DOMINUS GRAY, LLC

Securing Access to Opportunity

System Security Plan — CMMC Level 2

NIST SP 800-171 Rev 2 Compliance

PREPARED FOR

Meridian Defense Systems, Inc.

February 2026

Document ID: DG-SSP-2026-001

CONFIDENTIAL — DO NOT DISTRIBUTE

Service-Disabled Veteran-Owned Small Business

Table of Contents

1. Document Control

FIELD	VALUE
Document Title	System Security Plan — CMMC Level 2
Document ID	DG-SSP-2026-001
Version	1.0 — Initial Draft
Classification	CUI // SP-SSP

Author	Dominus Gray, LLC
Prepared For	Meridian Defense Systems, Inc.
Date Created	February 9, 2026
Last Reviewed	[Enter Review Date]
Next Review Date	[Enter Next Review Date]
Approving Authority	[Enter Authorizing Official Name & Title]
Distribution	Authorized Personnel Only

Revision History

VERSION	DATE	AUTHOR	DESCRIPTION
[1.1]	[Date]	[Author]	[Description of changes]
[1.2]	[Date]	[Author]	[Description of changes]

Distribution & Handling Notice

This document contains Controlled Unclassified Information (CUI) and is intended solely for authorized personnel of Meridian Defense Systems, Inc.. Distribution, reproduction, or disclosure to unauthorized parties is prohibited. Handle, store, transmit, and destroy in accordance with CUI marking requirements and NIST SP 800-171.

2. System Identification

FIELD	VALUE
System Name	[Enter System Name, e.g., Meridian CUI Enclave]
System Abbreviation	[Enter Abbreviation, e.g., MCE]
System Description	Information system used by Meridian Defense Systems, Inc. to process, store, and transmit Controlled Unclassified Information (CUI) in support of Department of Defense (DoD) contract requirements.
Operational Status	☐ Operational ☐ Under Development ☐ Major Modification

System Type	☐ Major Application ☐ General Support System ☐ Hybrid
Responsible Organization	Meridian Defense Systems, Inc.
CAGE Code	[Enter CAGE Code]
DUNS Number	[Enter DUNS/UEI Number]
Authorization Boundary	The authorization boundary encompasses all hardware, software, firmware, network components, and personnel that process, store, or transmit CUI. See Appendix A for network diagram.
System Location (Primary)	[Enter Primary Facility Address]
System Location (Alternate)	[Enter Alternate Facility Address(es)]
Information Types	CUI // CTI (Controlled Technical Information), CUI // ITAR, CUI // PROPIN

3. System Environment

3.1 Hardware Inventory

Document all hardware components within the authorization boundary that process, store, or transmit CUI.

ASSET ID	DEVICE TYPE	MANUFACTURER / MODEL	SERIAL NUMBER	LOCATION	CUI PROCESSING
HW-002	Workstation	[Manufacturer / Model]	[Serial #]	[Location]	☐ Yes ☐ No
HW-003	Network Device	[Manufacturer / Model]	[Serial #]	[Location]	☐ Yes ☐ No
HW-004	Mobile Device	[Manufacturer / Model]	[Serial #]	[Location]	☐ Yes ☐ No
[Add rows]					

3.2 Software Inventory

Document all software installed on systems within the authorization boundary.

SOFTWARE ID	SOFTWARE NAME	VERSION	VENDOR	PURPOSE	CUI PROCESSING
SW-002	[Database Software]	[Version]	[Vendor]	Data Storage	☐ Yes ☐ No
SW-003	[Endpoint Protection]	[Version]	[Vendor]	Security	☐ Yes ☐ No
SW-004	[Email Client]	[Version]	[Vendor]	Communication	☐ Yes ☐ No

[Add rows]

3.3 Network Architecture

Network Architecture Description

[Insert description of the network architecture supporting the CUI environment. Include:
• Network topology overview (DMZ, internal segments, CUI enclave)
• IP addressing scheme (generalized)
• Key network security devices (firewalls, IDS/IPS, proxies)
• Wireless network configuration and segmentation

Cloud Service Provider Requirements

Per DFARS 252.204-7012, any cloud service provider (CSP) processing, storing, or transmitting CUI must hold FedRAMP Moderate authorization or demonstrate equivalent security. Verify CSP authorization status at marketplace.fedramp.gov. Document CSP security posture in this SSP, including shared responsibility model and data residency requirements. A December 2023 DoD memo clarified that 'equivalency' claims require formal documentation and may be challenged during C3PAO assessment.

4. System Interconnections

Document all connections between this system and external information systems. Each interconnection must be authorized, documented, and monitored.

CONNECTION ID	EXTERNAL SYSTEM	ORGANIZATION	CONNECTION TYPE	DATA EXCHANGED	AUTHORIZATION
IC-002	[Cloud Service]	[CSP Name]	TLS 1.2+	CUI / Non-CUI	☐ ISA/MOU Signed
IC-003	[DoD System]	Department of Defense	Encrypted	CUI / CTI	☐ ISA/MOU Signed
[Add rows]					

Interconnection Security Agreement (ISA) Requirements

All system interconnections that transmit CUI must be covered by an Interconnection Security Agreement (ISA) or Memorandum of Understanding (MOU). Each agreement must specify:

- Security controls applied to the connection
- Data types authorized for transmission
- Points of contact for both organizations
- Incident reporting procedures
- Annual review and reauthorization requirements

5. CUI Description

5.1 Types of CUI Processed

Identify all categories of CUI processed, stored, or transmitted by this system.

CUI CATEGORY	CUI MARKING	APPLICABLE REGULATION	HANDLING
Export Controlled (ITAR)	CUI // SP-EXPT	ITAR 22 CFR 120-130	Specified
Proprietary Business Info	CUI // SP-PROPIN	FAR 52.215-1(e)	Basic
[Add categories as applicable]			

5.2 CUI Marking Requirements

- All CUI documents must include the CUI designation indicator in the header/banner
- CUI markings must include the category marking (e.g., CUI // SP-CTI)
- Limited dissemination controls must be applied where applicable
- Electronic files must include CUI metadata tagging where technically feasible
- Printed CUI must include markings on each page, front and back

5.3 CUI Data Flow

CUI Data Flow Description

[Insert description of how CUI flows through the system. Include:
• CUI ingestion points (email, file transfer, web portal, physical media)
• Processing and storage locations within the authorization boundary
• CUI transmission paths (internal and external)
• CUI egress points and controls

6. Security Control Implementation

Refer to Appendix B for the detailed CUI data flow diagram.]

NIST SP 800-171 Rev 2 — 110 Security Requirements

This section documents the implementation status of security controls organized by the 14 control families defined in NIST SP 800-171 Rev 2. For each family, representative controls are shown with full implementation details. The complete control-by-control assessment is maintained in the SSP Workbook (Excel companion document). This SSP template provides the narrative framework required for CMMC Level 2 certification.

6.1 Access Control (AC)

Limit system access to authorized users, processes, and devices, and limit the types of transactions and functions that authorized users are permitted to execute.

AC.L2-3.1.1	Authorized Access Control	MET
Requirement	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	AC-001	

AC.L2-3.1.2	Transaction & Function Control	MET
Requirement	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	AC-002	

AC.L2-3.1.3	CUI Flow Enforcement	NOT MET
Requirement	Control the flow of CUI in accordance with approved authorizations.	
Implementation Status	Not Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	Network Engineer	
Evidence Reference	AC-003	

AC.L2-3.1.5	Least Privilege	PARTIAL
Requirement	Employ the principle of least privilege, including for specific security functions and privileged accounts.	
Implementation Status	Partial	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	AC-005	

> Additional AC controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

6.2 Awareness & Training (AT)

Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

AT.L2-3.2.1	Role-Based Risk Awareness	PARTIAL
Requirement	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
Implementation Status	Partial	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	ISSO	
Evidence Reference	AT-001	

AT.L2-3.2.2	Role-Based Training	MET
Requirement	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	ISSO	
Evidence Reference	AT-002	

AT.L2-3.2.3	Insider Threat Awareness	MET
Requirement	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	ISSO	
Evidence Reference	AT-003	

> Additional AT controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

6.3 Audit & Accountability (AU)

Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

AU.L2-3.3.1	System Auditing	NOT MET
Requirement	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	
Implementation Status	Not Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	AU-001	

AU.L2-3.3.2	User Accountability	MET
Requirement	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	AU-002	

AU.L2-3.3.5	Audit Correlation	NOT MET
Requirement	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	
Implementation Status	Not Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	SOC Analyst	
Evidence Reference	AU-005	

> Additional AU controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

6.4 Configuration Management (CM)

Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

CM.L2-3.4.1	System Baselining	PARTIAL
Requirement	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
Implementation Status	Partial	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	CM-001	

CM.L2-3.4.2	Security Configuration Enforcement	MET
Requirement	Establish and enforce security configuration settings for information technology products employed in organizational systems.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	CM-002	

CM.L2-3.4.6	Least Functionality	NOT MET
Requirement	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	
Implementation Status	Not Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	CM-006	

> Additional CM controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

6.5 Identification & Authentication (IA)

Identify system users, processes acting on behalf of users, and devices. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

IA.L2-3.5.1	Identification	MET
Requirement	Identify information system users, processes acting on behalf of users, or devices.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	IA-001	

IA.L2-3.5.2	Authentication	MET
Requirement	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	IA-002	

IA.L2-3.5.3	Multi-Factor Authentication	PARTIAL
Requirement	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	
Implementation Status	Partial	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	IA-003	

IA.L2-3.5.4	Replay-Resistant Authentication	MET
Requirement	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	IA-004	

> Additional IA controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

6.6 Incident Response (IR)

Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

IR.L2-3.6.1	Incident Handling	NOT MET
Requirement	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
Implementation Status	Not Met
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]
Responsible Party	ISSO
Evidence Reference	IR-001

IR.L2-3.6.2	Incident Reporting	PARTIAL
Requirement	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
Implementation Status	Partial
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]
Responsible Party	ISSO
Evidence Reference	IR-002

IR.L2-3.6.3	Incident Response Testing	NOT MET
Requirement	Test the organizational incident response capability.
Implementation Status	Not Met
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]
Responsible Party	ISSO
Evidence Reference	IR-003

> Additional IR controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

6.7 Maintenance (MA)

Perform maintenance on organizational systems. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

MA.L2-3.7.1	System Maintenance	MET
Requirement	Perform maintenance on organizational information systems.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	MA-001	

MA.L2-3.7.2	Maintenance Tool Control	MET
Requirement	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	MA-002	

MA.L2-3.7.5	Nonlocal Maintenance	PARTIAL
Requirement	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	
Implementation Status	Partial	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	MA-005	

> Additional MA controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

6.8 Media Protection (MP)

Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. Limit access to CUI on system media to authorized users. Sanitize or destroy system media containing CUI before disposal or release for reuse.

MP.L2-3.8.1	Media Protection	MET
Requirement	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	ISSO	
Evidence Reference	MP-001	

MP.L2-3.8.3	Media Sanitization	MET
Requirement	Sanitize or destroy information system media containing CUI before disposal or release for reuse.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	MP-003	

MP.L2-3.8.9	CUI Backup Protection	NOT MET
Requirement	Protect the confidentiality of backup CUI at storage locations.	
Implementation Status	Not Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	MP-009	

> Additional MP controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

6.9 Personnel Security (PS)

Screen individuals prior to authorizing access to organizational systems containing CUI. Ensure that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

PS.L2-3.9.1	Personnel Screening	MET
Requirement	Screen individuals prior to authorizing access to organizational systems containing CUI.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	HR Manager	
Evidence Reference	PS-001	

PS.L2-3.9.2	Personnel Actions	MET
Requirement	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	HR Manager	
Evidence Reference	PS-002	

> Additional PS controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

6.10 Physical Protection (PE)

Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. Protect and monitor the physical facility and support infrastructure for organizational systems.

PE.L2-3.10.1	Physical Access Limitation	MET
Requirement	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	Facility Manager	
Evidence Reference	PE-001	

PE.L2-3.10.2	Physical Access Monitoring	MET
Requirement	Protect and monitor the physical facility and support infrastructure for organizational information systems.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	Facility Manager	
Evidence Reference	PE-002	

PE.L2-3.10.6	Alternate Work Site	PARTIAL
Requirement	Enforce safeguarding measures for CUI at alternate work sites.	
Implementation Status	Partial	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	ISSO	
Evidence Reference	PE-006	

> Additional PE controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

6.11 Risk Assessment (RA)

Periodically assess the risk to organizational operations, organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

RA.L2-3.11.1	Risk Assessment	MET
Requirement	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	ISSO	
Evidence Reference	RA-001	

RA.L2-3.11.2	Vulnerability Scanning	NOT MET
Requirement	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	
Implementation Status	Not Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	RA-002	

RA.L2-3.11.3	Vulnerability Remediation	PARTIAL
Requirement	Remediate vulnerabilities in accordance with risk assessments.	
Implementation Status	Partial	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	RA-003	

> Additional RA controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

6.12 Security Assessment (CA)

Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

CA.L2-3.12.1	Security Control Assessment	NOT MET
Requirement	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	
Implementation Status	Not Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	ISSO	
Evidence Reference	CA-001	

CA.L2-3.12.2	Plan of Action	PARTIAL
Requirement	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	
Implementation Status	Partial	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	ISSO	
Evidence Reference	CA-002	

CA.L2-3.12.3	Continuous Monitoring	NOT MET
Requirement	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	
Implementation Status	Not Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	ISSO	
Evidence Reference	CA-003	

CA.L2-3.12.4	System Security Plans	PARTIAL
Requirement	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	
Implementation Status	Partial	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	ISSM	
Evidence Reference	CA-004	

> Additional CA controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

6.13 System & Communications Protection (SC)

Monitor, control, and protect communications at the external boundaries and key internal boundaries of organizational systems. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security.

SC.L2-3.13.1	Boundary Protection	NOT MET
Requirement	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	
Implementation Status	Not Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	Network Engineer	
Evidence Reference	SC-001	

SC.L2-3.13.8	CUI Transmission Encryption	PARTIAL
Requirement	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	
Implementation Status	Partial	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	Network Engineer	
Evidence Reference	SC-008	

SC.L2-3.13.11	FIPS-Validated Cryptography	NOT MET
Requirement	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	
Implementation Status	Not Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	SC-011	

SC.L2-3.13.16	Data at Rest Encryption	MET
Requirement	Protect the confidentiality of CUI at rest.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	SC-016	

> Additional SC controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

6.14 System & Information Integrity (SI)

Identify, report, and correct information and system flaws in a timely manner. Provide protection from malicious code at appropriate locations within organizational systems. Monitor system security alerts and advisories and take action in response.

SI.L2-3.14.1	Flaw Remediation	NOT MET
Requirement	Identify, report, and correct information and information system flaws in a timely manner.	
Implementation Status	Not Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	SI-001	

SI.L2-3.14.2	Malicious Code Protection	MET
Requirement	Provide protection from malicious code at appropriate locations within organizational information systems.	
Implementation Status	Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	System Administrator	
Evidence Reference	SI-002	

SI.L2-3.14.3	Security Alerts & Advisories	PARTIAL
Requirement	Monitor system security alerts and advisories and take action in response.	
Implementation Status	Partial	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	SOC Analyst	
Evidence Reference	SI-003	

SI.L2-3.14.6	Security Alert Monitoring	NOT MET
Requirement	Monitor organizational information systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	
Implementation Status	Not Met	
Implementation Description	[Describe how this control is implemented within the authorization boundary. Include specific technologies, processes, and procedures used.]	
Responsible Party	SOC Analyst	
Evidence Reference	SI-006	

> Additional SI controls documented in full SSP workbook. Contact Dominus Gray for the complete control-by-control assessment template.

7. Personnel Roles & Responsibilities

Information System Security Manager (ISSM)

Name: [Enter Name]
Email: [Enter Email]
Phone: [Enter Phone]

Key Responsibilities:

- Oversee the organization-wide information security program
- Approve and sign the System Security Plan
- Ensure compliance with CMMC Level 2 requirements
- Authorize system interconnections and changes to the security posture
- Report security posture to senior leadership and authorizing officials

Information System Security Officer (ISSO)

Name: [Enter Name]
Email: [Enter Email]
Phone: [Enter Phone]

Key Responsibilities:

- Maintain the System Security Plan and supporting documentation

- Conduct ongoing security monitoring and assessment activities
- Manage POA&M items and track remediation progress
- Coordinate incident response activities and DCISE Portal reporting
- Manage security awareness training program
- Serve as primary liaison with C3PAO during certification assessments

System Administrator

Name: [Enter Name]
Email: [Enter Email]
Phone: [Enter Phone]

Key Responsibilities:

- Implement and maintain technical security controls
- Manage user accounts, access controls, and authentication mechanisms
- Perform system patching, updates, and configuration management
- Monitor system audit logs and investigate anomalies
- Execute backup and recovery procedures
- Maintain hardware and software inventories

Authorized Users

Name: All authorized personnel
Email: N/A
Phone: N/A

Key Responsibilities:

- Complete required security awareness training before accessing CUI
- Comply with all CUI handling, marking, and dissemination requirements
- Report suspected security incidents immediately to the ISSO
- Use only authorized devices and software to access CUI
- Protect authentication credentials and never share passwords
- Follow clean desk and screen lock policies

8. Security Assessment Schedule

The following assessment activities are conducted on a recurring basis to maintain compliance with CMMC Level 2 requirements and ensure ongoing effectiveness of security controls.

ASSESSMENT ACTIVITY	FREQUENCY	RESPONSIBLE PARTY	DESCRIPTION
Access Control Review	Quarterly	ISSO	Review user access rights, privileged accounts, and terminated employee access
Security Awareness Training	Annual	ISSO	CUI handling training with role-based modules and completion
Penetration Testing	Annual	Third Party	External penetration test of CUI boundary with remediation

Incident Response Exercise	Annual	ISSO / CSIRT	Tabletop exercise or functional drill of incident response plan
SSP Review & Update	Annual	ISSM	Comprehensive review and update of this System Security Plan
POA&M Review	Monthly	ISSO	Track remediation progress, update milestones, close
Configuration Audit	Quarterly	System Admin	Validate system configurations against approved baselines
Physical Security Inspection	Semi-Annual	Facility Manager	Inspect physical controls protecting CUI processing
Backup & Recovery Test	Quarterly	System Admin	Test backup restoration procedures for CUI systems
CMMC Self-Assessment	Annual	ISSO / ISSM	NIST SP 800-171A-based self-assessment with SPRS score
CMMC C3PAO Assessment	Triennial	C3PAO	Formal CMMC Level 2 certification assessment

8.1 Continuous Monitoring Strategy

This section documents the organization's approach to ongoing security monitoring per NIST SP 800-137. Continuous monitoring ensures that security controls remain effective and that the organization maintains its CMMC Level 2 compliance posture over time.

Automated Vulnerability Scanning

Define the frequency and scope of automated vulnerability scanning across all CUI systems. Include network-based and agent-based scanning, web application scanning, and database vulnerability assessments. Document remediation SLAs by severity level.

SIEM / Log Aggregation

Document the Security Information and Event Management (SIEM) solution used to aggregate, correlate, and analyze security logs from all systems within the authorization boundary. Include log sources, retention periods, alerting rules, and escalation procedures.

Configuration Monitoring

Describe the tools and processes used to monitor system configurations against approved baselines. Include change detection mechanisms, drift remediation procedures, and configuration audit frequency.

SPRS Score Maintenance

Document the process for maintaining and updating the Supplier Performance Risk System (SPRS) score. Include the frequency of self-assessments, the process for updating scores when controls change status, and the responsible party for SPRS submissions.

Annual Affirmation Requirement

CMMC requires annual affirmation of continued compliance. Organizations must submit an annual affirmation to the Cyber AB confirming that all CMMC Level 2 requirements continue to be met, all POA&M items have been closed, and no material changes have degraded the security posture. Failure to submit the annual affirmation will result in lapse of certification status.

Zero Trust Architecture Alignment

The DoD Zero Trust Strategy (November 2022) requires all DoD entities to adopt Zero Trust principles by FY2027. While CMMC Level 2 does not explicitly mandate Zero Trust, many NIST 800-171 controls (AC, IA, SC families) align with ZTA principles. Organizations should document Zero Trust alignment in their SSP to demonstrate forward-looking security posture.

FORWARD LOOK: NIST SP 800-171 Revision 3 Transition

NIST published SP 800-171 Rev 3 in May 2024, reducing 110 requirements to 97 through consolidation and alignment with SP 800-53 Rev 5. CMMC 2.0 currently mandates Rev 2 compliance. DoD has not announced a formal Rev 3 transition date (expected 2-3 year transition period). Organizations should maintain Rev 2 compliance while mapping controls to Rev 3 to minimize future transition effort. Key changes include new Supply Chain Risk Management (SR) family, Organization-Defined Parameters (ODPs), and enhanced continuous monitoring requirements.

9. Appendices

Appendix A: Network Architecture Diagram

Detailed network topology diagram showing the CUI authorization boundary, network segments, security devices, and data flow paths. Include DMZ, internal CUI enclave, and corporate network segments.

Appendix B: CUI Data Flow Diagram

Diagram showing how CUI enters, moves through, is processed, stored, and exits the authorization boundary. Include all ingestion, processing, storage, transmission, and destruction points.

Appendix C: Physical Network Diagram

Physical layout of network infrastructure including server rooms, wiring closets, and physical security boundaries.

Appendix D: Ports, Protocols, and Services

List of authorized ports, protocols, and services allowed at the CUI boundary and key internal boundaries.

Appendix E: SSP Control Workbook

Detailed control-by-control implementation documentation for all 110 NIST SP 800-171 Rev 2 requirements (Excel companion document).

Appendix F: Acronyms and Glossary

Definitions of acronyms and technical terms used throughout this document.

Common Acronyms

AO — Authorizing Official | C3PAO — CMMC Third-Party Assessment Organization | CUI — Controlled Unclassified Information
CMC — CMMC | CTI — Controlled Technical Information | CSIRT — Computer Security Incident Response Team
DCISE — Defense Industrial Base Cybersecurity (https://icf.dcise.cert.org) | DIBNet — Defense Industrial Base Network (decommissioned June 2025; replaced by DCISE Portal)
DFARS — Defense Federal Acquisition Regulation Supplement | FIPS — Federal Information Processing Standards | ISA — Interconnection Security Agreement
ISSM — Information System Security Manager | ISSO — Information System Security Officer
MFA — Multi-Factor Authentication | NIST — National Institute of Standards and Technology
POA&M — Plan of Action & Milestones | SPRS — Supplier Performance Risk System
SSP — System Security Plan | STIG — Security Technical Implementation Guide