DOMINUS GRAY, LLC

Securing Access to Opportunity

Monthly Security Posture Report

January 2026 — V-CISO Monthly Delivery

PREPARED FOR

Meridian Defense Systems, Inc.

January 2026

Document ID: DG-VCISO-RPT-2026-001

CONFIDENTIAL — DO NOT DISTRIBUTE

Service-Disabled Veteran-Owned Small Business

1. Executive Dashboard

This section provides a high-level summary of Meridian Defense Systems, Inc.'s security posture for January 2026. All metrics reflect the cumulative impact of V-CISO engagements, remediation activities, and ongoing monitoring throughout the reporting period.

OVERALL SECURITY SCORE	OPEN VULNERABILITIES	CMMC READINESS	ACTIVE INCIDENTS
72	47	68%	0
▲ +7 from last month (65)	▼ −36 from last month (83)	▲ +16% from last month (52%)	Clean month — no incidents

Monthly Assessment Summary

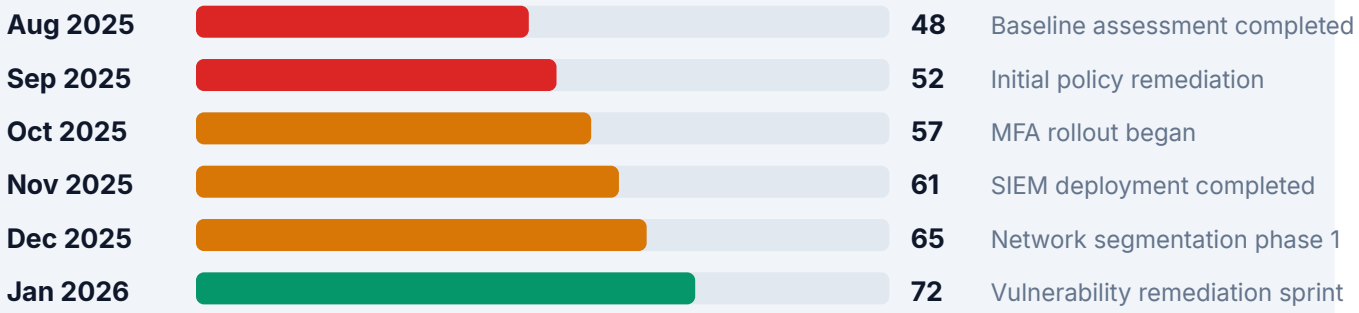
Meridian Defense Systems, Inc.'s security posture has improved significantly this month. The overall security score rose 7 points to 72/100, driven by aggressive vulnerability remediation (43% reduction in open vulnerabilities) and CMMC compliance initiatives. Zero security incidents were recorded, reflecting the

Zero Trust Architecture Progress

In alignment with DoD's FY2027 Zero Trust target, Meridian has completed initial ZTA assessment. Current adoption: Identity pillar — 60% (MFA deployed), Device pillar — 45% (endpoint verification in progress), Network pillar — 35% (micro-segmentation Phase 1 complete). Full ZTA roadmap targets 80% adoption by FY2027 deadline.

2. Security Score Trend — 6-Month View

SECURITY SCORE PROGRESSION

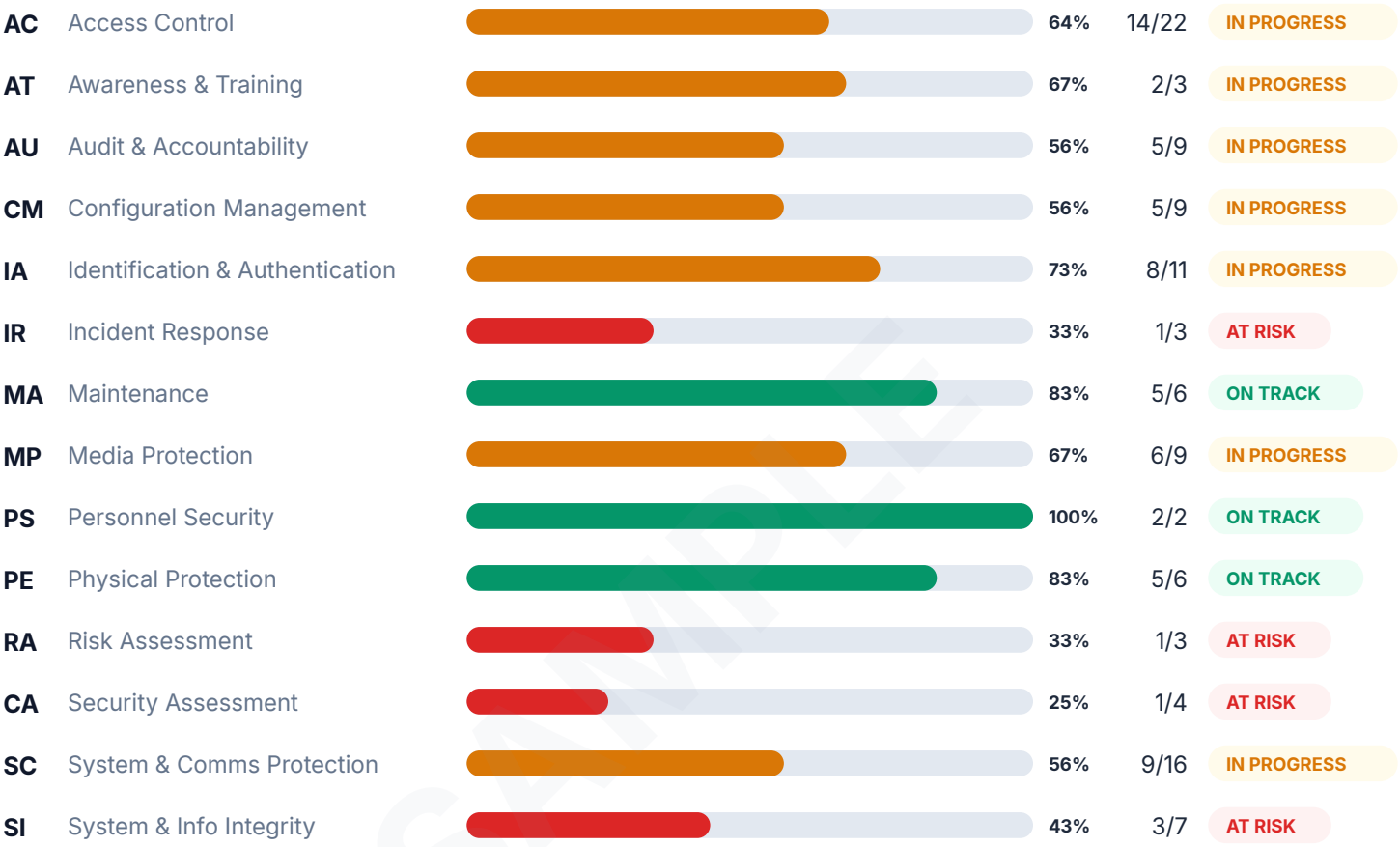


Trajectory Analysis

The security score has improved 24 points (+50%) since the V-CISO engagement began in August 2025. At the current rate of improvement, the organization is projected to reach the target score of 80 by April 2026 and 90+ by Q3 2026. The largest single-month gain occurred in January (+7 points), driven by the focused vulnerability remediation sprint.

3. CMMC Level 2 Compliance Progress

Progress against all 14 NIST SP 800-171 control families. Compliance percentages reflect controls fully implemented and validated. Target: 100% compliance prior to C3PAO assessment.



CMMC Progress Note

Overall CMMC readiness improved from 52% to 68% this month. Key gains include: MFA enforcement across all CUI systems (IA family +15%), SIEM deployment enabling centralized audit logging (AU family +12%), and updated baseline configurations for workstations (CM family +8%). Priority areas for February: Incident Response planning (IR at 33%) and Security Assessment program establishment (CA at 25%).

CMMC 2.0 Phase 2 Deadline: November 2026

Mandatory C3PAO assessments begin November 2026. Based on current remediation pace, Meridian is projected to be assessment-ready by August 2026. Recommend scheduling C3PAO engagement by Q2 2026 to secure assessment slots — demand is expected to significantly exceed C3PAO capacity.

4. Vulnerability Management Summary

Vulnerability metrics from the continuous scanning program. All CUI-processing systems are scanned weekly; general infrastructure is scanned monthly.

SEVERITY	OPEN	CLOSED THIS MONTH	NEW THIS MONTH	REMEDIATION SLA	SLA COMPLIANCE
CRITICAL	**3**	5	1	48 hours	MET
HIGH	**12**	18	4	7 days	MET
MEDIUM	**24**	14	6	30 days	PARTIAL
LOW	**8**	7	3	90 days	MET
TOTAL	**47**	**44**	**14**		

Vulnerability Trend

Net vulnerability count decreased by 30 this month (44 closed vs. 14 new discoveries). Critical vulnerabilities remain within SLA targets. The medium-severity SLA compliance is rated "Partial" due to 6 items approaching the 30-day deadline — remediation is scheduled for the first week of February. Zero vulnerabilities exceeded their remediation SLA this month.

5. Threat Landscape Briefing

Monthly intelligence briefing on threats relevant to the Defense Industrial Base (DIB) sector. Sources include CISA advisories, FBI IC3 reports, and commercial threat intelligence feeds.

CRITICAL

APT-41 / Wicked Panda — Active Campaign Targeting DIB

CISA Alert AA26-012A: Chinese state-sponsored group APT-41 observed conducting widespread exploitation of VPN appliances and edge devices in the defense sector. Tactics include credential harvesting via compromised supply chain software and lateral movement using living-off-the-land techniques. Recommendation: Verify all edge devices are patched to latest firmware; enable enhanced logging on VPN concentrators.

HIGH

Business Email Compromise — DoD Subcontractor Impersonation

FBI IC3 advisory: Increase in BEC attacks impersonating DoD prime contractors to redirect subcontractor payments. Attacks use compromised email accounts from legitimate .mil and .gov domains. Recommendation: Implement DMARC enforcement, require verbal confirmation for payment changes, add "external email" banners.

HIGH

Supply Chain Risk — SolarWinds-style Attacks on MSPs

Multiple managed service providers serving DIB clients have been compromised via trojanized RMM tool updates. Attackers used MSP access to pivot into defense contractor networks. Recommendation: Audit all third-party remote access tools; require MFA for vendor connections; review MSP security posture per NIST 800-171.

MEDIUM

Ransomware — LockBit 4.0 Targeting Manufacturing

LockBit 4.0 variant targeting manufacturing and defense companies with double-extortion tactics. Initial access through phishing emails with weaponized CAD file attachments. Recommendation: Block macro-enabled documents from external sources; ensure offline backup integrity; test incident response procedures.

6. Risk Register Summary — Top 5 Risks

Active risk register items ranked by composite risk score (Likelihood × Impact). Risk scores are reviewed monthly and updated based on remediation progress and threat intelligence.

#	RISK DESCRIPTION	LIKELIHOOD	IMPACT	SCORE	STATUS	OWNER
1	CUI boundary not segmented — unauthorized access to	4 / 5	5 / 5	**20**	HIGH	IT Director
2	Incomplete MFA coverage on CUI systems enables credential-based attacks	4 / 5	4 / 5	**16**	HIGH	CISO (V-CISO)
3	No incident response plan — unable to meet DoD 72-hr	3 / 5	5 / 5	**15**	MEDIUM	CISO (V-CISO)
4	Aging server infrastructure vulnerable to unpatched CVEs	3 / 5	4 / 5	**12**	MEDIUM	Sys Admin Lead
5	Third-party vendor access not governed by security	3 / 5	3 / 5	**9**	LOW	Procurement

Risk Movement This Month

Risk #1 (CUI Boundary) moved from Critical to High following completion of Phase 1 network segmentation. Risk #4 (Aging Infrastructure) was newly added after discovery of 3 end-of-life servers in the CUI environment during the January vulnerability scan. No risks were closed this month; 2 risks improved by one level.

7. Incident Summary

0 **Security Incidents**

No security incidents were reported or detected during the January 2026 reporting period. This represents the third consecutive month with zero incidents.

Monitoring Coverage

24/7 security monitoring is active across all CUI systems via the Dominus Gray managed SIEM platform.

- Endpoints monitored: 180 (100% coverage)
- Servers monitored: 12 of 12 (100% coverage)
- Network segments: 3 of 3 (100% coverage)
- Mean time to detect (MTTD): < 15 minutes
- Mean time to respond (MTTR): < 4 hours
- Alerts triaged this month: 342 (all false positives or informational)

8. Policy & Compliance Updates

Policy and compliance changes enacted during the January 2026 reporting period:

Updated: Remote Work & Telework Security Policy (v2.3)

Revised to include CUI-specific handling requirements for remote workers. New provisions: mandatory VPN with MFA, encrypted local storage only, prohibition on printing CUI at home offices, and quarterly remote workspace security verification. Effective February 1, 2026.

New: Third-Party Vendor Security Assessment Procedure

Established formal vendor security assessment process aligned with NIST 800-171 and CMMC requirements. All vendors with access to CUI or CUI systems must complete security questionnaire and provide evidence of adequate controls. Existing vendors to be assessed by March 31, 2026.

CMMC Certification Timeline Update

Based on current remediation progress, the revised C3PAO assessment timeline is Q3 2026. The Plan of Action & Milestones (POA&M) has been updated to reflect January progress. Conditional certification eligibility is projected for May 2026 (target SPRS score: 88+).

9. Key Accomplishments — January 2026

The following activities were completed by the Dominus Gray V-CISO team during the January reporting period:

- Completed vulnerability remediation sprint — closed 44 vulnerabilities including 5 critical items within 48-hour SLA
- Deployed multi-factor authentication (MFA) to remaining 23% of remote VPN users, achieving 100% MFA coverage on remote access
- Finalized and delivered Incident Response Plan (IRP) v1.0 including DCISE portal reporting procedures and CSIRT designation
- Conducted tabletop exercise simulating APT attack on CUI environment with IT team and executive leadership (12 participants)
- Completed Phase 1 network segmentation — CUI servers isolated into dedicated VLAN with firewall ACLs enforced
- Delivered CUI-specific security awareness training to all 247 employees (98% completion rate)

10. Next Month Priorities — February 2026

Planned activities for the February 2026 V-CISO engagement:

- Complete Phase 2 network segmentation — implement DMZ for external-facing CUI services and micro-segmentation within CUI enclave
- Deploy FIPS 140-2 validated cryptographic modules on VPN concentrators and endpoint encryption (BitLocker FIPS mode)
- Begin Security Assessment program — establish annual assessment cycle and schedule first internal penetration test
- Remediate remaining 6 medium-severity vulnerabilities approaching SLA deadline from January scan
- Conduct vendor security assessment for top 5 third-party providers with CUI access
- Begin Rev 3 gap analysis in Q3 2026 to prepare for eventual DoD transition from Rev 2

11. Recommendations for Leadership

The following strategic recommendations require executive awareness and/or approval. Each recommendation includes a business justification aligned with organizational objectives.

Recommendation 1

HIGH PRIORITY

Approve Budget for SIEM Platform Upgrade ($85,000)

The current SIEM deployment handles basic log aggregation but lacks advanced correlation, behavioral analytics, and automated response capabilities. Upgrading to an enterprise SIEM platform (Microsoft Sentinel or Splunk Enterprise) will enable compliance with CMMC audit & accountability requirements, reduce mean time to detect from 15 minutes to under 5 minutes, and provide the forensic capabilities needed for DoD incident reporting.

Business Justification

Required for CMMC Level 2 certification. Reduces incident response costs by an estimated 60%. Enables detection of advanced persistent threats targeting CUI. ROI: Protection of $4.2M annual DoD contract revenue.

Recommendation 2

MEDIUM PRIORITY

Authorize Hiring of Dedicated Security Analyst (FTE)

As the security program matures, daily operational security tasks are exceeding the capacity of the current IT team. A dedicated security analyst would manage vulnerability scanning, SIEM monitoring, incident triage, and compliance documentation. This role bridges the gap between the strategic V-CISO function and day-to-day security operations.

Business Justification

Sustains security improvements between monthly V-CISO engagements. Estimated salary: $75,000–$95,000. Alternative: Managed Security Operations Center (MSOC) at $8,000–$12,000/month. Dominus Gray can assist with recruitment and onboarding.

Recommendation 3

MEDIUM PRIORITY

Schedule Board-Level Cybersecurity Briefing (Q1 2026)

CMMC 2.0 requires demonstrated executive oversight of the cybersecurity program. A quarterly board-level briefing establishes the governance structure needed for certification and ensures leadership is informed of cyber risks to DoD contract performance. Dominus Gray will prepare the briefing materials and present alongside internal leadership.

Business Justification

CMMC governance requirement (CA.L2-3.12.1). Demonstrates due diligence to DoD prime contractors. Positions the organization favorably during C3PAO assessment. No additional cost — included in V-CISO engagement.

DOMINUS GRAY, LLC

Securing Access to Opportunity

Virtual CISO Services | CMMC Compliance | Cybersecurity Consulting
Vulnerability Management | Incident Response | Security Program Development

Contact
Odie Gray, CEO & Managing Principal
odie.gray@dominusgray.com
dominusgray.com
Houston, TX

SDVOSB | MBE | NaVOBA | VetHUB | SAM.gov Registered
Service-Disabled Veteran-Owned Small Business