DOMINUS GRAY, LLC

Securing Access to Opportunity

Plan of Action & Milestones — CMMC Level 2

NIST SP 800-171 Rev 2 Remediation Tracking

PREPARED FOR

Meridian Defense Systems, Inc.

February 2026

Document ID: DG-POAM-2026-001

CONFIDENTIAL — DO NOT DISTRIBUTE

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

CMMC 2.0 POA&M Rules & Requirements

⚠ CRITICAL: CMMC 2.0 POA&M Restrictions

Under CMMC 2.0, Plans of Action & Milestones are subject to strict limitations. Understanding these rules is essential for achieving and maintaining conditional certification status. Non-compliance with these rules will result in denial of conditional certification.

Minimum 88/110 SPRS Score Required

To qualify for conditional certification, the organization must achieve a minimum Supplier Performance Risk System (SPRS) score of 88 out of 110. Controls not yet fully implemented must be documented in the POA&M with specific remediation plans and milestones.

POA&Ms Only Allowed for 1-Point Controls

Only security requirements with a point value of 1 (one) are eligible for POA&M under conditional certification. These are typically lower-risk requirements where partial implementation provides some level of protection.

3-Point and 5-Point Controls MUST Be Fully Met

All security requirements with point values of 3 or 5 MUST be fully implemented before the C3PAO assessment. These high-impact controls cannot be placed on POA&M for conditional certification. Failure to meet any 3-point or 5-point control will result in assessment failure.

180-Day Maximum Remediation Window

All POA&M items must be fully remediated within 180 calendar days of the conditional certification date. Extensions are not permitted. Failure to close all POA&M items within the 180-day window will result in revocation of conditional certification status.

This document contains confidential and proprietary information.

Annual Affirmation Required

Organizations must provide an annual affirmation to the CMMC Accreditation Body (the Cyber AB) confirming continued compliance with all CMMC Level 2 requirements. This includes confirmation that all POA&M items have been closed and no new deficiencies have been identified.

⚠ FALSE CLAIMS ACT ENFORCEMENT

The DOJ Civil Cyber-Fraud Initiative holds contractors accountable for knowingly misrepresenting cybersecurity compliance. Inaccurate SPRS scores, falsified POA&M status, or unreported security gaps can result in treble damages, per-claim penalties, and debarment. In February 2025, a defense contractor paid $11.3M to settle FCA allegations. Ensure all POA&M entries accurately reflect current remediation status and maintain documented evidence of progress.

CMMC 2.0 Phased Rollout Timeline

Phase 1 (Nov 2025): Self-assessments begin; select C3PAO assessments for critical programs
Phase 2 (Nov 2026): Mandatory C3PAO assessments for all Level 2 contractors — CRITICAL DEADLINE
Phase 3 (Nov 2027): Level 3 (Expert) requirements begin for highest-sensitivity contracts
Phase 4 (Nov 2028): Universal compliance required across all DoD contracts containing CUI

POA&M Entry Template

Each POA&M entry must contain the following fields. Complete all fields for every identified weakness. Ensure entries are reviewed and updated monthly.

FIELD	DESCRIPTION
POA&M ID	Unique identifier for the POA&M entry (e.g., POAM-2026-001)
Control Reference	NIST SP 800-171 control identifier (e.g., AC.L2-3.1.12)
Control Title	Descriptive name of the security requirement
Weakness Description	Detailed description of the identified deficiency or gap

Risk Level	Risk rating: Critical, High, Medium, or Low
Point Value	SPRS point value: 1, 3, or 5 (only 1-point controls eligible for POA&M)
Remediation Plan	Specific steps to fully implement the control and close the weakness
Milestones & Target Dates	Measurable milestones with specific completion dates (within 180 days)
Responsible Party	Individual or role accountable for remediation
Resources Required	Budget, personnel, tools, and other resources needed
Interim Risk Mitigation	Temporary measures in place while full remediation is in progress
Status	Current status: Open | In Progress | Closed | Overdue
Evidence of Completion	Documentation proving the control has been fully implemented

Sample POA&M Entries

POAM-2026-001 — AC.L2-3.1.12: Remote Access Control

ELIGIBLE FOR POA&M

POA&M ID	POAM-2026-001
Control Reference	AC.L2-3.1.12
Control Title	Remote Access Control
Point Value	1 point — Eligible for conditional POA&M
Weakness Description	VPN access lacks MFA enforcement for 23% of remote users. Split tunneling remains enabled on some endpoints, creating potential for CUI exposure via unmonitored network paths.
Risk Level	Medium
Remediation Plan	Deploy MFA tokens to remaining remote users. Update VPN client configuration to disable split tunneling. Implement always-on VPN policy for CUI-accessing endpoints.
Responsible Party	Network Engineer
Resources Required	MFA hardware tokens ($2,400), VPN configuration effort (40 hrs)
Interim Risk Mitigation	Enhanced monitoring of VPN connections from non-MFA users. Restricted CUI access for split-tunnel endpoints.
Status	In Progress
Evidence of Completion	[To be documented upon completion]

Milestones & Target Dates

#	MILESTONE DESCRIPTION	TARGET DATE
1	[illegible] MFA tokens to remaining users	[illegible]
2	Update VPN client configurations (disable split tunneling)	April 1, 2026
3	Implement always-on VPN policy and validate enforcement	April 30, 2026

This document contains confidential and proprietary information.

POAM-2026-002 — AT.L2-3.2.1: Role-Based Risk Awareness

ELIGIBLE FOR POA&M

POA&M ID	POAM-2026-002
Control Reference	AT.L2-3.2.1
Control Title	Role-Based Risk Awareness
Point Value	1 point — Eligible for conditional POA&M
Weakness Description	Annual security training program exists but lacks CUI-specific handling modules. No role-based training tracks for system administrators, privileged users, or CUI data handlers.
Risk Level	Medium
Remediation Plan	Develop CUI-specific training content. Create role-based training tracks for administrators, privileged users, and general users. Implement quarterly phishing simulations.
Responsible Party	ISSO
Resources Required	LMS subscription upgrade ($3,600/yr), CUI training content development (60 hrs)
Interim Risk Mitigation	Supplemental CUI handling briefings provided to all personnel with CUI access. Email reminders on CUI marking requirements.
Status	Open
Evidence of Completion	[To be documented upon completion]

Milestones & Target Dates

#	MILESTONE DESCRIPTION	TARGET DATE
[illegible]	Develop CUI-specific training module content	[illegible]
2	Create role-based training tracks in LMS	March 30, 2026
3	Complete initial training rollout to all personnel	May 1, 2026

This document contains confidential and proprietary information.

POAM-2026-003 — PE.L2-3.10.6: Alternate Work Site Safeguards

ELIGIBLE FOR POA&M

POA&M ID	POAM-2026-003
Control Reference	PE.L2-3.10.6
Control Title	Alternate Work Site Safeguards
Point Value	1 point — Eligible for conditional POA&M
Weakness Description	Remote work policy exists but lacks specific CUI handling procedures for home offices. No technical controls to validate remote work environment security posture.
Risk Level	Low
Remediation Plan	Update remote work policy with CUI-specific requirements. Require encrypted drives and screen privacy filters for remote CUI access. Implement remote work security attestation process.
Responsible Party	ISSO
Resources Required	Privacy filters ($1,200), Policy development effort (20 hrs)
Interim Risk Mitigation	Remote workers verbally briefed on CUI handling expectations. Full-disk encryption verified on all remote endpoints.
Status	Open
Evidence of Completion	[To be documented upon completion]

Milestones & Target Dates

#	MILESTONE DESCRIPTION	TARGET DATE
1	Update remote work policy with CUI requirements	March 15, 2026
2	Procure privacy filters and distribute to remote workers	April 1, 2026
3	Implement annual remote work security attestation process	May 15, 2026

This document contains confidential and proprietary information.

POAM-2026-004 — IR.L2-3.6.1: Incident Handling Capability

MUST CLOSE BEFORE ASSESSMENT

POA&M ID	POAM-2026-004
Control Reference	IR.L2-3.6.1
Control Title	Incident Handling Capability
Point Value	3 points — NOT eligible for POA&M — must be fully met
Weakness Description	No documented incident response plan covering CUI incidents. No designated CSIRT. DCISE Portal reporting procedures not established. Incident handling is ad hoc with no defined roles, escalation paths, or playbooks.
Risk Level	High
Remediation Plan	Develop comprehensive IRP covering detection, analysis, containment, eradication, and recovery. Establish DCISE Portal reporting procedures. Designate and train CSIRT members.
Responsible Party	ISSO / ISSM
Resources Required	IRP development consulting ($8,000), Tabletop exercise facilitation ($3,500)
Interim Risk Mitigation	N/A — This is a 3-point control. MUST be fully implemented before C3PAO assessment. Cannot be placed on POA&M for conditional certification.
Status	In Progress
Evidence of Completion	[To be documented upon completion]

Milestones & Target Dates

#	MILESTONE DESCRIPTION	TARGET DATE
1	Draft incident response plan and DCISE Portal reporting procedures	February 28, 2026
2	Designate CSIRT members and conduct initial training	March 15, 2026
3	Conduct tabletop exercise to validate IRP	April 15, 2026

This document contains confidential and proprietary information.

POAM-2026-005 — RA.L2-3.11.2: Vulnerability Scanning

MUST CLOSE BEFORE ASSESSMENT

POA&M ID	POAM-2026-005
Control Reference	RA.L2-3.11.2
Control Title	Vulnerability Scanning
Point Value	3 points — NOT eligible for POA&M — must be fully met
Weakness Description	No regular vulnerability scanning program. Last scan was 14 months ago. No remediation SLAs defined. No process to prioritize vulnerabilities by risk to CUI environment.
Risk Level	High
Remediation Plan	Implement monthly vulnerability scanning program. Define remediation SLAs aligned with risk levels. Deploy automated scanning tool with dashboard reporting.
Responsible Party	System Administrator
Resources Required	Vulnerability scanning license ($12,000/yr), Remediation labor (ongoing)
Interim Risk Mitigation	N/A — This is a 3-point control. MUST be fully implemented before C3PAO assessment. Cannot be placed on POA&M for conditional certification.
Status	Open
Evidence of Completion	[To be documented upon completion]

Milestones & Target Dates

#	MILESTONE DESCRIPTION	TARGET DATE
[illegible]	[illegible] deploy vulnerability scanning tool (Tenable/Qualys)	[illegible]
2	Establish scanning schedule and remediation SLAs	March 15, 2026
3	Complete first full scan cycle with remediation tracking	April 30, 2026

POA&M Tracking Summary

TOTAL ITEMS	OPEN	IN PROGRESS	CLOSED	OVERDUE
5	3	2	0	0
Active POA&M entries	Not yet started	Actively remediating	Fully remediated	Past target date

Summary by Risk Level

	COUNT	POINT IMPACT	POA&M ELIGIBLE	NOTES
CRITICAL	0	0	No	All critical items must be resolved before assessment

HIGH	2	6	Varies	Only 1-point high-risk items eligible for POA&M
MEDIUM	2	2	Yes (1-pt)	Remediate within 180-day window
LOW	1	1	Yes (1-pt)	Remediate within 180-day window

Timeline Summary

POA&M ID	CONTROL	FINAL MILESTONE	DAYS REMAINING	
POAM-2026-001	AC.L2-3.1.12	April 30, 2026	[Calculate]	In Progress
POAM-2026-002	AT.L2-3.2.1	May 1, 2026	[Calculate]	Open
POAM-2026-003	PE.L2-3.10.6	May 15, 2026	[Calculate]	Open
POAM-2026-004	IR.L2-3.6.1	April 15, 2026	[Calculate]	NOT MET
POAM-2026-005	RA.L2-3.11.2	April 30, 2026	[Calculate]	NOT MET

POA&M Closure Requirements

To close a POA&M item, the following must be completed:
1. All milestones achieved and documented
2. Control fully implemented and operational
3. Evidence collected and stored in evidence repository
4. ISSO validation of control effectiveness
5. ISSM approval of closure

Monthly Review Log

Document each monthly POA&M review meeting. All POA&M items must be reviewed at least monthly to track remediation progress, identify blockers, and update milestones. Maintain this log as evidence of ongoing POA&M management.

Review #1 — March 2026

Review Date: [Enter Date]	**Attendees:** [Enter Names]
Items Reviewed: [Enter Count]	**Items Closed:** [Enter Count]
Items Added: [Enter Count]	**Blockers Identified:** [Enter Description]

Notes / Decisions: [Enter meeting notes, decisions, and action items]

Review #2 — April 2026

Review Date: [Enter Date]

Items Reviewed: [Enter Count]

Items Added: [Enter Count]

Attendees:[Enter Names]

Items Closed:[Enter Count]

Blockers Identified: [Enter Description]

Review #3 — May 2026

Review Date: [Enter Date]

Items Reviewed: [Enter Count]

Items Added: [Enter Count]

Attendees:[Enter Names]

Items Closed:[Enter Count]

Blockers Identified: [Enter Description]

Review #4 — June 2026

Review Date: [Enter Date]

Items Reviewed: [Enter Count]

Items Added: [Enter Count]

Attendees:[Enter Names]

Items Closed:[Enter Count]

Blockers Identified: [Enter Description]

Review #5 — July 2026

Review Date: [Enter Date]

Items Reviewed: [Enter Count]

Items Added: [Enter Count]

Attendees:[Enter Names]

Items Closed:[Enter Count]

Blockers Identified: [Enter Description]

Review #6 — August 2026

Review Date: [Enter Date]

Items Reviewed: [Enter Count]

Items Added: [Enter Count]

Attendees:[Enter Names]

Items Closed:[Enter Count]

Blockers Identified: [Enter Description]

Notes / Decisions:[Enter meeting notes, decisions, and action items]