGH**	**SC** System & Communications Protection **CRITICAL**	**SI** System & Information Integrity **HIGH**	

Risk Distribution Summary

CRITICAL	HIGH	MEDIUM	LOW
4	10	5	1
20% of findings	50% of findings	25% of findings	5% of findings

Risk Rating Criteria

CRITICAL: Control failure directly blocks CMMC certification or exposes CUI to immediate compromise. Typically 5-point controls.
HIGH: Significant security gap that materially weakens CUI protection. Must be addressed before C3PAO assessment.
LOW: Minor gap with limited direct impact. Can be addressed during normal

5. Detailed Findings by Control Family

AC — Access Control

14 Met | 5 Partial | 3 Not Met

64%

22 Controls

AC.L2-3.1.3: CUI Flow Control

CRITICAL

Point Value: 5

Finding: No network segmentation between CUI and non-CUI environments. CUI data traverses shared network segments without boundary controls.

Impact: Direct exposure of CUI to unauthorized network segments. C3PAO will fail this control.

Recommendation: Implement VLAN segmentation with firewall ACLs between CUI and corporate networks. Deploy jump servers for administrative access.

AC.L2-3.1.5: Least Privilege

HIGH

Point Value: 3

Finding: Admin accounts used for daily operations. 47 users have domain admin privileges; only 8 require elevated access.

Impact: Excessive privilege increases blast radius of compromised accounts.

Recommendation: Implement tiered admin model. Remove unnecessary admin rights. Deploy PAM solution for just-in-time elevation.

AC.L2-3.1.12: Remote Access Control

MEDIUM

Point Value: 1

Finding: VPN access lacks MFA for 23% of remote users. Split tunneling enabled on some endpoints.

Impact: Unauthorized remote access pathway to CUI environment.

Recommendation: Enforce MFA on all VPN connections. Disable split tunneling. Implement always-on VPN policy.

AT — Awareness & Training

1 Met | 2 Partial | 0 Not Met

33%

3 Controls

AT.L2-3.2.1: Security Awareness

MEDIUM

Point Value: 1

Finding: Annual security training exists but lacks CUI-specific modules. No role-based training for system administrators.

Impact: Personnel may not recognize CUI handling requirements.

Recommendation: Develop CUI-specific training module. Implement role-based training tracks. Add quarterly phishing simulations.

AU — Audit & Accountability

5 Met | 2 Partial | 2 Not Met

56%

9 Controls

AU.L2-3.3.1: System Auditing

HIGH

Point Value: 5

Finding: Audit logging not enabled on 4 of 12 servers processing CUI. No centralized log aggregation. Logs stored locally with 30-day retention.

Impact: Inability to detect, investigate, or respond to security incidents in CUI environment.

Recommendation: Deploy SIEM (Splunk/Sentinel). Enable audit logging on all CUI systems. Implement 1-year log retention with immutable storage.

AU.L2-3.3.5: Audit Log Correlation

HIGH

Point Value: 3

Finding: No capability to correlate audit records across systems. Manual log review only.

Impact: Cannot detect coordinated attacks or lateral movement.

Recommendation: Implement SIEM correlation rules. Deploy automated alerting for high-risk events.

CM — Configuration Management

5 Met | 3 Partial | 1 Not Met

56%

9 Controls

CM.L2-3.4.1: Baseline Configuration

MEDIUM

Point Value: 3

Finding: Baseline configurations exist for servers but not for workstations or network devices. No automated compliance scanning.

Impact: Configuration drift creates unknown vulnerabilities.

Recommendation: Establish baselines using CIS Benchmarks. Deploy configuration scanning tool. Implement change detection.

This document contains confidential and proprietary information.

CM.L2-3.4.6: Least Functionality

HIGH

Point Value: 3

Finding: Unnecessary services running on CUI servers (FTP, Telnet, legacy protocols). No application whitelisting.

Impact: Expanded attack surface on CUI-processing systems.

Recommendation: Disable unnecessary services per DISA STIGs. Implement application whitelisting on CUI endpoints.

IA — Identification & Authentication

7 Met | 3 Partial | 1 Not Met

64%

11 Controls

IA.L2-3.5.3: Multi-Factor Authentication

CRITICAL

Point Value: 5

Finding: MFA deployed for cloud services but not enforced for on-premises CUI systems, VPN, or privileged accounts.

Impact: Single-factor authentication on CUI systems is a C3PAO automatic failure.

Recommendation: Deploy MFA across all CUI access points: on-prem login, VPN, RDP, and admin consoles. Hardware tokens for privileged accounts.

IR — Incident Response

1 Met | 1 Partial | 1 Not Met

33%

3 Controls

IR.L2-3.6.1: Incident Handling

HIGH

Point Value: 3

Finding: No documented incident response plan. No designated CSIRT. No DCISE Cybersecurity Reporting Portal (https://icf.dcise.cert.org) reporting procedures established.

Impact: Unable to meet DoD 72-hour incident reporting requirement. Breach response will be ad hoc.

Recommendation: Develop comprehensive IRP covering detection, analysis, containment, eradication, recovery. Establish DCISE Cybersecurity Reporting Portal (https://icf.dcise.cert.org) reporting procedures. Designate and train CSIRT.

MA — Maintenance

4 Met | 2 Partial | 0 Not Met

67%

6 Controls

MA.L2-3.7.5: Nonlocal Maintenance

MEDIUM

Point Value: 1

Finding: Remote maintenance sessions not logged or monitored. Third-party vendor remote access uses shared credentials.

Impact: Unauthorized maintenance access goes undetected.

Recommendation: Implement session recording for remote maintenance. Issue unique credentials to each vendor. Require MFA.

This document contains confidential and proprietary information.

MP — Media Protection

6 Met | 2 Partial | 1 Not Met

67%

9 Controls

MP.L2-3.8.9: CUI Backup Protection

HIGH

Point Value: 3

Finding: Backup tapes containing CUI stored in unlocked cabinet. No encryption on backup media. Off-site transport not secured.

Impact: CUI data loss or exposure through physical media theft.

Recommendation: Encrypt all backup media (AES-256). Implement locked storage with access logging. Use bonded courier for off-site transport.

PS — Personnel Security

2 Met | 0 Partial | 0 Not Met

100%

2 Controls

All 2 controls in the Personnel Security family are fully implemented. No findings.

PE — Physical Protection

5 Met | 1 Partial | 0 Not Met

83%

6 Controls

PE.L2-3.10.6: Alternate Work Site

LOW

Point Value: 1

Finding: Remote work policy exists but lacks specific CUI handling procedures for home offices.

Impact: CUI may be accessed in uncontrolled environments.

Recommendation: Update remote work policy with CUI-specific requirements. Require encrypted drives and screen privacy filters for remote CUI access.

RA — Risk Assessment

1 Met | 1 Partial | 1 Not Met

33%

3 Controls

RA.L2-3.11.2: Vulnerability Scanning

HIGH

Point Value: 3

Finding: No regular vulnerability scanning program. Last scan was 14 months ago. No remediation SLAs.

Impact: Unknown vulnerabilities in CUI environment. Cannot demonstrate continuous monitoring.

Recommendation: Implement monthly vulnerability scanning (Tenable/Qualys). Define remediation SLAs: Critical 48hr, High 7d, Medium 30d. Report monthly.

CA — Security Assessment

1 Met 2 Partial 1 Not Met

25%

4 Controls

CA.L2-3.12.1: Security Assessments

HIGH

Point Value: 3

Finding: No periodic security assessment program. This gap assessment is the first formal evaluation.

Impact: No ongoing validation of security control effectiveness.

Recommendation: Establish annual security assessment cycle. Include penetration testing of CUI boundary. Document findings and track remediation.

SC — System & Communications Protection

9 Met 4 Partial 3 Not Met

56%

16 Controls

SC.L2-3.13.1: Boundary Protection

CRITICAL

Point Value: 5

Finding: CUI environment shares network boundary with general corporate network. No DMZ for external-facing CUI services.

Impact: Core CMMC L2 requirement. Failure here blocks certification.

Recommendation: Architect dedicated CUI enclave with defined security boundary. Implement next-gen firewall with IPS at boundary. Create DMZ for external CUI services.

SC.L2-3.13.8: CUI Transmission Encryption

HIGH

Point Value: 3

Finding: TLS 1.2+ enforced for web traffic. Internal email between CUI users not encrypted. File transfers use unencrypted SMB.

Impact: CUI exposed in transit within internal network.

Recommendation: Implement S/MIME or equivalent for internal CUI email. Deploy SMB signing and encryption. Validate all CUI transmission paths use FIPS 140-2 validated encryption.

SC.L2-3.13.11: FIPS-Validated Cryptography

CRITICAL

Point Value: 5

Finding: VPN and disk encryption use non-FIPS validated modules. Wireless encryption not FIPS-compliant.

Impact: Non-negotiable CMMC requirement. All cryptography protecting CUI must use FIPS 140-2 validated modules.

Recommendation: Replace or reconfigure VPN to use FIPS 140-2 validated modules. Enable FIPS mode on Windows endpoints. Validate all cryptographic implementations. Note: Cloud services processing, storing, or transmitting CUI must use FedRAMP Moderate (or equivalent) authorized CSPs per DFARS 252.204-7012. Verify all cloud service providers at marketplace.fedramp.gov.

This document contains confidential and proprietary information.

SI — System & Information Integrity

43%

3 Met | 2 Partial | 2 Not Met

7 Controls

SI.L2-3.14.1: Flaw Remediation

HIGH

Point Value: 3

Finding: Patch management process exists but is inconsistent. 34% of CUI systems are 60+ days behind on critical patches.

Impact: Known vulnerabilities exploitable in CUI environment.

Recommendation: Implement automated patch management (WSUS/SCCM). Define patch SLAs aligned with CMMC. Generate monthly compliance reports.

SI.L2-3.14.6: Security Alerts

MEDIUM

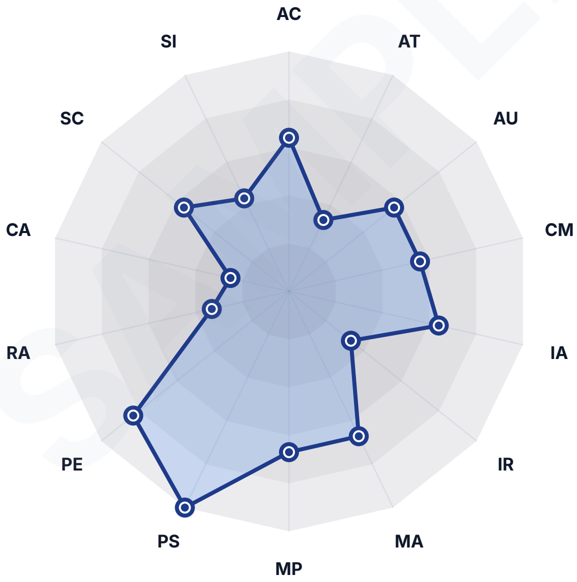
Point Value: 3

Finding: No process to monitor security advisories from vendors and CISA. No mechanism to evaluate applicability to CUI environment.

Impact: May miss critical vulnerabilities affecting CUI systems.

Recommendation: Subscribe to CISA alerts, vendor security bulletins. Assign responsibility for triage and response. Document in IRP.

Control Family Maturity Radar



FORWARD LOOK: NIST SP 800-171 Revision 3

NIST published SP 800-171 Rev 3 in May 2024, consolidating 110 controls into 97 requirements aligned with SP 800-53 Rev 5. CMMC 2.0 currently requires Rev 2 compliance; DoD has not announced a Rev 3 transition date. Dominus Gray recommends maintaining Rev 2 compliance while conducting a parallel Rev 3 gap analysis to minimize future transition effort. Key Rev 3 changes include: new Supply Chain Risk Management (SR) controls, Organization-Defined Parameters (ODPs) replacing vague timing language, and enhanced continuous monitoring requirements.

FedRAMP Moderate Requirement

Cloud services processing, storing, or transmitting CUI must use FedRAMP Moderate (or equivalent) authorized CSPs per DFARS 252.204-7012. Verify all cloud service providers at marketplace.fedramp.gov.

6. Remediation Roadmap

The following phased roadmap prioritizes remediation by risk severity, control dependencies, and C3PAO assessment readiness. The timeline targets assessment readiness within 10–14 months.

Phase 1: Foundation & Critical Fixes

Months 1–3

TASK	CONTROLS	EFFORT	DEPENDENCIES	POINT
CUI Network Segmentation & Boundary	AC.L2-3.1.3, SC.L2-3.13.1	High	Network architecture review	10
FIPS 140-2 Cryptography	SC.L2-3.13.11	High	Crypto inventory	5
MFA Deployment (all CUI access)	IA.L2-3.5.3	Medium	Identity provider setup	5
SIEM Deployment & Log	AU.L2-3.3.1, AU.L2-3.3.5	High	Infrastructure ready	8
Incident Response Plan Development	IR.L2-3.6.1	Medium	None	3

Phase 2: Core Implementation

Months 3–9

TASK	CONTROLS	EFFORT	DEPENDENCIES	POINT
Privileged Access Management	AC.L2-3.1.5	Medium	Phase 1 network segmentation	3
Vulnerability Scanning Program	RA.L2-3.11.2	Medium	Asset inventory	3
Configuration Baseline (DISA STIGs)	CM.L2-3.4.1, CM.L2-3.4.6	High	Endpoint inventory	6
Automated Patch Management	SI.L2-3.14.1	Mediu	Configuration baselines	3
CUI Transmission Encryption	SC.L2-3.13.8	Medium	FIPS crypto in place	3
Backup Media Encryption &	MP.L2-3.8.9	Low	FIPS crypto in place	3
Security Assessment Program	CA.L2-3.12.1	Medium	Scanning tools deployed	3

Phase 3: Maturity & Assessment Prep

Months 9–14

TASK	CONTROLS	EFFORT	DEPENDENCIES	POINT
SSP Finalization & Evidence Collection	All families	High	All controls implemented	
CUI Training Program (role-	AT.L2-3.2.1	Low	CUI scope defined	1
Security Alert Monitoring Process	SI.L2-3.14.6	Low	SIEM operational	3
Remote Work CUI Policy	PE.L2-3.10.6	Low	CUI policies finalized	1
Remote Maintenance Controls	MA.L2-3.7.5	Low	PAM solution	1
Full Mock Assessment	All families	Mediu	All above complete	
C3PAO Selection & Scheduling	N/A	Low	Mock assessment passed	

7. Business Impact Analysis

CMMC certification is not optional for DoD contractors handling CUI. Without certification, Meridian Defense Systems, Inc. will be ineligible to bid on or maintain contracts requiring CMMC Level 2. The following analysis quantifies the business impact of the current gaps.

RISK: Do Nothing

- Loss of DoD contract eligibility ($25M–$50M+ annual revenue at risk)
- Inability to bid on new CMMC-required solicitations
- Breach exposure: $4.88M average cost (IBM 2024)
- DCISE Portal reporting failures: potential False Claims Act liability
- Supply chain disqualification by prime contractors
- Competitive displacement by CMMC-certified competitors

VALUE: Certification ROI

- Protects $25M–$50M+ in existing DoD revenue
- Unlocks new contract opportunities requiring CMMC L2
- 80% reduction in breach probability (NIST framework)
- Insurance premium reductions (documented security program)
- Competitive advantage: early certification = market differentiation
- Investment-to-protected-revenue ratio: 140:1 to 590:1

⚠ FALSE CLAIMS ACT LIABILITY

The DOJ Civil Cyber-Fraud Initiative actively pursues contractors who misrepresent their cybersecurity compliance. Inaccurate SPRS scores or false self-assessments can result in treble damages and per-claim penalties. In February 2025, a contractor paid $11.3M to settle False Claims Act allegations related to cybersecurity misrepresentation. Accurate self-assessment and documented remediation are essential legal protections.

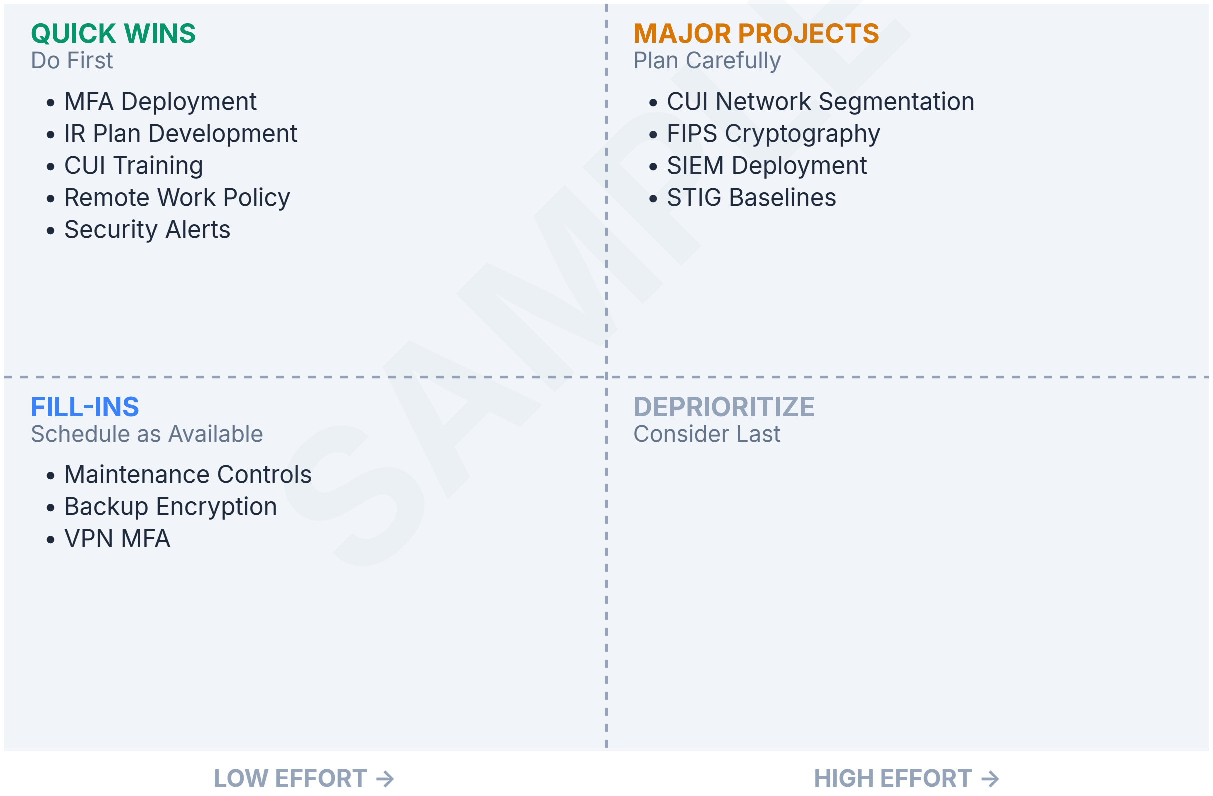
Investment Summary

Estimated remediation investment: $85,000–$200,000 (consulting + technology)
C3PAO assessment fee: $30,000–$80,000 (paid directly to assessor)
Total investment: $115,000–$280,000
Revenue protected: $25,000,000–$50,000,000+

Return on investment: Every $1 spent protects $89–$435 in contract revenue.

8. Effort vs. Impact Prioritization Matrix

This matrix categorizes all findings by implementation effort versus security impact, enabling efficient resource allocation. Focus on the upper-right quadrant (high impact, manageable effort) for maximum return.



QUICK WINS
Do First

- MFA Deployment
- IR Plan Development
- CUI Training
- Remote Work Policy
- Security Alerts

MAJOR PROJECTS
Plan Carefully

- CUI Network Segmentation
- FIPS Cryptography
- SIEM Deployment
- STIG Baselines

FILL-INS
Schedule as Available

- Maintenance Controls
- Backup Encryption
- VPN MFA

DEPRIORITIZE
Consider Last

9. Recommendations & Next Steps

Based on this assessment, Dominus Gray recommends the following engagement model to bring Meridian Defense Systems, Inc. to CMMC Level 2 certification readiness within 10–14 months:

01 **Remediation Planning Workshop** — **Week 1–2**
2-day on-site workshop to finalize remediation priorities, assign owners, establish KPIs, and build the project plan. Align IT, security, and business leadership.

02 **Phase 1 Critical Remediation** — **Months 1–3**
Address all critical and 5-point control deficiencies: network segmentation, FIPS cryptography, MFA enforcement, SIEM deployment. These are certification blockers.

03 **SSP Development & Documentation** — **Months 2–6**
Build the System Security Plan documenting all 110 controls. Create supporting documentation: network diagrams, data flow maps, CUI boundary definitions.

04 **Phase 2 Core Implementation** — **Months 3–9**
Implement remaining control deficiencies: PAM, vulnerability management, patch management, configuration baselines, backup controls.

05 **Evidence Collection & POA&M** — **Months 8–11**
Gather assessment evidence for all 320 assessment objectives. Create POA&M for any remaining 1-point items (only 1-point controls eligible for POA&M).

06 **Mock Assessment & C3PAO Prep** — **Months 10–14**
Full mock assessment simulating C3PAO evaluation. Identify and remediate any remaining gaps. Select and schedule C3PAO. Prepare personnel for assessment interviews.

Engagement Options

Option A — Full CMMC Readiness Program: $85,000–$200,000 (10–14 months)
Includes all phases above, SSP development, POA&M management, mock assessment, and C3PAO coordination.

Option B — V-CISO + CMMC Bundle: $8,000–$15,000/month (12-month retainer)
Ongoing security leadership plus CMMC readiness program. Includes monthly reporting, policy management, and incident response capability.

Option C — Phase 1 Pilot: $25,000–$40,000 (90 days)
Critical remediation only. Addresses the 4 certification blockers and establishes the foundation for full program.

Forward-Looking: Zero Trust Architecture

The DoD Zero Trust Strategy, published in November 2022, mandates that all DoD entities achieve a Zero Trust Architecture (ZTA) baseline by FY2027. NIST SP 800-207 defines the foundational principles of Zero Trust. Many CMMC Level 2 controls directly align with ZTA principles, positioning compliant organizations for a smoother transition to full Zero Trust implementation.

- Identity-Centric Security — CMMC MFA and least-privilege controls (AC.L2-3.1.5, IA.L2-3.5.3) map directly to ZTA Pillar 1 (Identity)
- Micro-Segmentation — CUI boundary protection (SC.L2-3.13.1) aligns with ZTA network micro-segmentation requirements
- Continuous Monitoring — Audit and vulnerability scanning requirements (AU.L2-3.3.1, RA.L2-3.11.2) support ZTA continuous diagnostics and monitoring
- Data-Centric Protection — CUI encryption and media protection controls align with ZTA Pillar 5 (Data)
- Automation & Orchestration — SIEM, automated patching, and configuration management provide the visibility layer required for ZTA decision engines

Software Supply Chain & SBOM Requirements

Executive Order 14028 (May 2021) directs federal agencies to enhance software supply chain security. DoD contractors should prepare for Software Bill of Materials (SBOM) requirements by inventorying all software components, establishing provenance verification, and integrating SBOM generation into development workflows. NIST SP 800-161 Rev 1 provides supply chain risk management guidance that complements CMMC controls. Organizations should begin tracking third-party software dependencies and maintaining current SBOMs for all CUI-processing systems.

Appendix A: Assessment Methodology

This assessment was conducted using the following standards and procedures:

- NIST Special Publication 800-171 Rev 2 — Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST Special Publication 800-171A — Assessing Security Requirements for CUI (320 assessment objectives)
- CMMC Assessment Process (CAP) — Cyber AB assessment methodology
- NIST Special Publication 800-53 Rev 5 — Referenced for enhanced control guidance
- DoD Assessment Methodology (DoDAM) — SPRS scoring methodology
- DISA Security Technical Implementation Guides (STIGs) — Configuration baseline reference
- FIPS 140-2/140-3 — Cryptographic module validation requirements

Control Assessment Status Definitions

MET The control is fully implemented and operating as intended. Evidence supports complete compliance with all assessment objectives.

PARTIALLY MET The control is partially implemented. Some assessment objectives are satisfied but gaps remain that must be remediated.

NOT MET The control is not implemented or evidence is insufficient to demonstrate compliance. Full remediation required.

Risk Rating Definitions

CRITICAL Exploitation is likely and would result in severe impact to CUI confidentiality. Blocks CMMC certification. Requires immediate remediation (0–30 days).

HIGH Exploitation is possible and would result in significant impact. Must be addressed before C3PAO assessment (30–90 days).

MEDIUM Exploitation requires specific conditions. Impact is moderate. Should be addressed within 180 days. May qualify for POA&M if 1-point control.

LOW Limited exploitability or impact. Address during normal operations. Qualifies for POA&M under conditional certification.

Appendix B: Glossary & References

C3PAO — CMMC Third-Party Assessment Organization — accredited by Cyber AB to conduct official CMMC assessments

CAP — CMMC Assessment Process — the standardized methodology for conducting CMMC assessments

CCP — Certified CMMC Professional — entry-level CMMC certification held by assessment team members

CCA — Certified CMMC Assessor — qualified to lead CMMC assessments and make certification recommendations

CUI — Controlled Unclassified Information — sensitive but unclassified information requiring safeguarding

DIBNet — Defense Industrial Base Network (decommissioned June 2025; replaced by DCISE Portal at https://icf.dcise.cert.org)

DFARS — Defense Federal Acquisition Regulation Supplement — DoD-specific acquisition rules

FIPS 140-2 — Federal Information Processing Standard for cryptographic module validation

FCI — Federal Contract Information — information provided by or generated for the government under contract

POA&M — Plan of Action & Milestones — documented plan to address identified security deficiencies

RPO — Registered Provider Organization — authorized by Cyber AB to provide CMMC consulting

SPRS — Supplier Performance Risk System — DoD portal for posting self-assessment scores

SSP — System Security Plan — documentation of how an organization meets security requirements

STIG — Security Technical Implementation Guide — DoD configuration standards published by DISA

References

- NIST SP 800-171 Rev 2, Protecting CUI in Nonfederal Systems (February 2020, Updated January 2021)
- NIST SP 800-171A, Assessing Security Requirements for CUI (June 2018)
- CMMC 2.0 Final Rule, 32 CFR Part 170 (Effective November 10, 2025)
- DFARS 252.204-7012, Safeguarding Covered Defense Information
- DFARS 252.204-7019/7020/7021, CMMC Assessment and Certification Requirements
- IBM Cost of a Data Breach Report 2024
- NIST Cybersecurity Framework (CSF) 2.0 (February 2024)

DOMINUS GRAY, LLC

Securing Access to Opportunity

Odie Gray, CEO
odie.gray@dominusgray.com
www.dominusgray.com

SDVOSB | MBE | NaBOVA | VetHUB | SAM.gov Registered