SAMPLE DOCUMENTATION DISCLAIMER

CMMC Level 2 Assessment Package

Cogswell Cogs, Inc. — Fictional Demonstration Entity

---

1. Purpose and Limitations

This documentation package, which includes a System Security Plan (SSP), Plan of Action and Milestones (POA&M), Network Topology Diagram, Data Flow Diagram, Facility Floor Plan, and Diagram-to-SSP Crosswalk, is provided solely for educational and demonstrative purposes. All content is built around 'Cogswell Cogs, Inc.,' a wholly fictional entity. Nothing in this package describes, references, or discloses any real organization, system, facility, contract, or security posture.

2. Not Legal or Professional Advice

Nothing in this package constitutes legal, regulatory, or certified cybersecurity advice. The documentation reflects one reasonable interpretation of NIST SP 800-171 Rev 2 implementation for a small Defense Industrial Base (DIB) contractor, but it's illustrative, not prescriptive. Reviewing or adopting these materials does not guarantee a passing outcome in any CMMC Level 2 or NIST SP 800-171 assessment, and it doesn't substitute for engagement with a Certified Third-Party Assessment Organization (C3PAO) or qualified legal counsel.

3. No Consulting Relationship Established

Access to or review of this sample package does not create a consulting engagement, attorney-client relationship, or any other professional relationship with David Koran & Associates. Every defense contractor's environment is different. Security controls, system boundaries, CUI data flows, and POA&M remediation strategies must be designed and validated against each organization's specific infrastructure, contractual obligations, and risk posture. This package is a starting point for understanding, not a ready-to-submit deliverable.

4. Limitation of Liability

David Koran & Associates assumes no liability for any actions taken, decisions made, or assessments conducted on the basis of this sample documentation. Organizations are solely responsible for their own compliance with DFARS 252.204-7012, 32 CFR Part 170, FAR 52.204-21, and all other applicable federal regulations and contract requirements. Use of this material is entirely at the reader's own risk.

5. Intellectual Property

This documentation package, including all fictional company data, framework narrative, document structures, and annotated guidance language, is the intellectual property of David Koran & Associates. It may be used for private study, staff training, or internal demonstration purposes. It may not be redistributed, resold, published, or represented as original work without prior written authorization.

David Koran & Associates
CMMC Compliance Consulting for the Defense Industrial Base
11 Park Street, Essex Junction, VT 05452
Office: (802) 404-1815
www.davidkoran.com

CMMC Registered Practitioner | ABA Associate Member

SYSTEM SECURITY PLAN

CMMC Level 2 / NIST SP 800-171 Rev 2

Cogswell Cogs, Inc.

Organization	Cogswell Cogs, Inc.
System Name	CUI Processing Environment (CPE)
System Owner	Victor Cogswell, CEO
ISSO / Security Contact	Margaret Cogswell, IT Manager
IT Administrator	Harlan Spacely
CAGE Code	7CG42
Contract Number(s)	W52P1J-23-C-0088 (Army Contracting Command – ACC-APG)
Facility Address	742 Skypad Boulevard, Orbit City, CA 90210
Document Version	3.0
Date Prepared	March 20, 2025 (v1.0 original)
Date Last Reviewed	March 20, 2026
SPRS Score (Self-Assessment)	107 (submitted January 15, 2026; reflects 1 partially implemented practice — see POA&M)

HANDLING NOTICE

This document may contain Controlled Unclassified Information (CUI). Handle and protect accordingly per 32 CFR Part 2002 and the Cogswell Cogs CUI Program Policy. Do not distribute without authorization from the System Owner.

1. About This Document

This System Security Plan (SSP) documents the security practices implemented by Cogswell Cogs, Inc. to protect Controlled Unclassified Information (CUI) processed, stored, and transmitted by the CUI Processing Environment (CPE). It satisfies the requirements of NIST SP 800-171 practice 3.12.4 and supports Cogswell Cogs' CMMC Level 2 certification under 32 CFR Part 170.

This SSP is reviewed annually, updated after any significant change to the system or its operating environment, and updated to reflect the closure of POA&M items. The ISSO is responsible for maintaining this document. The System Owner (CEO) approves all substantive revisions.

1.1 Status Definitions

Status Value	Meaning
Implemented	Fully in place across all applicable system components.
Partially Implemented	In place for some components or partially; a POA&M entry is required.
Not Implemented	Not yet implemented; a POA&M entry is required.
Not Applicable	Does not apply to this system; written rationale required.
Inherited	Fully satisfied by an external provider (e.g., FedRAMP CSP). Evidence required.

1.2 Supporting Documentation

Document	Location	Last Updated
Plan of Action & Milestones (POAM-001)	*SharePoint GCC High / Compliance / POA&M*	March 2026
Network Diagram (SAD-001 Appendix A)	*SharePoint GCC High / IT / Architecture*	January 2026
Data Flow Diagram (SAD-001 Appendix B)	*SharePoint GCC High / IT / Architecture*	January 2026
Hardware Inventory (INV-HW-001)	*SharePoint GCC High / IT / Inventory*	February 2026
Software Inventory (INV-SW-001)	*SharePoint GCC High / IT / Inventory*	March 2025

Document	Location	Last Updated
Access Control Policy (ACP-001)	*SharePoint GCC High / Policies*	November 2024
Incident Response Plan (IRP-001)	*SharePoint GCC High / Policies*	November 2024
Vulnerability Scan Reports (Nessus)	*SharePoint GCC High / Security / Scans*	February 2025
Risk Assessment Report (RA-2024-001)	*SharePoint GCC High / Security / RA*	August 2024
CUI Program Policy (CUI-POL-001)	*SharePoint GCC High / Policies*	September 2024

2. System Overview

2.1 System Description

Cogswell Cogs, Inc. is a precision mechanical components manufacturer headquartered in Orbit City, CA. The company produces gear assemblies, cog mechanisms, and motion control components under Contract W52P1J-23-C-0088 with the Army Contracting Command (ACC-APG). Under this contract, Cogswell Cogs receives, processes, and transmits Controlled Technical Information (CUI//SP-CTI) in the form of engineering specifications, technical drawings, test data, and program documentation related to DoD platform components.

The CUI Processing Environment (CPE) consists of 12 Windows 11 workstations in the engineering and program management areas, one Windows Server 2022 file server (FS-01), one Active Directory domain controller (DC-01), a Cisco managed switch, a SonicWall TZ570 perimeter firewall, FortiGate SSL VPN, Cisco Meraki wireless access points, and the Microsoft 365 GCC High tenant (cogs well.onmicrosoft.us). Twelve (12) employees are authorized to access CUI.

2.2 CUI Types

CUI Category	Description / Contract Source	Storage Location
CUI//SP-CTI	Controlled Technical Information: engineering drawings, CAD files, specifications, test and evaluation data for DoD gear and motion control components under W52P1J-23-C-0088.	*FS-01 (CUI Share); SharePoint GCC High; workstation local encrypted drives (temporary processing only)*
CUI//SP-EXPT	Export Controlled information: technical parameters subject to EAR/ITAR restrictions related to military-grade tolerances and material compositions.	*FS-01 (Export-CTI subfolder, restricted access group); SharePoint GCC High (Export CTI site)*
CUI//PRVCY	Privacy: names, contact information, and security screening records for CUI-authorized employees stored in HR files.	*SharePoint GCC High (HR site, access restricted to HR Manager and CEO)*

2.3 System Boundary and Scope

The CPE boundary includes all hardware, software, personnel, and facilities associated with the creation, processing, storage, transmission, and destruction of CUI in support of Contract W52P1J-23-C-0088. The boundary encompasses the 742 Skypad Boulevard facility, all systems described in Section 2.1, and the Microsoft 365 GCC High tenant.

The following are explicitly outside the CPE boundary: the cogswellcogs.com public website (no CUI), employee personal devices (prohibited from CUI access), and the general corporate guest Wi-Fi network (VLAN 30, physically isolated from CUI systems). The boundary is illustrated in the Network Diagram (SAD-001, Appendix A).

2.4 Cloud Service Providers

Provider / Service	Service Type	FedRAMP Status	CUI Processed
Microsoft 365 GCC High	SaaS (Email, SharePoint, Teams, Intune, Defender)	FedRAMP High Authorized (IL4)	CTI, Export-CTI, Privacy CUI (email, document storage, collaboration)
Microsoft Azure GCC High	IaaS (Blob Storage – backup archive)	FedRAMP High Authorized (IL4)	Backup copies of CUI data (encrypted, WORM-protected)
Tenable.io Essentials	SaaS (Vulnerability Scanning)	FedRAMP Moderate (scan metadata only; no CUI)	Scan results (no CUI content transmitted)
KnowBe4	SaaS (Security Awareness Training)	SOC 2 Type II (no CUI)	No CUI; training completion records and phishing metrics only

2.5 System Interconnections

Connected System	Owner / Org	Data Flow	Agreement Type	Notes
DoD SAFE (DoD Secure Access File Exchange)	Defense Information Systems Agency (DISA)	Inbound	DFARS 252.204-7012 accepted	Used to receive CUI deliverables from ACC-APG contracting officer. TLS-encrypted. No CUI stored on SAFE beyond download.
Microsoft 365 GCC High Tenant	Microsoft Corporation	Bidirectional	Microsoft Customer Agreement + FedRAMP ATO	Primary platform for CUI email, document storage, and collaboration. Within CPE boundary.
ACC-APG Contracting Portal (Wide Area Workflow)	Army Contracting Command – APG	Bidirectional	DFARS clause-governed	Used for contract invoicing and submission. CUI is not routinely transmitted through WAWF; deliverables use DoD SAFE.

Connected System	Owner / Org	Data Flow	Agreement Type	Notes
Koran & Associates (CMMC Consultant)	David Koran & Associates	Bidirectional	NDAA-compliant subcontractor agreement with CMMC flowdown	Receives read-only access to this SSP and supporting documentation for annual review. No CUI system access.

2.6 Roles and Responsibilities

Role	Assigned Individual	Responsibilities
System Owner	Victor Cogswell (CEO)	Accountable for overall security posture. Authorizes access and system changes. Accepts residual risk. Approves SSP revisions and CMMC certification submission.
ISSO / Security Contact	Margaret Cogswell (IT Manager)	Day-to-day security operations. Maintains and updates this SSP. Manages POA&M. Coordinates CMMC assessment activities. Serves as primary IR Lead.
IT Administrator	Harlan Spacely	Implements and maintains technical controls. Manages AD accounts, patches, firewall rules, and SIEM configuration. Executes backup and recovery procedures.
CUI Handlers (Engineering)	8 licensed engineers (see PAR-001 for list)	Process CUI under Contract W52P1J-23-C-0088. Subject to annual security awareness training and CUI handling procedures.
CUI Handlers (Program Mgmt)	3 program managers (see PAR-001 for list)	Manage program documentation and deliverables. Handle CUI in SharePoint GCC High and DoD SAFE. Subject to CUI training requirements.
CMMC Consultant	David Koran, Koran & Associates (subcontractor)	Provides annual independent review of this SSP, POA&M, and technical controls. Does not hold system access credentials.

3. Applicable Laws, Regulations, and Standards

Authority / Reference	Applicability to Cogswell Cogs
32 CFR Part 2002	Governs the CUI program governmentwide; establishes marking, safeguarding, and dissemination controls for all three CUI categories handled by Cogswell Cogs.
32 CFR Part 170	Implements the CMMC program. Cogswell Cogs requires CMMC Level 2 certification as a condition of Contract W52P1J-23-C-0088 renewal (Phase 1 enforcement applies).
DFARS 252.204-7012	Requires adequate security for covered contractor information systems. Obligates Cogswell Cogs to report cyber incidents to DoD within 72 hours and preserve media for 90 days.
DFARS 252.204-7019	Requires a current NIST SP 800-171 self-assessment score posted to SPRS. Cogswell Cogs submitted a score of 89 on February 14, 2025.
DFARS 252.204-7020	NIST SP 800-171 DoD Assessment requirement. Score on file in SPRS. Contract W52P1J-23-C-0088 includes this clause.
DFARS 252.204-7021	CMMC contract clause. CMMC Level 2 certification required at next contract award. Cogswell Cogs is pursuing C3PAO-conducted assessment in Q3 2025.
NIST SP 800-171 Rev 2	Primary technical standard. All 110 practices are implemented, partially implemented, or documented as not applicable in this SSP.
NIST SP 800-171A	Assessment procedures used by the ISSO for internal control assessments (SCA-2024-001) and referenced by C3PAOs during CMMC assessment.
NIST SP 800-88 Rev 1	Media sanitization standard. Referenced by MSP-001 and applied to all CUI media sanitization events per practice 3.8.3.
NIST SP 800-30 Rev 1	Risk assessment methodology used for RA-2024-001. Selected as the baseline methodology for all Cogswell Cogs risk assessment activities.
FAR 52.204-21	Basic safeguarding of covered contractor information systems. Satisfied by this SSP and the full NIST SP 800-171 implementation.
ITAR (22 CFR Parts 120-130)	Export Administration Regulations apply to CUI//SP-EXPT materials. Export control compliance is addressed in the Export Control Policy (ECP-001) coordinated with outside counsel.

4. Security Practice Implementations

This section documents implementation status and supporting detail for each of the 110 NIST SP 800-171 Rev 2 security practices across all 14 practice families. Implementation descriptions reflect the state of the CPE as of the date of this SSP. Practices with a status of Partially Implemented or Not Implemented have corresponding entries in the POA&M (Section 5).

4.1 AC — Access Control (3.1.x, 22 Practices)

Cogswell Cogs controls system access through Active Directory group policies, role-based access controls, and a formal access authorization process administered by the IT Administrator. Remote access is provided exclusively via FortiGate SSL VPN with MFA enforced through Microsoft Authenticator. Mobile devices are managed through Microsoft Intune.

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices.	**Implemented**	Active Directory Domain Controller (DC-01)	Access is limited to Active Directory domain accounts. All workstations and servers require domain authentication. Guest accounts are disabled via Group Policy (GPO-SEC-001). A formal account request and approval process documented in the Access Control Policy (ACP-001) requires ISSO and system owner authorization before any account is provisioned.	IT Administrator
3.1.2	Limit system access to the types of transactions and functions authorized users are permitted to execute.	**Implemented**	Active Directory Domain Controller (DC-01)	Role-based access groups in Active Directory restrict access to CUI file shares. Engineering staff have read/write to project folders. Program managers have read-only to CUI deliverable folders. Administrators have elevated rights documented in the Privileged Access Register (PAR-001). GPO	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				enforces software restriction policies.	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	**Partially Implemented**	File Server (FS-01, Windows Server 2022); Microsoft 365 GCC High (Exchange Online, SharePoint, Teams)	CUI is stored on FS-01 in access-controlled shares and in SharePoint GCC High. Data Loss Prevention (DLP) policies in Microsoft Purview are configured to flag CUI exfiltration via email. DLP coverage does not yet extend to USB output from workstations. A POA&M is in place to deploy endpoint DLP via Intune by Q3 2025.	ISSO
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	**Implemented**	Active Directory Domain Controller (DC-01)	Separation of duties is enforced by policy (SoD Policy SDP-001) and technically through AD group separation. No single user holds both IT Administrator and Finance roles. The ISSO does not hold system owner authority. Account provisioning requires approval from the system owner independent of the IT Administrator.	System Owner / ISSO
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	**Implemented**	Active Directory Domain Controller (DC-01)	Least privilege is enforced through AD role-based groups. Standard users have no local administrator rights on workstations (enforced via GPO). Privileged Access Register (PAR-001) documents all privileged accounts. Quarterly access reviews confirm that assigned privileges remain appropriate and are performed by the ISSO.	IT Administrator / ISSO
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	**Implemented**	Active Directory Domain Controller (DC-01)	IT Administrator (H. Spacely) maintains two accounts: a standard user account for day-to-day email and productivity, and a separate admin account (admin.hspacely)	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				used exclusively for system administration tasks. Policy (ACP-001 Sec 4.2) prohibits use of admin accounts for email, browsing, or non-administrative tasks.	
3.1.7	Prevent non-privileged users from executing privileged functions and capture execution in audit logs.	**Implemented**	Active Directory Domain Controller (DC-01)	GPO restricts standard users from running privileged operations. User Account Control (UAC) is set to highest level across all workstations via GPO (GPO-SEC-003). All privileged function executions are captured in Windows Security Event Log and forwarded to the central log server (SIEM-01) where they are retained per the audit logging policy.	IT Administrator
3.1.8	Limit unsuccessful logon attempts.	**Implemented**	Active Directory Domain Controller (DC-01)	Active Directory account lockout policy (GPO-SEC-001) enforces lockout after 5 consecutive failed logon attempts within a 15-minute window. Accounts remain locked for 30 minutes or until reset by the IT Administrator. Policy applies to all domain accounts including VPN authentication via LDAP integration.	IT Administrator
3.1.9	Provide privacy and security notices consistent with CUI rules.	**Implemented**	All in-scope systems	A CUI-compliant system banner (Banner-001) is displayed at login for all workstations and the VPN portal. The banner text was reviewed against NARA guidance and approved by legal counsel. Banner content includes system monitoring notice, prohibition on unauthorized use, and consent to monitoring. Last reviewed March 2025.	ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.1.10	Use session lock with pattern-hiding displays after a period of inactivity.	**Implemented**	Windows 11 Workstations (WS-01 through WS-12)	GPO (GPO-SEC-002) enforces screen lock after 15 minutes of inactivity on all workstations. Screen saver password protection is enabled. FS-01 and DC-01 servers enforce session lock after 10 minutes. Remote desktop sessions terminate after 30 minutes of inactivity per RDP policy settings.	IT Administrator
3.1.11	Terminate (automatically) a user session after a defined condition.	**Implemented**	Active Directory Domain Controller (DC-01); FortiGate SSL VPN	Active Directory Group Policy (GPO-SEC-002) terminates idle sessions after 60 minutes on all systems. FortiGate VPN sessions are configured with an 8-hour hard timeout and a 60-minute idle timeout. Microsoft 365 GCC High enforces a session timeout of 8 hours per tenant conditional access policy (CAP-003).	IT Administrator
3.1.12	Monitor and control remote access sessions.	**Implemented**	FortiGate SSL VPN	All remote access is routed through FortiGate SSL VPN. VPN session logs are forwarded to SIEM-01 in real time. The ISSO reviews VPN access logs weekly for anomalies. Remote access is restricted to company-managed devices enrolled in Microsoft Intune. Split tunneling is disabled; all traffic routes through the VPN.	ISSO / IT Administrator
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	**Implemented**	FortiGate SSL VPN	FortiGate SSL VPN enforces TLS 1.2 minimum with AES-256-GCM cipher suites. Weak cipher suites (RC4, 3DES, SSL 3.0) are disabled. VPN configuration was reviewed by an external security consultant (Koran & Associates) in January 2025.	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				Configuration documentation is maintained in the System Configuration Baseline (SCB-VPN-001).	
3.1.14	Route remote access via managed access control points.	**Implemented**	FortiGate SSL VPN	All remote access is routed exclusively through the FortiGate VPN gateway at the Orbit City facility. Direct remote desktop connections from the internet are blocked at the perimeter firewall (SonicWall TZ570). No alternative remote access paths are permitted. Conditional Access Policy (CAP-001) in Azure AD GCC High blocks authentication from non-VPN IP ranges.	IT Administrator
3.1.15	Authorize remote execution of privileged commands and access to security-relevant information via remote access only for documented operational needs.	**Implemented**	FortiGate SSL VPN	Privileged remote access is documented in the Remote Access Authorization Register (RAAR-001). IT Administrator remote administration sessions are conducted via VPN with MFA. Remote privileged sessions are logged and reviewed by the ISSO. No privileged remote access is permitted without documented authorization.	ISSO / IT Administrator
3.1.16	Authorize wireless access prior to allowing such connections.	**Implemented**	Cisco Meraki MR46 Access Points	Wireless access requires pre-authorization documented in the Wireless Access Authorization Register (WAAR-001). The CUI network SSID is restricted to domain-joined devices via 802.1X certificate-based authentication using Active Directory Certificate Services. A separate guest SSID is network-segmented and	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				blocked from all internal resources.	
3.1.17	Protect wireless access using authentication and encryption.	**Implemented**	Cisco Meraki MR46 Access Points	CUI network SSID uses WPA3-Enterprise with 802.1X authentication. Encryption is AES-256. Guest SSID uses WPA3-Personal with isolation enabled. SSID names do not reveal organizational identity. Wireless configuration baseline is documented in SCB-WIFI-001. Annual wireless security review was completed February 2025.	IT Administrator
3.1.18	Control connection of mobile devices.	**Implemented**	Microsoft Intune (MDM)	Mobile devices that access CUI must be enrolled in Microsoft Intune. Intune compliance policies enforce device encryption, screen lock, and current OS patch level before CUI access is granted. Unenrolled personal devices are blocked from accessing M365 GCC High via Conditional Access Policy (CAP-002). BYOD devices are not permitted to access CUI file shares.	IT Administrator / ISSO
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	**Implemented**	Microsoft Intune (MDM)	Intune device compliance policy requires BitLocker encryption on Windows laptops and device encryption on iOS and Android devices. Encryption compliance is verified automatically by Intune before granting access to M365 GCC High. Non-compliant devices are blocked automatically. Encryption status reports reviewed quarterly by ISSO.	IT Administrator
3.1.20	Verify and control/limit connections to external systems.	**Implemented**	SonicWall TZ570 Firewall	All connections to external systems are governed by the External	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				System Connection Policy (ESCP-001). Outbound connections are subject to SonicWall application control and URL filtering. External file sharing is restricted to approved channels (SharePoint GCC High). Connections to unapproved cloud storage (Dropbox, personal Google Drive, etc.) are blocked at the firewall.	
3.1.21	Limit use of portable storage devices on external systems.	**Implemented**	Windows 11 Workstations (WS-01 through WS-12)	USB removable storage is prohibited on all CUI workstations and servers via GPO (GPO-SEC-005) using Windows Device Installation restrictions by device class. No exceptions are authorized or active. This prohibition is consistent with the Media Protection policy (MSP-001) and the Access Control Policy (ACP-001), both of which use identical language: portable storage devices are not permitted on any system within the CPE boundary. Any future exception request would require ISSO and System Owner written approval, a formal policy amendment, and a corresponding POA&M review; no such requests are pending.	IT Administrator
3.1.22	Control CUI posted or processed on publicly accessible systems.	**Not Applicable**	N/A	Cogswell Cogs does not operate any publicly accessible web servers or portals. The company website (cogswellcogs.com) is hosted by a third-party provider and contains only marketing content. CUI is never posted to public-facing systems. No customer portals or	ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				extranet systems are in operation.	

4.2 AT — Awareness and Training (3.2.x, 3 Practices)

Cogswell Cogs delivers annual security awareness training through KnowBe4, supplemented by quarterly phishing simulations. Role-based training for the IT Administrator and ISSO is conducted separately and documented in individual training records maintained by HR.

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.2.1	Ensure managers, system administrators, and users are aware of security risks and applicable policies.	**Implemented**	All in-scope systems	Annual security awareness training is delivered through KnowBe4 (Module Set: CMMC Essentials). Training covers CUI handling, phishing recognition, password hygiene, physical security, and incident reporting. Completion is tracked in KnowBe4; completion records are exported to HR annually. All 12 CUI-authorized users completed the most recent training cycle by January 31, 2025. Training records retained for three years.	ISSO / HR
3.2.2	Ensure personnel are trained to carry out their assigned information security responsibilities.	**Implemented**	All in-scope systems	Role-based training is assigned based on job function. IT Administrator (H. Spacely) completed CompTIA Security+ and annual CMMC practitioner training (8 hours, January 2025). ISSO (M. Cogswell) completed Registered Practitioner training and an annual CMMC update	HR / ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				module. System Owner (V. Cogswell) completed executive cybersecurity awareness training (2 hours). Training certificates are on file with HR.	
3.2.3	Provide security awareness training on recognizing and reporting potential threats, including social engineering attacks.	**Implemented**	All in-scope systems	Social engineering and insider threat awareness is integrated into the annual KnowBe4 training curriculum and reinforced through quarterly phishing simulations. Phishing simulation results (click rate, reporting rate) are tracked by the ISSO. Users who click simulated phishing emails are automatically enrolled in a remedial training module. Q4 2024 phishing simulation click rate: 4.2%. Reporting rate: 68%.	ISSO

4.3 AU — Audit and Accountability (3.3.x, 9 Practices)

Cogswell Cogs collects audit logs from all in-scope systems and centralizes them in a Wazuh SIEM (SIEM-01) running on a dedicated Ubuntu 22.04 server. Windows event logs, firewall logs, VPN logs, and M365 audit logs are ingested. Log retention is 90 days online and 12 months archived to Azure Blob Storage (GCC High).

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.3.1	Create and retain system audit logs to enable monitoring, analysis, investigation, and reporting.	**Implemented**	All in-scope systems; Wazuh SIEM (SIEM-01)	All in-scope systems forward audit logs to SIEM-01 (Wazuh) via encrypted syslog (TLS). Windows Security Event logs are forwarded using Wazuh agents installed on all workstations and	IT Administrator / ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				servers. M365 audit logs are pulled via the Office 365 Management Activity API. Logs are retained 90 days on SIEM-01 and archived to Azure GCC High Blob Storage for 12 months. Log retention policy is documented in ALP-001.	
3.3.2	Ensure that actions of individual system users can be uniquely traced to those users.	**Implemented**	Active Directory Domain Controller (DC-01); SIEM-01	All domain accounts are uniquely named (firstname.lastname format). Shared accounts are not permitted. Active Directory audit policy logs all authentication events, privilege use, and object access to individual accounts. SIEM-01 correlates all events to the originating user account. The IT Administrator maintains an account inventory in the Privileged Access Register (PAR-001).	IT Administrator
3.3.3	Review and update logged events.	**Implemented**	SIEM-01	The logged event list was established in August 2024 and is reviewed semi-annually by the ISSO. Current logged events include: logon/logoff (success and failure), account creation/deletion/modification, privilege escalation, object access on CUI file shares, process creation, policy changes, and firewall rule changes. Last review: February 2025. Documented in Event Logging Standard (ELS-001).	ISSO
3.3.4	Alert in the event of an audit logging process failure.	**Implemented**	SIEM-01; Wazuh	Wazuh SIEM is configured with an agent health monitoring rule that generates a Priority 1 alert if an agent stops sending logs for more than 15 minutes. Alerts are delivered via email to	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				the IT Administrator and ISSO. Monthly SIEM health checks verify that all agents are reporting. Log source status dashboard is reviewed weekly by the IT Administrator.	
3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response.	**Partially Implemented**	SIEM-01	Wazuh SIEM provides correlation across Windows, firewall, and VPN log sources. Correlation rules are based on the Wazuh default ruleset plus custom rules developed by the IT Administrator. M365 audit log ingestion is in place but correlation between M365 events and on-premises events is not yet fully automated. A POA&M is in place to complete M365 cross-source correlation by Q2 2025.	IT Administrator / ISSO
3.3.6	Provide audit record reduction and report generation to support on-demand analysis.	**Implemented**	SIEM-01	Wazuh SIEM provides a web-based dashboard with pre-built reports for authentication events, file access on CUI shares, and VPN session activity. Custom reports can be generated on demand by the ISSO. Weekly automated summary reports are emailed to the ISSO and IT Administrator. Report templates are documented in SIEM Operations Guide (SOG-001).	IT Administrator
3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source.	**Implemented**	All in-scope systems	All domain-joined systems synchronize time to DC-01, which is configured as the authoritative NTP source polling time.windows.com (NIST). GPO (GPO-NET-001) enforces NTP configuration. Time synchronization status is	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				verified as part of monthly system checks. Maximum time skew is set to 5 minutes, which triggers an automatic Kerberos authentication failure alert.	
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	**Implemented**	SIEM-01; Azure GCC High	SIEM-01 is accessible only to the IT Administrator and ISSO via MFA-protected administrative accounts. Log data on SIEM-01 is stored on an isolated RAID volume with ACLs preventing modification by non-root users. Archived logs in Azure GCC High Blob Storage have immutability policies (WORM) configured with a 12-month retention lock. Log access changes generate alerts to the ISSO.	IT Administrator
3.3.9	Limit management of audit logging to a subset of privileged users.	**Implemented**	SIEM-01	Wazuh SIEM administrative access is restricted to the IT Administrator account (admin.hspacely) and the ISSO account (admin.mcogswell). Standard user accounts have no access to SIEM-01. The system owner can view read-only dashboards but cannot modify log configurations. Access controls are reviewed quarterly.	ISSO

4.4 CM — Configuration Management (3.4.x, 9 Practices)

Cogswell Cogs maintains system configuration baselines using CIS Level 1 benchmarks for Windows 11 and Windows Server 2022, enforced through Group Policy. Changes to in-scope systems follow a formal change

management process documented in Change Management Procedure CMP-001.

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems.	**Implemented**	All in-scope systems	System configuration baselines are documented in the System Configuration Baseline register (SCB-001 through SCB-009, one per system type). Hardware and software inventories are maintained in a spreadsheet (INV-HW-001 and INV-SW-001) updated monthly. Baselines are derived from CIS Level 1 benchmarks and reviewed annually. Last baseline review: January 2026. Asset inventory was last audited February 28, 2026.	IT Administrator
3.4.2	Establish and enforce security configuration settings for IT products.	**Implemented**	Active Directory Domain Controller (DC-01); Windows 11 Workstations (WS-01 through WS-12)	Security configuration settings are enforced through Group Policy Objects (GPOs). The following GPOs are in scope: GPO-SEC-001 (account policy), GPO-SEC-002 (session and screen lock), GPO-SEC-003 (UAC and application control), GPO-SEC-004 (Windows Defender configuration), GPO-SEC-005 (USB restriction), GPO-NET-001 (NTP and DNS). GPO compliance is verified monthly using Group Policy Results.	IT Administrator
3.4.3	Track, review, approve, and log changes to organizational systems.	**Implemented**	All in-scope systems	All changes to in-scope systems are submitted through the Change Management Request (CMR) process (CMP-001). Change requests require ISSO review for security impact and system owner	IT Administrator / ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				approval for significant changes. Emergency changes are permitted with post-hoc ISSO notification within 24 hours. A change log (CHG-LOG-001) is maintained in SharePoint GCC High. Unauthorized changes trigger an alert from SIEM-01.	
3.4.4	Analyze the security impact of changes prior to implementation.	**Implemented**	All in-scope systems	Security impact analysis is a required field on all CMR forms. The IT Administrator completes an initial impact assessment; the ISSO reviews for security implications. High-impact changes (new systems, firewall rule changes, privileged account additions) require written ISSO approval before implementation. Security impact documentation is retained with the CMR record in SharePoint GCC High.	ISSO
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes.	**Implemented**	All in-scope systems	Change access restrictions are documented in CMP-001. Logical changes require IT Administrator credentials with MFA. Physical access to server room hardware requires keycard access (IT Administrator and ISSO only). Changes involving CUI data stores require system owner sign-off. Access logs for the server room are reviewed alongside change records to verify authorized access.	IT Administrator / System Owner
3.4.6	Employ the principle of least functionality by configuring systems to provide only essential capabilities.	**Implemented**	Windows 11 Workstations (WS-01 through WS-12); File Server	Unnecessary Windows features (Internet Information Services, Windows Media Player, Remote Registry, Telnet Client, TFTP Client) are	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
			(FS-01, Windows Server 2022)	disabled via GPO (GPO-SEC-003) on all workstations and servers. FS-01 runs only File and Storage Services and is not configured as a domain controller or print server. Ports not required by business operations are blocked on the host-based Windows Firewall.	
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	**Implemented**	All in-scope systems; SonicWall TZ570 Firewall	The SonicWall TZ570 firewall enforces a deny-by-default outbound policy with exceptions for business-required traffic documented in the Firewall Rule Register (FRR-001). Host-based Windows Firewall on workstations and servers blocks inbound connections not explicitly required. A list of prohibited applications is maintained in the Prohibited Software Policy (PSP-001). Prohibited application usage is monitored via SIEM-01.	IT Administrator
3.4.8	Apply deny-by-exception or allow-by-exception policy to prevent unauthorized software use.	**Partially Implemented**	Windows 11 Workstations (WS-01 through WS-12)	An approved software list (ASL-001) is maintained and enforced through AppLocker policy on Windows 11 workstations for most application categories. AppLocker is not yet fully deployed on FS-01 and DC-01. A POA&M is in place to extend AppLocker coverage to servers by Q3 2025. Unapproved software installation is also technically restricted by removing local admin rights from all standard users.	IT Administrator
3.4.9	Control and monitor user-installed software.	**Implemented**	Windows 11 Workstations (WS-01	User-installed software is controlled by removing local administrator rights	IT Administrator / ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
			through WS-12); SIEM-01	from all standard user accounts (GPO-SEC-003). The software inventory (INV-SW-001) is reconciled monthly against SIEM-01 application telemetry and Microsoft Intune device compliance reports. Any newly detected application not on the approved software list (ASL-001) triggers an alert to the IT Administrator for investigation.	

4.5 IA — Identification and Authentication (3.5.x, 11 Practices)

All users and devices accessing Cogswell Cogs systems are authenticated through Active Directory with MFA enforced via Microsoft Entra ID Conditional Access policies. MFA is mandatory for all remote access and all M365 GCC High access. Hardware security tokens (YubiKey 5) are issued to the IT Administrator and ISSO for privileged account access.

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.5.1	Identify system users, processes acting on behalf of users, and devices.	**Implemented**	Active Directory Domain Controller (DC-01)	All users are assigned a unique Active Directory account following the naming convention firstname.lastname. Service accounts follow the naming convention svc.[function] and are documented in the Service Account Register (SAR-001). All domain-joined devices have unique machine accounts in AD. Non-domain devices are blocked from accessing CUI resources via	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				Conditional Access policies.	
3.5.2	Authenticate the identities of users, processes, or devices as a prerequisite to allowing access.	**Implemented**	Active Directory Domain Controller (DC-01)	Authentication is required before any access to organizational resources. Domain-joined workstations require domain credential authentication. CUI file shares, VPN access, and M365 GCC High require authentication via Entra ID. Device authentication for network access uses 802.1X certificate-based authentication for wireless. All authentication events are logged to SIEM-01.	IT Administrator
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	**Implemented**	Active Directory Domain Controller (DC-01); Microsoft Entra ID	MFA is enforced via Entra ID Conditional Access policies for all user accounts accessing M365 GCC High (CAP-001). VPN authentication requires MFA via FortiToken integration with Entra ID. Privileged accounts (IT Administrator, ISSO) use YubiKey 5 hardware tokens as a second factor. Local console access to servers is restricted to the server room, which requires physical keycard access as the second factor.	IT Administrator / ISSO
3.5.4	Employ replay-resistant authentication mechanisms for network access.	**Implemented**	Active Directory Domain Controller (DC-01); FortiGate SSL VPN	Kerberos authentication (used for domain logon) is inherently replay-resistant through the use of time-limited tickets (5-minute maximum clock skew). VPN authentication uses SAML 2.0 tokens with short-lived assertions (10-minute expiry). M365 GCC High uses OAuth 2.0 with short-lived tokens. TLS 1.2+ on all network authentication sessions prevents session replay.	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.5.5	Employ identifier management practices.	**Implemented**	Active Directory Domain Controller (DC-01)	Identifier management is governed by the Identity Management Policy (IMP-001). User IDs are never reused after account deletion. Departed employee accounts are disabled and renamed with a TERMINATED_ prefix and retained for 90 days before deletion. Service accounts are reviewed quarterly. Account issuance requires documented approval. All account lifecycle events are logged to SIEM-01.	IT Administrator / ISSO
3.5.6	Disable identifiers after a defined inactivity period.	**Implemented**	Active Directory Domain Controller (DC-01)	Active Directory accounts are automatically disabled after 90 days of inactivity via a scheduled PowerShell script (Disable-StaleAccounts.ps1) that runs weekly and reports results to the ISSO. The inactivity threshold is defined in IMP-001. Disabled accounts are reviewed monthly; accounts inactive for more than 180 days are deleted after ISSO confirmation.	IT Administrator / ISSO
3.5.7	Enforce a minimum password complexity and change of passwords when new passwords are created.	**Implemented**	Active Directory Domain Controller (DC-01)	Password policy enforced via AD Fine-Grained Password Policy (FGPP): minimum 15 characters, complexity requirement (uppercase, lowercase, number, symbol), 90-day maximum age, no reuse of last 24 passwords. Privileged accounts (IT Administrator, ISSO) have a separate FGPP requiring 20-character minimum and 60-day maximum age. New passwords set at account creation must be changed at first logon.	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.5.8	Prohibit password reuse for a specified number of generations.	**Implemented**	Active Directory Domain Controller (DC-01)	AD Fine-Grained Password Policy prohibits reuse of the last 24 passwords for standard users and the last 30 passwords for privileged accounts. Password history is stored securely by Active Directory. Policy compliance is automatically enforced; users cannot override the restriction. Policy settings documented in IMP-001.	IT Administrator
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	**Implemented**	Active Directory Domain Controller (DC-01)	All new accounts and all password resets are configured with the 'User must change password at next logon' flag set in Active Directory. Temporary passwords are communicated to users via secure channel (in-person or encrypted email). Temporary passwords have a 24-hour validity window; accounts not activated within 24 hours are disabled automatically.	IT Administrator
3.5.10	Store and transmit only cryptographically protected passwords.	**Implemented**	Active Directory Domain Controller (DC-01); Windows 11 Workstations (WS-01 through WS-12)	Active Directory stores passwords using the Kerberos AES-256 encryption protocol. LM hash storage is disabled via GPO (GPO-SEC-001). NTLMv1 is disabled; only NTLMv2 and Kerberos are permitted. Windows FIPS mode is enabled on all systems via GPO (GPO-SEC-006). Password transmission occurs only over encrypted channels (Kerberos, TLS 1.2+). Plain-text authentication protocols (Telnet, FTP, HTTP Basic Auth) are blocked.	IT Administrator
3.5.11	Obscure feedback of authentication information.	**Implemented**	All in-scope systems	All system login interfaces (Windows login screens, VPN portal, web applications)	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				mask password characters with asterisks or dots during entry. Login error messages are generic ('Invalid username or password') and do not disclose whether the username or password was incorrect, preventing username enumeration. Verified on all in-scope interfaces as of January 2025 system review.	

4.6 IR — Incident Response (3.6.x, 3 Practices)

Cogswell Cogs maintains a written Incident Response Plan (IRP-001) reviewed annually by the ISSO and system owner. The plan incorporates the 72-hour DIBCAC reporting requirement under DFARS 252.204-7012. Incident records are tracked in a SharePoint GCC High incident log. The most recent tabletop exercise was conducted October 2024.

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.6.1	Establish an operational incident-handling capability for organizational systems.	**Implemented**	All in-scope systems	The Incident Response Plan (IRP-001) defines six phases: Preparation, Detection and Analysis, Containment, Eradication, Recovery, and Post-Incident Review. Roles and responsibilities are assigned to the ISSO (IR Lead), IT Administrator (Technical Response), and System Owner (Business Decision Authority). External resources include a retainer with Koran & Associates for IR support. IRP was last reviewed and approved by the	ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				System Owner on November 1, 2024.	
3.6.2	Track, document, and report incidents to designated officials and/or authorities.	**Implemented**	SharePoint GCC High (Incident Log); M365 GCC High	All security incidents are documented in the Incident Tracking Log (ITL-001) maintained in SharePoint GCC High. Each incident record captures: date/time discovered, systems affected, CUI involved, containment actions, eradication steps, root cause, and lessons learned. For incidents involving CUI compromise or potential compromise, DFARS 252.204-7012 imposes a mandatory 72-hour reporting deadline from the time the contractor discovers the incident. The 72-hour clock and the DIBNet portal reporting procedure are explicitly documented in IRP-001, Section 4.3 ('Reporting Obligations'), which designates the ISSO as the reporting official with the System Owner as backup. Failure to report within 72 hours is treated as a contractual and regulatory hard fail. The ISSO maintains DIBNet portal credentials and the DoD Cyber Crime Center (DC3) reporting address on file. Copies of all incident reports submitted to DoD are retained in SharePoint GCC High for a minimum of 3 years.	ISSO / System Owner
3.6.3	Test the organizational incident response capability.	**Implemented**	All in-scope systems	An annual IR tabletop exercise is conducted by the ISSO with participation from the IT Administrator, System Owner, and at least two CUI handlers. The October 2024 tabletop exercise tested a	ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				ransomware scenario involving CUI file shares. Results were documented in the IR Exercise After Action Report (IREAR-2024-001). Two corrective actions were identified and added to the POA&M. Next exercise is scheduled for October 2025.	

4.7 MA — Maintenance (3.7.x, 6 Practices)

System maintenance at Cogswell Cogs is performed by the IT Administrator with documented authorization. Third-party maintenance (hardware repair, specialized support) requires prior ISSO approval and is escorted by the IT Administrator. Remote maintenance sessions are conducted exclusively via the VPN with MFA and are logged.

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.7.1	Perform maintenance on organizational systems.	**Implemented**	All in-scope systems	Routine maintenance is performed by the IT Administrator per the Maintenance Policy (MTP-001). Maintenance activities include monthly patch cycles, quarterly hardware inspections, semi-annual backup restoration tests, and annual network equipment firmware updates. Maintenance activities are logged in the System Maintenance Log (SML-001) maintained in SharePoint GCC High. All maintenance is authorized by the ISSO before execution.	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel that conduct system maintenance.	**Implemented**	All in-scope systems	Approved maintenance tools are documented in the Maintenance Tools Register (MTR-001). Tools used on CUI systems must be company-owned, inventoried, and scanned for malware before use. External technicians (e.g., hardware vendors) must sign a Non-Disclosure Agreement (NDA) and be escorted by the IT Administrator. Remote maintenance by vendors is permitted only via the VPN with ISSO-issued temporary credentials.	IT Administrator / ISSO
3.7.3	Ensure equipment removed for off-site maintenance is sanitized.	**Implemented**	All in-scope systems	Equipment removed for off-site maintenance is sanitized prior to removal using NIST SP 800-88-compliant procedures (Purge method for SSDs, Clear method for HDDs). Sanitization is documented on the Media Sanitization Record (MSR-001). If sanitization is not possible before removal (e.g., failed drive), the equipment is escorted by the IT Administrator to the repair facility and returned without being left unattended.	IT Administrator
3.7.4	Check media containing diagnostic and test programs for malicious code before use.	**Implemented**	Windows 11 Workstations (WS-01 through WS-12)	All diagnostic media (USB drives, optical discs) brought onto CUI systems are scanned with Microsoft Defender for Endpoint before connection or execution. The IT Administrator maintains a dedicated, isolated workstation (WS-MAINT-01) for malware scanning of maintenance media. Scan results are documented in the maintenance log.	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				This process applies to both internal IT staff and third-party technicians.	
3.7.5	Require MFA to establish nonlocal maintenance sessions via external network connections and terminate such connections when complete.	**Implemented**	FortiGate SSL VPN	All nonlocal maintenance sessions require VPN authentication with MFA (YubiKey or FortiToken). Vendor remote access uses time-limited VPN credentials created by the IT Administrator, activated only during the approved maintenance window, and revoked immediately upon session completion. Session activity is logged by SIEM-01. The IT Administrator monitors all vendor remote sessions in real time.	IT Administrator / ISSO
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	**Implemented**	All in-scope systems	Third-party maintenance personnel who do not hold appropriate access authorization are escorted at all times by the IT Administrator. Escorted maintenance is documented in the Visitor and Maintenance Escort Log (VMEL-001). No third-party maintenance personnel are permitted to access CUI systems without being under continuous direct supervision. The policy is documented in MTP-001 and communicated to all maintenance vendors.	IT Administrator

4.8 MP — Media Protection (3.8.x, 9 Practices)

Cogswell Cogs restricts CUI to approved digital systems and minimizes physical media. USB storage is technically blocked on all workstations. Physical documents containing CUI are stored in locked cabinets and

shredded when no longer needed using a cross-cut shredder. Media sanitization follows NIST SP 800-88 procedures documented in the Media Sanitization Policy (MSP-001).

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.8.1	Protect system media containing CUI, both paper and digital.	**Implemented**	File Server (FS-01, Windows Server 2022); M365 GCC High; Physical Storage	Digital CUI is stored on access-controlled file shares on FS-01 and in SharePoint GCC High. Physical documents containing CUI are stored in locked file cabinets in the engineering area, accessible only to personnel with CUI access authorization. Server room physical access requires keycard. Backup media (external drives) are stored in a locked fireproof cabinet in the server room.	IT Administrator / ISSO
3.8.2	Limit access to CUI on system media to authorized users.	**Implemented**	File Server (FS-01, Windows Server 2022); Microsoft 365 GCC High (Exchange Online, SharePoint, Teams)	CUI file shares on FS-01 are accessible only to Active Directory security groups defined in the Access Control Matrix (ACM-001). SharePoint GCC High sites containing CUI are restricted to explicitly authorized users. Access is granted based on the principle of least privilege and requires system owner approval. Access is reviewed quarterly by the ISSO using AD group membership reports.	IT Administrator / ISSO
3.8.3	Sanitize or destroy system media before disposal or reuse.	**Implemented**	All in-scope systems	All media sanitization follows NIST SP 800-88 Rev 1 procedures documented in MSP-001. SSDs and flash media are purged using manufacturer-provided Secure Erase commands. HDDs are wiped using DBAN (DoD 5220.22-M standard). Physical destruction is used for failed or unrecoverable media. All sanitization	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				events are recorded on the Media Sanitization Record (MSR-001) with method, date, and witness signature.	
3.8.4	Mark media with necessary CUI markings and distribution limitations.	**Implemented**	All in-scope systems	Physical media and documents containing CUI are labeled with the appropriate CUI designation (CUI//SP-CTI for Controlled Technical Information) per NARA CUI guidance and the company CUI Marking Policy (CMP-002). Digital files stored on FS-01 are organized in folders named with CUI designations. Email containing CUI in M365 GCC High is labeled using Microsoft Purview sensitivity labels ('CUI - Controlled Technical Information').	All CUI Handlers
3.8.5	Control access to media containing CUI and maintain accountability during transport.	**Implemented**	All in-scope systems	Transport of physical CUI media is governed by the CUI Transport Policy (CTP-001). Physical media is transported in sealed, opaque containers with tamper-evident tape. Courier and overnight carrier shipments use tracked services with chain of custody documentation. Electronic transmission of CUI uses only approved encrypted channels (SharePoint GCC High, M365 encrypted email). Hand-carried media requires ISSO authorization.	ISSO / All CUI Handlers
3.8.6	Implement cryptographic mechanisms to protect CUI during transport unless otherwise protected by physical safeguards.	**Implemented**	Microsoft 365 GCC High (Exchange Online, SharePoint, Teams);	All CUI transmitted electronically is protected by TLS 1.2 or higher. M365 GCC High enforces TLS for all email transmission; opportunistic TLS is	IT Administrator / ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
			FortiGate SSL VPN	required with fallback blocking for CUI-labeled emails. File transfers to external parties use SharePoint GCC High secure sharing links with expiration dates and recipient-specific access. Unencrypted email transmission of CUI is blocked by DLP policies.	
3.8.7	Control the use of removable media on system components.	**Implemented**	Windows 11 Workstations (WS-01 through WS-12)	USB removable storage devices are blocked on all CUI workstations via GPO (GPO-SEC-005). The GPO uses device class restrictions to block storage devices while permitting HID devices (keyboard, mouse) and smart card readers. Any authorized exception requires written ISSO approval, is configured as a time-limited GPO exception, and is logged. No authorized exceptions are currently active.	IT Administrator
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	**Not Applicable**	N/A	USB removable storage is prohibited entirely on all CUI systems (see 3.8.7), making this practice fully satisfied through the more restrictive control already implemented. No portable storage devices are permitted on CUI workstations regardless of ownership identification.	IT Administrator
3.8.9	Protect the confidentiality of backup CUI at storage locations.	**Implemented**	Veeam Backup; Azure GCC High	System backups are managed by Veeam Backup and Replication. Backup jobs are encrypted with AES-256 using keys stored in the Veeam encryption key manager. Backup files on-site are stored on an isolated NAS (NAS-01) in the locked server room. Off-site backups are replicated to Azure GCC High Blob Storage with	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				server-side encryption and immutability policies enabled. Backup encryption keys are stored separately from backup media.	

4.9 PS — Personnel Security (3.9.x, 2 Practices)

Cogswell Cogs conducts pre-employment background checks on all personnel who will access CUI. Offboarding procedures are documented in the HR Separation Checklist (HSC-001) and require same-day account disablement for involuntary terminations.

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	**Implemented**	All in-scope systems	Pre-employment screening for CUI-authorized positions includes: criminal background check (7-year felony search), identity verification, and employment history verification. Screening is performed by Checkr (third-party screening provider) under a signed Business Associate Agreement. Personnel Security Policy (PSP-001) defines screening requirements by role. IT Administrator and ISSO positions require additional federal criminal background check. No individual is granted CUI access until screening is complete.	HR / System Owner
3.9.2	Ensure that CUI is protected during and after personnel actions such as terminations and transfers.	**Implemented**	All in-scope systems	The HR Separation Checklist (HSC-001) governs all CUI-access terminations and transfers. For involuntary	HR / IT Administrator / ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				terminations, IT Administrator disables AD accounts and revokes VPN access within 2 hours of notification. For planned terminations, access is revoked on the last day of employment. All company-issued equipment is collected before final departure. CUI materials (including physical documents) are returned and inventoried. Transfer procedures require access re-authorization for the new role before prior access is revoked.	

4.10 PE — Physical Protection (3.10.x, 6 Practices)

Cogswell Cogs operates from a single facility at 742 Skypad Boulevard, Orbit City, CA. Physical access to the facility is controlled by keycard (HID ProxKey4). The server room requires a separate keycard and is accessible only to the IT Administrator and ISSO. Visitor access requires sign-in and escort.

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.10.1	Limit physical access to organizational systems to authorized individuals.	**Implemented**	HID Access Control System; Server Room	Physical access to the main facility is controlled by HID keycard readers at all entry points. Keycard access to the server room is restricted to the IT Administrator and ISSO. Access rights are provisioned in the HID ProxPoint system by the IT Administrator. Access rights are reviewed quarterly. All keycard assignments are documented in the	IT Administrator / Facilities Manager

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				Physical Access Register (PAR-002). Lost or stolen keycards are revoked within 2 hours of report.	
3.10.2	Protect and monitor the physical facility and support infrastructure.	**Implemented**	Verkada Security Cameras; Facility Management	Facility is protected by Verkada security cameras at all entry/exit points and in the server room. Camera footage is retained for 30 days. The engineering area (where CUI workstations are located) has motion-activated cameras. Uninterruptible power supplies (APC SmartUPS) protect all CUI servers and network equipment. The server room has a dedicated HVAC unit with temperature monitoring alerts configured to notify the IT Administrator.	IT Administrator / Facilities Manager
3.10.3	Escort visitors and monitor visitor activity.	**Implemented**	Visitor Management System (VMS-01)	All visitors are required to sign in at reception using the paper Visitor Log (VL-001) recording: visitor name, organization, purpose, host employee, escort identity, time in and time out. Visitors are escorted at all times while on premises. Visitors are never left unattended in areas where CUI systems or materials are present. Visitor badges are color-coded to distinguish from employee badges. Visitor logs are retained for 12 months.	All Employees / Facilities Manager
3.10.4	Maintain audit logs of physical access.	**Implemented**	HID Access Control System	HID access control system maintains electronic audit logs of all keycard access events (entry, exit, failed access attempts). Logs are retained in the HID system for 12 months. The IT Administrator reviews access logs	IT Administrator / ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				weekly for anomalies (after-hours access, repeated failures, access by terminated employee credentials). Monthly access review reports are provided to the ISSO.	
3.10.5	Control and manage physical access devices.	**Implemented**	HID Access Control System	Physical access devices (keycards) are issued to employees upon completion of background check and access authorization. All keycard issuances are documented in PAR-002. Lost or stolen keycards are reported immediately and revoked within 2 hours. Keycards are collected during the offboarding process (HSC-001). An inventory of all issued access devices is maintained and reconciled quarterly.	IT Administrator / Facilities Manager
3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	**Implemented**	Microsoft Intune (MDM); Remote Worker Policy	Remote workers handling CUI are governed by the Remote Work Policy (RWP-001). Requirements include: dedicated workspace without cohabitant access during CUI work, use of company-issued encrypted laptop only, VPN connection required before accessing any CUI, privacy screen filter required in public locations, physical CUI documents prohibited at home (electronic access only). Remote workers acknowledge RWP-001 annually. MDM compliance policies verify encryption and VPN usage.	ISSO / HR

4.11 RA — Risk Assessment (3.11.x, 3 Practices)

Cogswell Cogs conducts an annual risk assessment using the NIST SP 800-30 Rev 1 methodology. Vulnerability scanning is performed monthly using Tenable Nessus Essentials and quarterly by an external party (Koran & Associates). Remediation timelines are defined in the Vulnerability Management Policy (VMP-001).

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.11.1	Periodically assess the risk to organizational operations, assets, and individuals from operation of organizational systems.	**Implemented**	All in-scope systems	Risk Assessment RA-2025-001 was completed June 10, 2025 using the NIST SP 800-30 Rev 1 methodology, covering all 14 NIST SP 800-171 practice families, the physical environment, and the M365 GCC High and Azure GCC High cloud environments. The assessment incorporated the FortiGate VPN upgrade (December 2024) and Endpoint DLP deployment completed May 2025. Koran & Associates performed an independent review of RA-2025-001 in July 2025. The next annual risk assessment is due no later than August 31, 2026, and is pre-calendared by the ISSO. Risk findings and treatment decisions are documented in RA-2025-001 and are reflected in the current POA&M.	ISSO
3.11.2	Scan for vulnerabilities in organizational systems periodically and when new vulnerabilities are identified.	**Implemented**	All in-scope systems; Tenable Nessus	Tenable Nessus Essentials performs authenticated vulnerability scans of all in-scope systems monthly (first Sunday of each month). Unauthenticated scans are performed weekly via a scheduled Nessus scan task. Koran & Associates performs an external penetration test	IT Administrator / ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				and vulnerability assessment quarterly. Scan results are reviewed within 5 business days by the IT Administrator. CISA KEV alerts trigger ad hoc scans within 48 hours.	
3.11.3	Remediate vulnerabilities in accordance with risk assessments.	**Implemented**	All in-scope systems	Vulnerability remediation timelines are defined in VMP-001: Critical (CVSS 9.0+) within 15 days, High (CVSS 7.0-8.9) within 30 days, Medium (CVSS 4.0-6.9) within 90 days. Remediation is tracked in the Vulnerability Tracking Register (VTR-001) in SharePoint GCC High. Exceptions require written ISSO approval and a POA&M entry. Tenable scan trending confirms remediation completion. No unmitigated Critical findings are currently open.	IT Administrator / ISSO

4.12 CA — Security Assessment (3.12.x, 4 Practices)

Cogswell Cogs maintains this SSP as the primary governance document for its CMMC Level 2 compliance program. Security controls are assessed annually through internal review and by an external consultant. All deficiencies are tracked in the POA&M.

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective.	**Implemented**	All in-scope systems	Annual internal security control assessment SCA-2025-001 was completed December 5, 2025, using NIST SP 800-171A assessment	ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				procedures. The assessment covered all 110 practices and identified one partially implemented practice (3.13.12 — Teams enforcement-mode policy pending). All prior 2024 deficiencies (3.1.3, 3.3.5, 3.4.8, 3.11.1) were verified as remediated and closed. Koran & Associates performed an independent review of SCA-2025-001 in January 2026 and confirmed the findings. The next annual assessment (SCA-2026-001) is scheduled for November 2026.	
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities.	**Implemented**	SharePoint GCC High (POA&M)	The POA&M (POAM-001) is maintained in SharePoint GCC High and updated at least quarterly. Each POA&M entry includes: practice ID, deficiency description, planned completion date, milestone steps, resource requirements, and responsible party. The ISSO reviews the POA&M monthly and reports status to the system owner. CMMC Phase 1 enforcement has elevated POA&M completion to a board-level priority. Current open items: 4 practices (see Section 5).	ISSO / System Owner
3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	**Implemented**	All in-scope systems; SIEM-01	Ongoing monitoring activities are defined in the Continuous Monitoring Plan (CMP-003): daily SIEM alert review, weekly access and VPN log review, monthly patch compliance and vulnerability scan, quarterly access recertification and	ISSO / IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				backup restoration test, semi-annual firewall rule review, and annual full security control assessment. Monitoring activity completion is tracked in a monitoring log maintained by the ISSO.	
3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and relationships with or connections to other systems.	**Implemented**	All in-scope systems	This document (SSP-001, Version 3.0, dated March 20, 2026) constitutes the SSP for the Cogswell Cogs CUI Processing Environment. The SSP is reviewed annually and updated following any significant system change, security incident, or personnel change affecting system roles. The SSP was last reviewed by the System Owner and ISSO on March 20, 2026. It is maintained in SharePoint GCC High with full version history and is provided to Koran & Associates for independent annual review.	ISSO / System Owner

4.13 SC — System and Communications Protection (3.13.x, 16 Practices)

Cogswell Cogs employs a defense-in-depth network architecture with perimeter protection (SonicWall TZ570), network segmentation (CUI VLAN, guest VLAN), and encrypted communications for all CUI data in transit. FIPS 140-2 mode is enabled on all Windows systems. M365 GCC High provides FIPS-compliant encryption for cloud-hosted CUI.

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.13.1	Monitor, control, and protect communications at the external boundaries and key internal boundaries of organizational systems.	**Implemented**	SonicWall TZ570 Firewall; Windows 11 Workstations + SonicWall TZ570	Perimeter protection is provided by SonicWall TZ570 in stateful inspection mode with deep packet inspection, intrusion prevention (IPS), gateway antivirus, and application control enabled. Firewall rules enforce a default-deny posture with explicit allow exceptions documented in FRR-001. Internal boundary protection between the CUI VLAN and general VLAN is enforced by VLAN ACLs on the Cisco managed switch. Firewall logs are forwarded to SIEM-01.	IT Administrator
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security.	**Implemented**	All in-scope systems	Cogswell Cogs does not develop custom software. System architecture follows security-by-design principles documented in the System Architecture Document (SAD-001): network segmentation by function and data classification, least functionality on all systems, encrypted storage and transmission for CUI, defense-in-depth layering (perimeter firewall, host-based firewall, endpoint protection, SIEM), and documented system boundaries.	IT Administrator / ISSO
3.13.3	Separate user functionality from system management functionality.	**Implemented**	Active Directory Domain Controller (DC-01); Windows 11 Workstations (WS-01 through WS-12)	User and administrative functions are separated through distinct user accounts (standard vs. admin), separate workstation profiles, and GPO enforcement. Administrative tools (Active Directory Users and Computers, Server Manager, Wazuh console) are accessible only through admin-level	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				accounts. Standard user workstation environments do not display or permit access to system management utilities.	
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	**Implemented**	Windows 11 Workstations (WS-01 through WS-12); File Server (FS-01, Windows Server 2022)	Object reuse is addressed through Windows NTFS file permissions preventing cross-user data access in shared directories. Memory is cleared on system restart per Windows default behavior. CUI file shares are not accessible from the guest network VLAN. Shared printers that may process CUI documents are located in the secured engineering area. Print logs are retained by the print server.	IT Administrator
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	**Implemented**	Cisco SG350-28 Managed Switch; SonicWall TZ570	Network architecture implements four VLANs: VLAN 10 (CUI Processing, 192.168.10.0/24), VLAN 20 (General Corporate, 192.168.20.0/24), VLAN 30 (Guest/DMZ, 192.168.30.0/24), VLAN 40 (Management, 192.168.40.0/24). VLAN segregation is enforced by the Cisco SG350-28 managed switch. Inter-VLAN routing is controlled by firewall ACLs. Guest VLAN has no path to CUI or corporate VLANs.	IT Administrator
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception.	**Implemented**	SonicWall TZ570 Firewall	SonicWall TZ570 perimeter firewall and internal VLAN ACLs implement default-deny on all traffic with explicit permit rules for business-required communications. Inbound traffic is denied by default; outbound traffic is filtered by the SonicWall Application	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				Control and Content Filtering modules. Approved exceptions are documented in the Firewall Rule Register (FRR-001) with business justification, approver, and review date.	
3.13.7	Prevent remote devices from simultaneously connecting to the system and to resources in other domains (split tunneling).	**Implemented**	FortiGate SSL VPN	FortiGate SSL VPN is configured to disable split tunneling for all CUI remote access profiles. All remote device traffic is routed through the VPN gateway during active sessions. Configuration is enforced via FortiGate SSL VPN policy settings and verified in the VPN Configuration Baseline (SCB-VPN-001). Quarterly VPN configuration reviews confirm the split tunneling prohibition remains in effect.	IT Administrator
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission.	**Implemented**	All in-scope systems; Microsoft 365 GCC High (Exchange Online, SharePoint, Teams)	All CUI data in transit is encrypted using TLS 1.2 or higher. M365 GCC High enforces TLS 1.2+ for all communications. SharePoint GCC High secure links use HTTPS with TLS 1.2+. VPN uses TLS 1.2 with AES-256-GCM. Internal SMB file share traffic between workstations and FS-01 uses SMB 3.1.1 with AES-128-GCM encryption. SMBv1 is disabled. Cryptographic standards are documented in the Encryption Standard (ECS-001).	IT Administrator
3.13.9	Terminate network connections after a defined period of inactivity.	**Implemented**	FortiGate SSL VPN; Microsoft 365 GCC High (Exchange Online,	FortiGate VPN sessions terminate after 60 minutes of inactivity (hard timeout: 8 hours). M365 GCC High Conditional Access policy (CAP-003) enforces a	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
			SharePoint, Teams)	session lifetime of 8 hours with a 60-minute sign-in frequency for CUI-access applications. Windows workstation sessions lock after 15 minutes and require re-authentication. Network connections to FS-01 SMB shares time out after 30 minutes of inactivity via server-side timeout settings.	
3.13.10	Establish and manage cryptographic keys for required cryptography employed in organizational systems.	**Implemented**	Microsoft 365 GCC High (Exchange Online, SharePoint, Teams); Veeam Backup	Cryptographic key management is documented in the Key Management Policy (KMP-001). Microsoft-managed keys are used for M365 GCC High encryption (BYOK is not currently implemented; assessed as proportionate risk for company size). Veeam backup encryption keys are stored in the Veeam Key Management module, separately from backup data, with access limited to the IT Administrator. BitLocker recovery keys are stored in Active Directory (AD DS key backup). Key custodian is the IT Administrator.	IT Administrator / ISSO
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	**Implemented**	All in-scope systems	Windows FIPS mode is enabled on all in-scope systems via GPO (GPO-SEC-006), enforcing the 'System cryptography: Use FIPS compliant algorithms' Group Policy setting. M365 GCC High uses FIPS 140-2 validated cryptographic modules (Microsoft CMVP Certificate #3196). FortiGate firmware cryptographic modules are FIPS 140-2 compliant by design; the specific CMVP validation	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				certificate number for the deployed firmware version (7.4.x) must be confirmed against the NIST CMVP Active Certificates list at csrc.nist.gov/projects/cryptographic-module-validation-program before the C3PAO assessment and documented as an evidence artifact. Until that certificate number is on file, this practice is treated as implemented with a pending evidence task. FIPS compliance across all components is reviewed quarterly and documented in ECS-001.	
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of use to present users.	**Partially Implemented**	Microsoft Teams (M365 GCC High); Conference Room Poly Studio Devices	PARTIALLY IMPLEMENTED. Physical privacy covers have been installed on all Poly Studio conference room cameras (completed August 2025) as the primary compensating control. Microsoft Teams admin policy to prevent remote activation of microphones and cameras via the Teams Admin Center is configured in audit mode (September 2025) and is pending enforcement-mode deployment following compatibility testing with scheduled Teams Phone firmware updates. A POA&M entry captures full enforcement-mode deployment as a Q2 2026 deliverable. Physical covers satisfy the 'indication of use' requirement per NIST SP 800-171A assessment guidance; the Teams policy enforcement gap remains an open item. Note: per 32 CFR Part	ISSO / IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				170, POA&M items accepted at the time of C3PAO assessment must be remediated within 180 days of the assessment date.	
3.13.13	Control and monitor the use of mobile code.	**Implemented**	Windows 11 Workstations (WS-01 through WS-12); Microsoft 365 GCC High (Exchange Online, SharePoint, Teams)	JavaScript and active content execution in web browsers is controlled through Microsoft Edge policies deployed via Intune (managed browser settings). Microsoft Defender for Endpoint provides mobile code (macro, script) execution monitoring on workstations. Office macro execution is restricted to digitally signed macros only via Intune policy. No unsigned scripts are permitted to execute on CUI workstations. Mobile code events are logged to SIEM-01.	IT Administrator
3.13.14	Control and monitor the use of VoIP technologies.	**Implemented**	Microsoft 365 GCC High (Exchange Online, SharePoint, Teams); Microsoft Teams Phone	VoIP services are provided through Microsoft Teams Phone (M365 GCC High), which is the sole authorized VoIP platform. Third-party VoIP applications (Zoom Phone, RingCentral, etc.) are blocked by the SonicWall application control policy. Teams Phone call logs are retained in the M365 GCC High compliance center. Teams administrative controls prohibit unauthenticated guest calling. Reviewed and documented in Communications Security Policy (CSP-001).	IT Administrator
3.13.15	Protect the authenticity of communications sessions.	**Implemented**	All in-scope systems; Microsoft 365 GCC High (Exchange	Session authenticity is protected through TLS with mutual authentication where supported, SAML 2.0	IT Administrator

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
			Online, SharePoint, Teams)	tokens for application access via Entra ID, and Kerberos for domain authentication. HTTPS is enforced for all internal web applications. HTTP Strict Transport Security (HSTS) is enabled on the VPN web portal. Certificate validity is monitored by the IT Administrator; expired certificates trigger automated alerts via Entra ID.	
3.13.16	Protect the confidentiality of CUI at rest.	**Implemented**	Windows 11 Workstations (WS-01 through WS-12); File Server (FS-01, Windows Server 2022); Microsoft 365 GCC High (Exchange Online, SharePoint, Teams)	CUI at rest is protected by: BitLocker (AES-256) on all workstation and server system volumes and data drives; SMB encryption on FS-01 file shares; Microsoft GCC High encryption at rest for SharePoint, Exchange, and Teams; AES-256 encryption on Veeam backup files; NTFS encrypted file system (EFS) on selected high-sensitivity CUI directories. Encryption status is monitored via Intune compliance reports and BitLocker recovery key audit in AD.	IT Administrator

4.14 SI — System and Information Integrity (3.14.x, 7 Practices)

Cogswell Cogs deploys Microsoft Defender for Endpoint (MDE) as the primary endpoint protection platform across all in-scope workstations and servers, managed centrally through the Microsoft Defender portal in GCC High. Patch management follows a monthly cycle using Windows Server Update Services (WSUS).

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
3.14.1	Identify, report, and correct information and system flaws in a timely manner.	**Implemented**	All in-scope systems; WSUS	Patch management is executed monthly via Windows Server Update Services (WSUS). Critical patches (CVSS 9.0+) and CISA Known Exploited Vulnerabilities (KEV) are deployed within 15 days. Standard patches deploy within 30 days on a monthly Patch Tuesday cycle. Patch compliance reporting is generated monthly by WSUS and verified by Nessus scan delta analysis. Patch exceptions require ISSO approval and a POA&M entry. Current patch compliance: 97% (3 workstations pending reboot).	IT Administrator
3.14.2	Provide protection from malicious code at appropriate locations within organizational systems.	**Implemented**	All in-scope systems; Microsoft Defender for Endpoint	Microsoft Defender for Endpoint (MDE) Plan 2 is deployed on all workstations and servers, managed through the GCC High Microsoft Defender portal. Real-time protection, cloud-delivered protection, and automatic sample submission are enabled. MDE provides endpoint detection and response (EDR) capabilities. SonicWall gateway antivirus scans all inbound and outbound traffic at the perimeter. M365 GCC High Defender for Office 365 provides email attachment scanning.	IT Administrator
3.14.3	Monitor system security alerts and advisories and take action in response.	**Implemented**	SIEM-01; Microsoft Defender Portal	The IT Administrator monitors SIEM-01 (Wazuh) alerts daily and the Microsoft Defender portal weekly for endpoint security alerts. The ISSO subscribes to CISA alerts (US-CERT), Microsoft Security Response Center (MSRC) bulletins, and the DIBNet	IT Administrator / ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
				Cyber Advisories distribution list. Alert response procedures are documented in the Security Alert Response Procedure (SARP-001). Priority 1 alerts require ISSO notification within 1 hour.	
3.14.4	Update malicious code protection mechanisms when new releases are available.	**Implemented**	Windows 11 Workstations (WS-01 through WS-12); Microsoft Defender for Endpoint	Microsoft Defender for Endpoint definition updates are delivered automatically from Microsoft's cloud (multiple times daily). Update delivery is verified through the MDE portal; devices with outdated definitions (>24 hours) generate a compliance alert. Engine and platform updates are managed through WSUS monthly cycle or pushed on-demand for critical updates. Definition update compliance is included in the monthly patch compliance report.	IT Administrator
3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources.	**Implemented**	Windows 11 Workstations (WS-01 through WS-12); Microsoft Defender for Endpoint	Microsoft Defender for Endpoint performs real-time scanning on all file operations. Weekly full system scans are scheduled via MDE policy on all workstations and servers (Sunday 2:00 AM). Files downloaded from the internet or received via email are scanned before execution (enforced by Defender SmartScreen and Defender for Office 365). Removable media scanning is enabled but USB storage is prohibited (3.8.7), effectively eliminating the primary external file introduction vector.	IT Administrator
3.14.6	Monitor organizational systems, including inbound and outbound	**Implemented**	SIEM-01; SonicWall TZ570	Network traffic monitoring is provided by SonicWall IPS,	IT Administrator / ISSO

Practice	Requirement	Status	System Component	Implementation Description	Responsible Role
	communications traffic, to detect attacks and indicators of potential attacks.		Firewall; Microsoft Defender for Endpoint	application control, and threat intelligence feeds. SIEM-01 (Wazuh) ingests and correlates firewall logs, Windows Security events, and MDE alerts. Microsoft Defender for Endpoint provides network-level threat detection on endpoints (network protection enabled). Monthly threat hunt reviews examine SIEM-01 telemetry for indicators of compromise (IOCs) using CISA-published IOC lists. Findings are documented in monthly security review records.	
3.14.7	Identify unauthorized use of organizational systems.	**Implemented**	SIEM-01; Active Directory Domain Controller (DC-01)	Unauthorized use detection is implemented through SIEM-01 correlation rules that alert on: logon outside business hours, multiple failed logon attempts, access to CUI shares by accounts not in authorized groups, VPN access from unexpected geographic locations, and USB device insertion attempts (blocked but logged). User behavior baselines were established during initial SIEM deployment. Alerts are reviewed by the ISSO and IT Administrator and investigated per SARP-001.	ISSO / IT Administrator

5. Plan of Action and Milestones (POA&M Summary)

The table below summarizes all open deficiencies identified in this SSP. Four items from the 2024 assessment cycle (3.1.3, 3.3.5, 3.4.8, and 3.11.1) were remediated and closed in 2025. One item remains open. The full POA&M (POAM-001) is maintained in SharePoint GCC High with complete milestone detail, resource assignments, and progress tracking. The ISSO reviews the POA&M monthly and reports status to the System Owner quarterly.

Practice	Deficiency	Current Status	Target Completion	Responsible Party	Milestones
3.13.12	Teams admin policy not yet in enforcement mode. Physical camera covers on Poly Studio conference room units were installed August 2025 (compensating control). Teams Admin Center policy is currently in audit mode pending firmware compatibility testing.	**Partially Implemented**	June 30, 2026	IT Admin / ISSO	M1 (Apr 2026): Complete Teams Phone firmware compatibility testing. M2 (May 2026): Enable enforcement-mode camera/microphone policy in Teams Admin Center. M3 (Jun 2026): Verify policy enforcement across all conference room devices and document closure. NOTE: Per 32 CFR Part 170, this item must be remediated within 180 days of the C3PAO assessment date or it will constitute a finding that prevents certification.

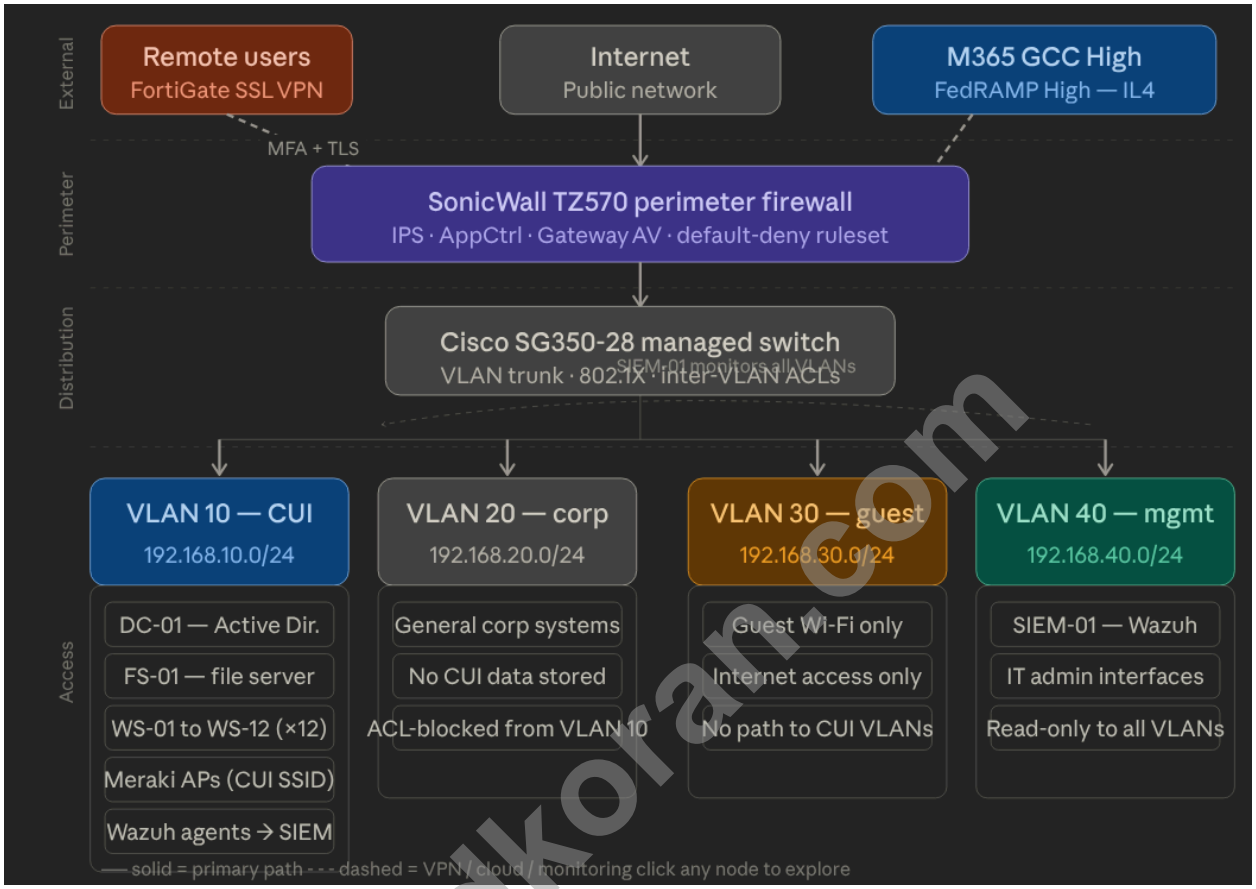
6. Document Review and Approval

Review Date	Reviewer	Version	Changes
March 20, 2026	M. Cogswell (ISSO) / V. Cogswell (System Owner)	3.0	Annual review. Updated SPRS score to 107 (January 15, 2026 submission). Closed POA&M items 3.1.3, 3.3.5, 3.4.8, and 3.11.1 as remediated. Updated 3.13.12 status to Partially Implemented; POA&M target extended to June 30, 2026. Updated 3.13.11 to require CMVP certificate verification. Updated 3.6.2 with explicit 72-hour reporting language. Refreshed asset inventory audit date (February 28, 2026). Added RA-2025-001 reference. Incorporated SCA-2025-001 findings.
December 5, 2025	M. Cogswell (ISSO)	2.3	Completed SCA-2025-001 internal assessment. Verified closure of 3.1.3 (Endpoint DLP fully deployed May 2025), 3.3.5 (M365 correlation rules active April 2025), 3.4.8 (AppLocker deployed to servers August 2025), and 3.11.1 (RA-2025-001 completed June 2025). Updated 3.13.12 POA&M milestone after physical camera covers installed August 2025.
March 20, 2025	M. Cogswell (ISSO) / V. Cogswell (System Owner)	2.1	Added 3.13.12 POA&M entry; updated SPRS score (89); updated cloud provider table to reflect Azure GCC High backup deployment; updated SIEM-01 log retention policy to reflect WORM archive.
November 1, 2024	M. Cogswell (ISSO)	2.0	Full annual review. Incorporated findings from SCA-2024-001. Added 3.3.5, 3.4.8, 3.11.1, and 3.1.3 POA&M entries. Updated IR plan reference to IRP-001 v2.
August 10, 2023	M. Cogswell (ISSO) / V. Cogswell (System Owner)	1.0	Initial SSP creation for CMMC Level 2 program. Authored by Koran & Associates; reviewed and approved by Cogswell Cogs ISSO and System Owner.

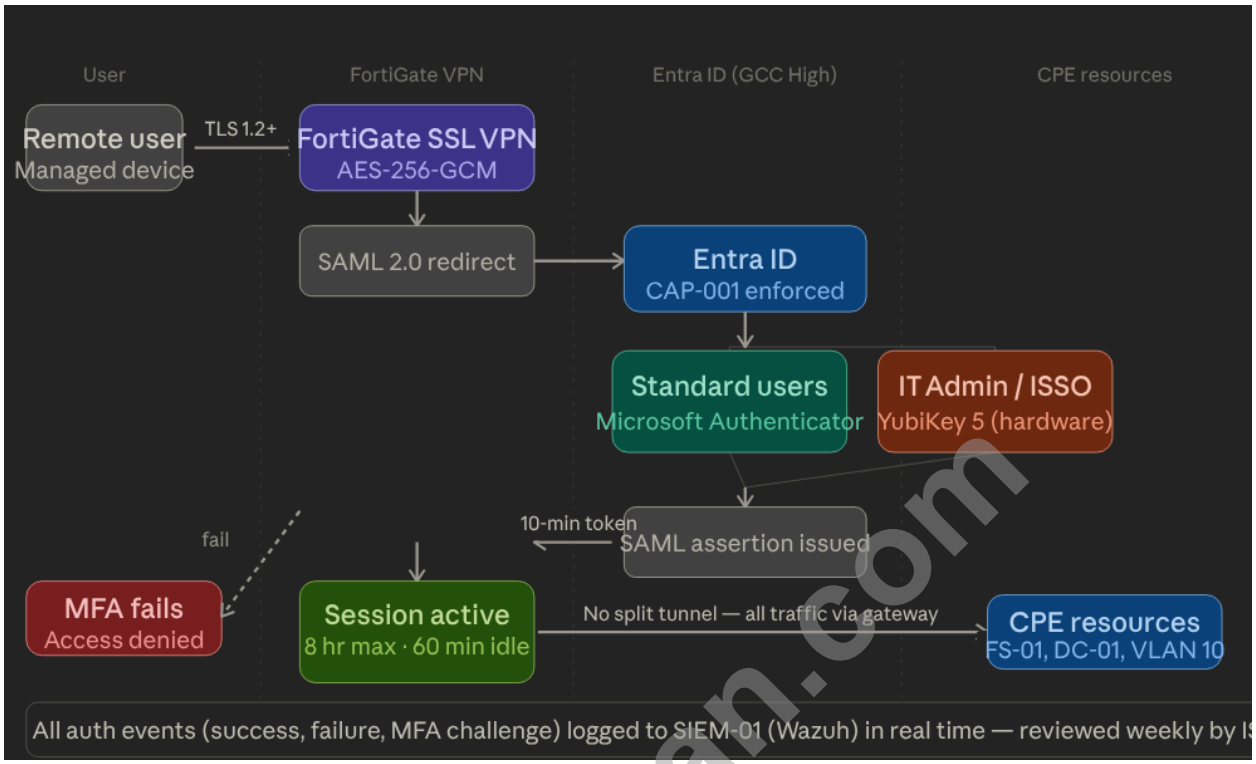
System Owner Authorization

System Owner Name	Victor Cogswell
Signature	
Title	Chief Executive Officer, Cogswell Cogs, Inc.
Date	March 20, 2026

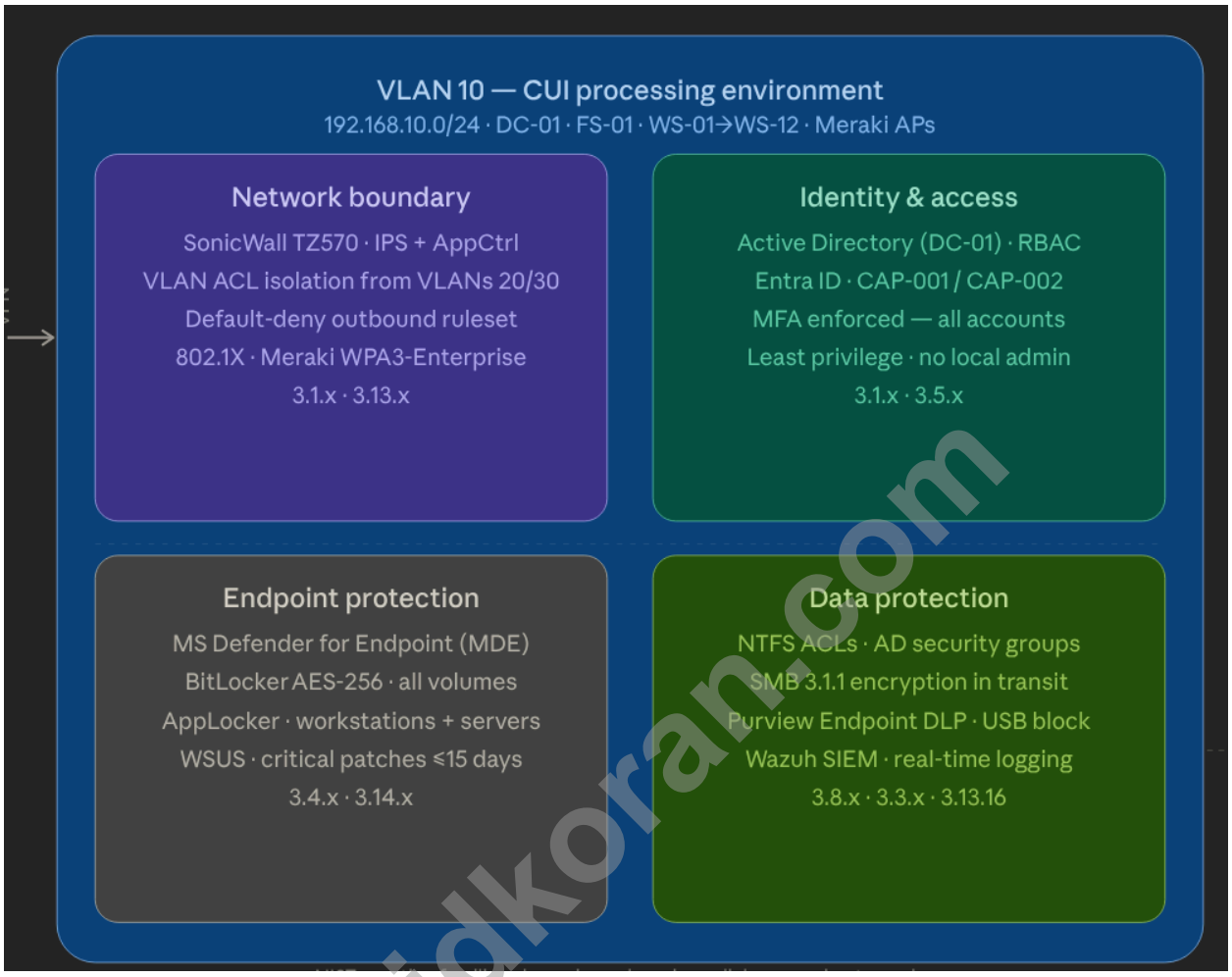
Network Topology



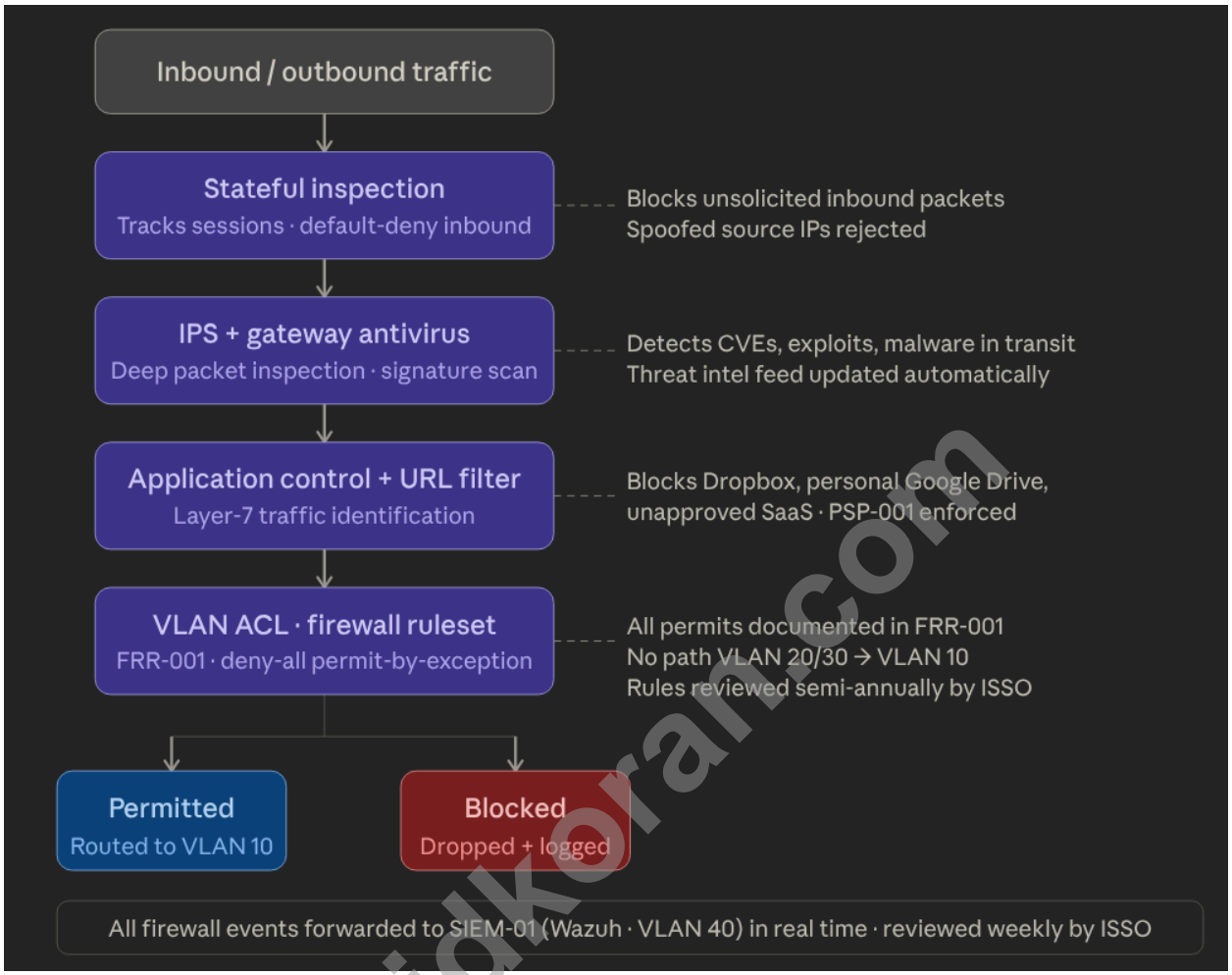
Authentication Chain



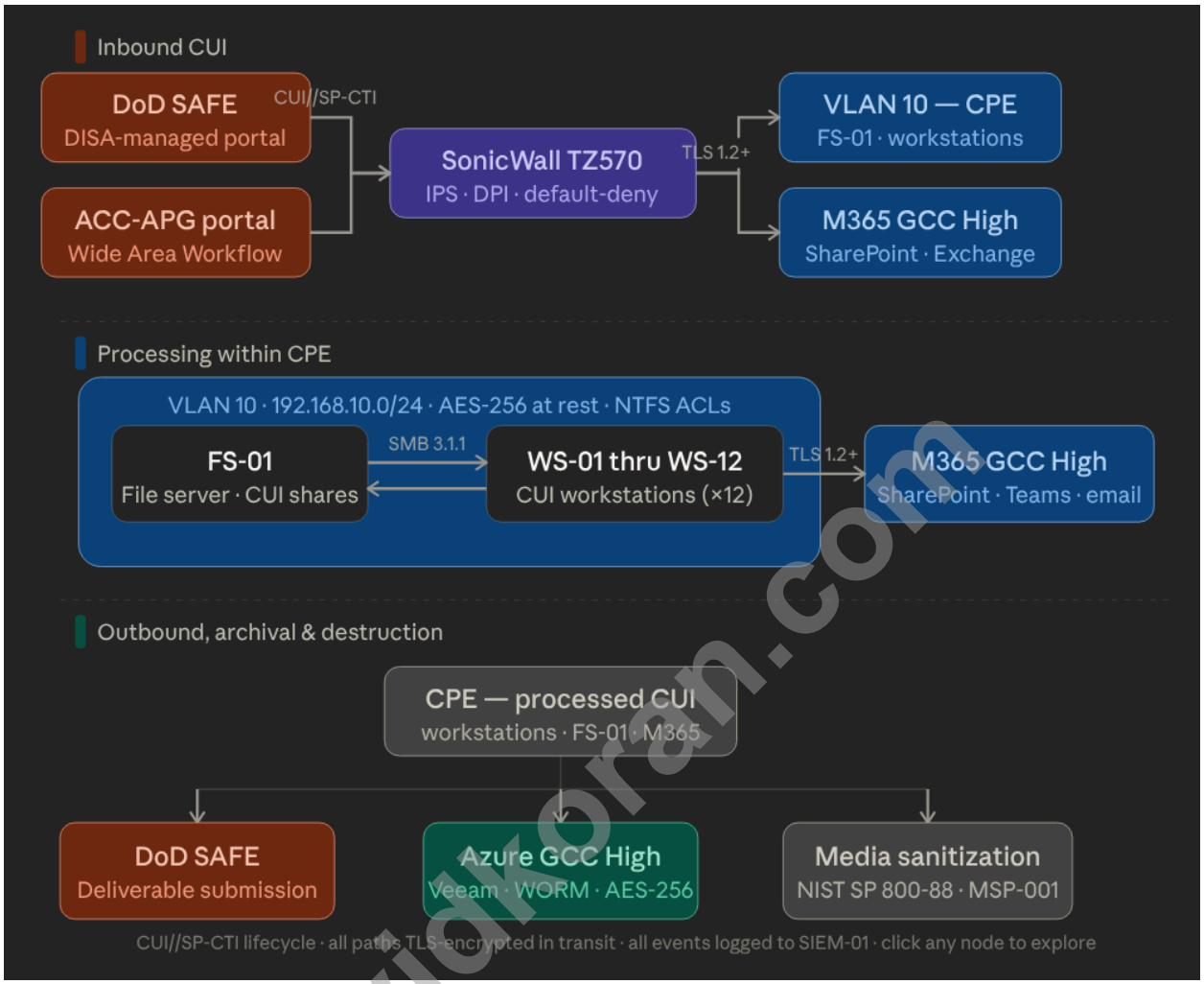
CUI Processing Environment Diagram



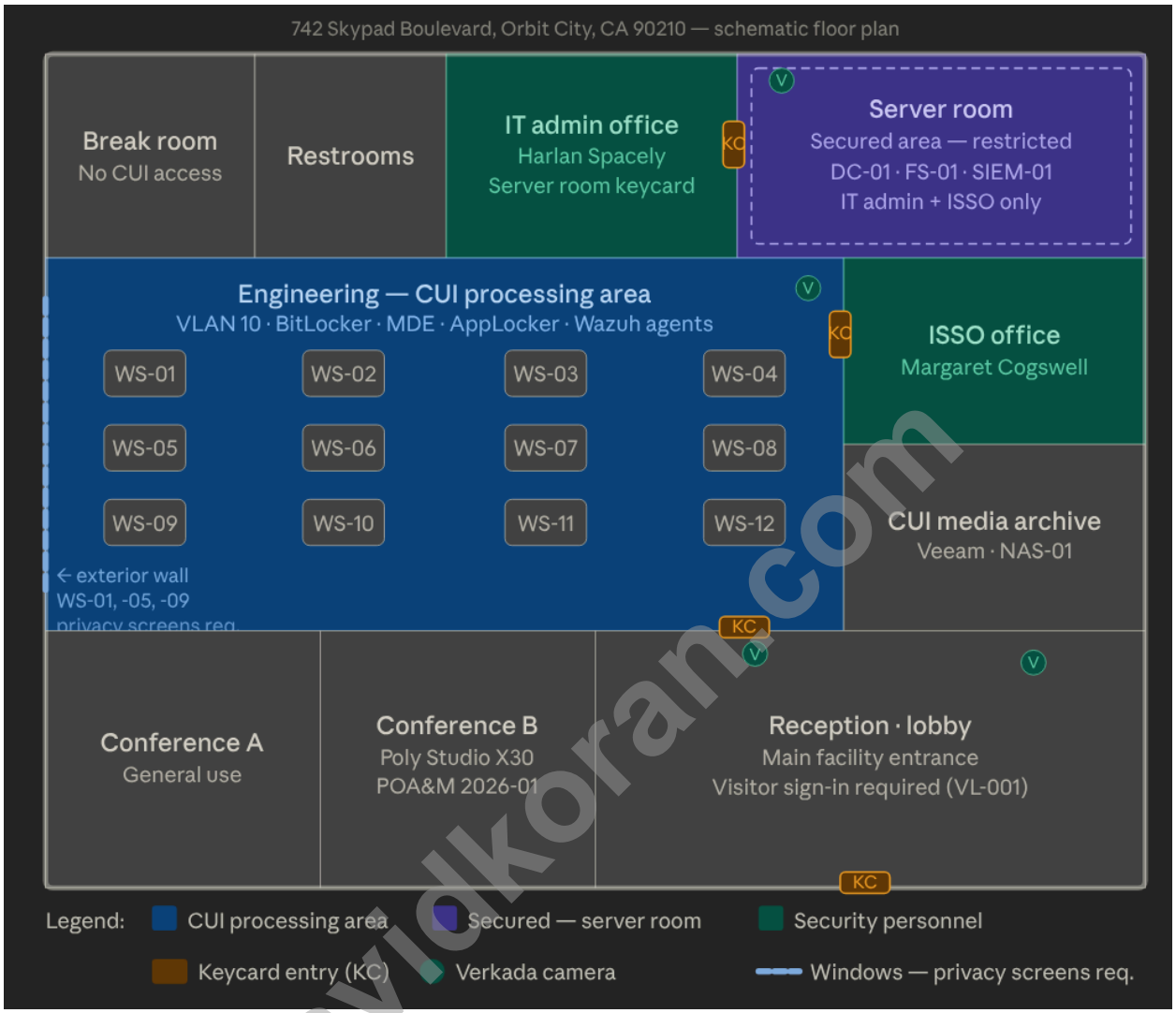
SonicWall TZ570 - packet inspection stack, VLAN 10 perimeter



CUI Flow



Floor Plan



Facility Security Parameter Layers

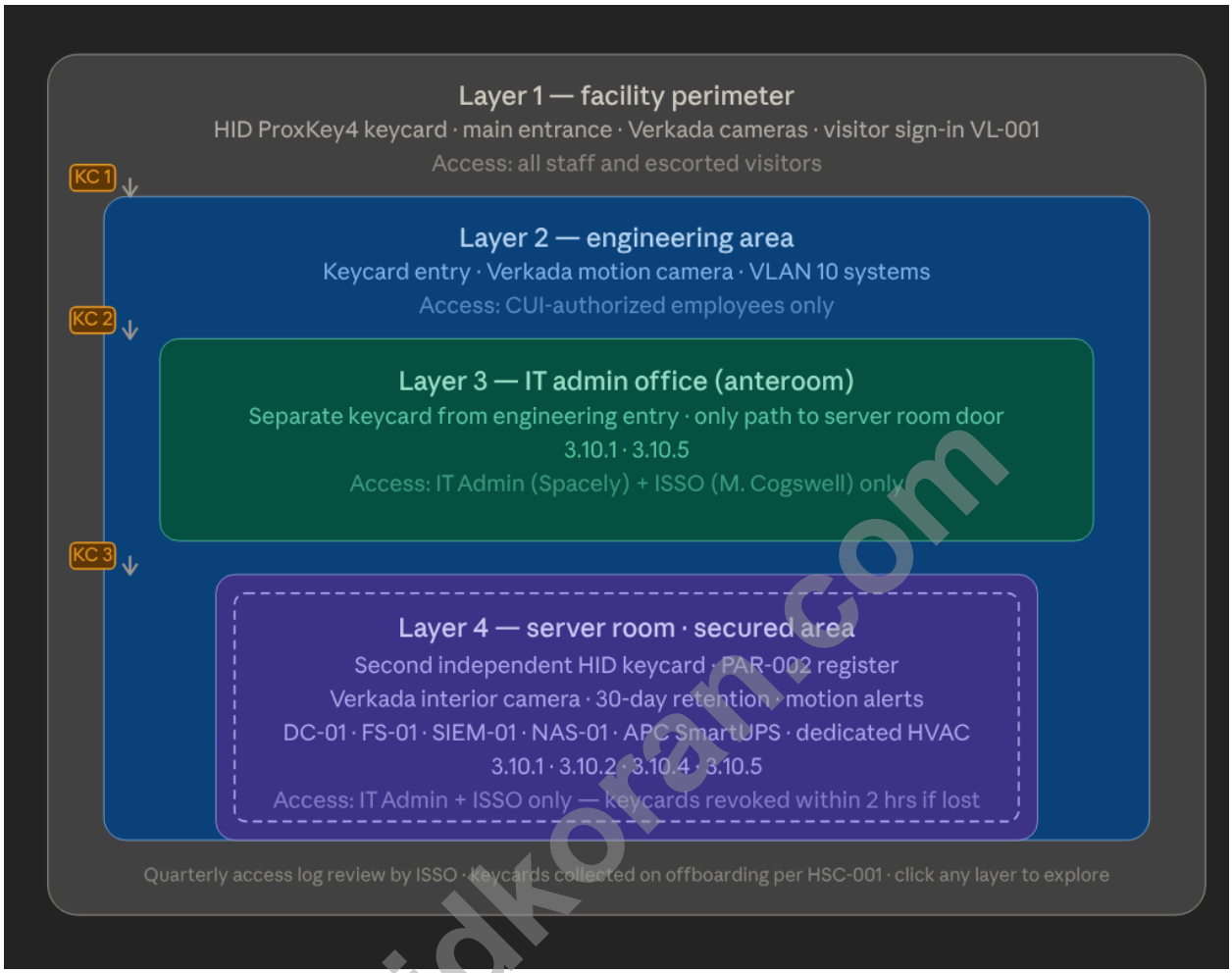


DIAGRAM-TO-SSP CROSSWALK

Cogswell Cogs, Inc. — CUI Processing Environment

CMMC Level 2 / NIST SP 800-171 Rev 2

SAD-001 Appendix — Evidence and Practice Mapping

Organization	Cogswell Cogs, Inc.
CAGE Code	7CG42
SSP Reference	SSP-001 v3.0 · POAM-001 v3.2
Prepared by	Margaret Cogswell, ISSO
Date	March 20, 2026
Total figures	8 (7 completed · 1 pending — Fig 8, Wazuh SIEM-01)

HANDLING NOTICE — CUI//SP-CTI. Handle per 32 CFR Part 2002.

1. Purpose and Scope

This Diagram-to-SSP Crosswalk maps each figure in the Cogswell Cogs System Architecture Document (SAD-001) to the specific NIST SP 800-171 Rev 2 practices it is intended to evidence. It is designed as a C3PAO assessment preparation tool: an assessor may use this crosswalk to identify which diagram to examine for a given practice, and Cogswell Cogs personnel may use it to confirm that every evidenced practice has a corresponding figure and named evidence artifact on file before the assessment begins.

Figures 1 through 7 are completed and available in SharePoint GCC High under the SAD-001 document set. Figure 8 (Wazuh SIEM-01 read-only configuration) is marked Partially Implemented and is the subject of a pre-assessment evidence task assigned to Harlan Spacely, IT Administrator. This task must be completed before the C3PAO assessment commences.

1.1 Status Key

Status	Meaning
Implemented	Figure is complete. Evidence artifacts are on file in SharePoint GCC High. Practice is evidenced and ready for C3PAO review.
Partially Implemented	Figure or evidence artifact is not yet complete. A pre-assessment task is assigned. Must be resolved before the C3PAO assessment date.

2. Diagram-to-Practice Crosswalk

The table below covers all eight figures. The Evidence Artifacts column lists the specific files or configuration exports an assessor will request when examining each practice. All completed artifacts are stored in SharePoint GCC High at the path: Compliance / SAD-001 / Evidence.

Figure	Title / Location	NIST Practices	What this diagram proves	Evidence artifacts required	Status
Fig 1	Network topology (SAD-001 App. A)	**3.1.1** — limit system access **3.1.3** — CUI flow control **3.13.1** — boundary protection **3.13.5** — network segmentation **3.13.6** — deny by default	Documents four VLAN segments (10/20/30/40), the SonicWall TZ570 perimeter firewall, Cisco SG350 managed switch, FortiGate VPN gateway, and Meraki wireless APs. Confirms VLAN 10 (CUI) is physically and logically isolated from VLANs 20, 30, and 40. Shows no routing path from guest or corporate VLANs to CUI systems.	• Network diagram (SAD-001) • Cisco SG350 VLAN config export • SonicWall ACL ruleset (FRR-001) • Inter-VLAN routing table	**Implemented**
Fig 2	FortiGate VPN auth flow (SAD-001 App. D)	**3.1.12** — monitor remote access **3.1.13** — encrypt remote access **3.1.14** — managed access points **3.5.3** — MFA for remote access **3.5.4** — replay-resistant auth **3.13.7** — no split tunneling	Documents the full SAML 2.0 handshake between FortiGate SSL VPN and Entra ID GCC High. Confirms MFA enforcement (Microsoft Authenticator for standard users; YubiKey 5 for IT Admin and ISSO). Confirms TLS 1.2+ with AES-256-GCM. Confirms split tunneling is disabled. Confirms 8-hour session hard timeout and 60-minute idle timeout.	• FortiGate VPN config baseline (SCB-VPN-001) • Entra ID CAP-001 screenshot • FortiGate session policy export • MFA enrollment report	**Implemented**
Fig 3	VLAN 10 defense layers	**3.1.1** — limit system access	Maps all four control layers protecting VLAN 10: network boundary	• AD group policy results	**Implemented**

Figure	Title / Location	NIST Practices	What this diagram proves	Evidence artifacts required	Status
	(SAD-001 App. E)	**3.1.5** — least privilege **3.4.2** — security config settings **3.5.3** — MFA enforcement **3.13.1** — boundary protection **3.13.16** — CUI at rest **3.14.2** — malware protection	(SonicWall IPS/AppCtrl, 802.1X), identity and access (Active Directory RBAC, Entra ID CAP-001/002, MFA), endpoint protection (MDE, BitLocker, AppLocker, WSUS), and data protection (NTFS ACLs, SMB 3.1.1, Purview DLP, Wazuh). Confirms every CUI system is covered by at least two independent control layers.	(GPO-SEC-001 through -006) • Intune compliance report • MDE device inventory • BitLocker recovery key audit (AD DS) • Nessus scan report	
Fig 4	SonicWall TZ570 inspection stack (SAD-001 App. F)	**3.13.1** — boundary protection **3.13.6** — deny by default **3.13.8** — encryption in transit **3.14.2** — malware protection **3.14.6** — monitor for attacks	Documents all four inspection layers in sequence: stateful inspection, IPS + gateway AV, application control + URL filtering (blocking Dropbox, personal Google Drive per PSP-001), and VLAN ACL firewall ruleset (FRR-001). Confirms default-deny posture. Confirms all events forwarded to SIEM-01 on VLAN 40. Establishes technical evidence for deny-all-permit-by-exception.	• SonicWall running configuration export • FRR-001 firewall rule register • SonicWall IPS signature update log • AppCtrl policy screenshot	**Implemented**
Fig 5	CUI data flow diagram (SAD-001 App. B)	**3.1.3** — CUI flow control **3.8.3** — media sanitization **3.8.5** — media transport **3.8.6** — encrypt in transit **3.8.9** — backup CUI **3.13.8** — encrypt in transit	Traces CUI lifecycle from inbound receipt (DoD SAFE, ACC-APG portal via TLS 1.2+) through internal processing (VLAN 10 NTFS ACLs, SMB 3.1.1, M365 GCC High SharePoint/Exchange) to outbound delivery (DoD SAFE submission), archival (Veeam to Azure GCC High WORM Blob Storage, AES-256), and destruction (NIST SP 800-88 MSP-001). Confirms CUI does not	• DLP policy config (Purview) • Veeam backup encryption config • Azure GCC High WORM policy screenshot • MSP-001 media sanitization records (MSR-001) • DoD SAFE transfer logs	**Implemented**

Figure	Title / Location	NIST Practices	What this diagram proves	Evidence artifacts required	Status
		3.13.16 — CUI at rest	traverse VLAN 20, 30, or any unapproved path.		
Fig 6	742 Skypad Blvd. facility floor plan (SAD-001 App. C)	**3.10.1** — limit physical access **3.10.2** — protect facility **3.10.3** — escort visitors **3.10.4** — physical access logs **3.10.5** — access devices **3.10.6** — alternate work sites	Documents four physical security zones: facility perimeter (KC 1), engineering CUI area (KC 2), IT admin anteroom (KC 3), server room secured area (KC 3 + interior controls). Identifies all keycard entry points (HID ProxKey4, PAR-002). Documents Verkada camera placement at all entry and CUI areas. Marks WS-01, WS-05, WS-09 as requiring privacy screens due to proximity to exterior west wall. Flags Conference Room B with POA&M 2026-01.	• HID ProxPoint access log export • PAR-002 physical access register • Verkada camera coverage report • Privacy screen installation photos (WS-01, -05, -09) • Visitor log (VL-001) samples	**Implemented**
Fig 7	Server room physical control layers (SAD-001 App. C-1)	**3.10.1** — limit physical access **3.10.2** — monitor facility **3.10.4** — physical access logs **3.10.5** — control access devices	Documents two-stage physical access sequencing to the server room: passage through the IT admin office anteroom is required before the server room door is reachable. Confirms only IT Admin (Spacely) and ISSO (Cogswell) hold KC 3 authorization. Documents Verkada interior camera, APC SmartUPS, dedicated HVAC with temperature alerting. Confirms lost/stolen keycard revocation within 2 hours. Confirms quarterly access log review by ISSO.	• HID access log: server room entry events • PAR-002: KC 3 authorization holders • Verkada camera footage retention policy • APC SmartUPS monitoring config • HVAC temperature alert config	**Implemented**
Fig 8 (pending)	Wazuh SIEM-01 read-only config (SAD-001 App. G)	**3.3.1** — create audit logs **3.3.2** — user traceability **3.3.5** — correlate audit records	Demonstrates that SIEM-01 on VLAN 40 receives log data from all VLANs via one-way Wazuh agent push (agents on VLAN 10/20/40 push to SIEM-01; SIEM-01 has no management interface reachable from VLAN 10). Confirms SIEM-01 cannot modify traffic on any	• Wazuh agent ossec.conf showing server IP and one-way push • Wazuh manager network interface config (no route to VLAN 10) • Firewall rule confirming	**Partially Implemented**

Figure	Title / Location	NIST Practices	What this diagram proves	Evidence artifacts required	Status
		3.3.8 — protect audit information **3.3.9** — limit log management access **3.14.6** — monitor for attacks	VLAN. Confirms log admin access is restricted to IT Admin and ISSO accounts. Confirms M365 GCC High audit log ingestion via Graph API connector (closed POA&M item 3.3.5).	SIEM-01 outbound blocked to VLAN 10 • Wazuh admin user list (IT Admin + ISSO only) • M365 Graph API connector config	

3. Pre-Assessment Task — Figure 8 (Wazuh SIEM-01)

Figure 8 is the only outstanding evidence gap in this crosswalk. The SSP (Section 4.11, practices 3.3.8 and 3.3.9) states that SIEM-01 on VLAN 40 has read-only monitoring access to all VLANs, but no configuration artifact currently on file proves the one-way enforcement. This is the specific gap a C3PAO will probe: an assessor will want to see not just that SIEM-01 receives logs, but that it has no management path back to VLAN 10 devices.

3.1 Required Evidence Artifacts

#	Artifact	What to capture	Owner / Due
1	**Wazuh agent config (ossec.conf)**	Export ossec.conf from any VLAN 10 agent (e.g., DC-01). Show <server><address> pointing to SIEM-01 IP and confirm no reverse management channel is configured. Key line: <protocol>tcp</protocol> with no server-initiated connection.	**Harlan Spacely** Before assessment
2	**SIEM-01 network interface config**	Screenshot or export of SIEM-01 (Ubuntu 22.04) network interface showing it is bound to VLAN 40 (192.168.40.x) only, with no interface on VLAN 10 (192.168.10.x).	**Harlan Spacely** Before assessment
3	**Firewall rule confirming no SIEM-01 → VLAN 10 path**	Export the SonicWall TZ570 ruleset showing there is no permit rule allowing traffic from 192.168.40.x (VLAN 40) to 192.168.10.x (VLAN 10) initiated by SIEM-01. The monitoring traffic flows from VLAN 10 agents to SIEM-01, not the reverse.	**Harlan Spacely** Before assessment
4	**Wazuh admin user list**	Screenshot of Wazuh web console user management showing only two accounts: IT Admin (admin.hspacely) and ISSO (admin.mcogswell). Confirms practice 3.3.9 — log management restricted to privileged users.	**Harlan Spacely** Before assessment
5	**M365 Graph API connector config**	Screenshot of the Azure AD application registration in GCC High tenant with AuditLog.Read.All permission assigned. Confirms M365 audit logs are pulled (read only) by SIEM-01. This was the evidence artifact for closed POA&M item 3.3.5.	**Harlan Spacely** Already on file (EVD-3.3.5-001) — confirm current

3.2 What the Assessor Will Test

A C3PAO examining SIEM-01 under practices 3.3.8 and 3.3.9 will typically perform the following verification steps. Margaret Cogswell (ISSO) should walk through each of these in advance:

Step	Assessor action / Cogswell Cogs response
1	Assessor asks: 'Show me that SIEM-01 cannot send commands or modify configurations on VLAN 10 systems.' — Response: Show the firewall rule (Artifact 3) and the SIEM-01 network interface config (Artifact 2). Point to the absence of any VLAN 40 → VLAN 10 permit rule. Note that Wazuh agent architecture is agent-initiated pull: agents push logs outbound to SIEM-01; SIEM-01 never initiates a connection to agents for operational purposes.
2	Assessor asks: 'Who can make changes to the SIEM-01 log configuration?' — Response: Open the Wazuh admin console (Artifact 4) and show two accounts only. Note that standard CUI users have no access to SIEM-01. Reference practice 3.3.9.
3	Assessor asks: 'Can you show me a log entry from a VLAN 10 system in SIEM-01?' — Response: Open Wazuh dashboard, pull a sample Windows Security Event log entry from DC-01 or FS-01 (a logon event from the last 24 hours works well). Show the agent name, the source IP (192.168.10.x), and the event timestamp. This demonstrates 3.3.1 and 3.3.2.
4	Assessor asks: 'Are M365 GCC High audit events in this SIEM?' — Response: Open the M365 audit log section in Wazuh (or show a recent SharePoint file access event). Reference the Graph API connector config (Artifact 5) as the ingestion mechanism. This demonstrates the closed POA&M item 3.3.5.
5	Assessor asks: 'How are SIEM logs protected from tampering?' — Response: Reference practice 3.3.8. Show the RAID volume ACLs on SIEM-01 preventing non-root modification, and the Azure GCC High WORM archive policy. Note that SIEM admin access requires MFA (same Entra ID CAP-001 that covers all privileged accounts).

4. Practice Coverage Summary

The table below lists every NIST SP 800-171 practice family and confirms which figure(s) provide primary evidence for that family. Families marked with an asterisk (*) are also covered in the SSP Section 4 narrative and the POA&M but do not have a dedicated diagram — their evidence comes from policy documents, training records, and system configuration exports rather than architectural figures.

Family	Practice IDs	Primary figure(s)	Notes
AC	3.1.1 – 3.1.22	**Fig 1, Fig 2, Fig 3**	Network topology (Fig 1) covers boundary and flow controls. VPN auth flow (Fig 2) covers remote access practices. VLAN 10 layers (Fig 3) covers least privilege and endpoint enforcement.
AT	3.2.1 – 3.2.3	** (no diagram)*	Evidenced by KnowBe4 training completion records, phishing simulation reports, and role-based training certificates in HR files.
AU	3.3.1 – 3.3.9	**Fig 8 (pending)**	Wazuh SIEM-01 config diagram (Fig 8) is the primary evidence artifact. See Section 3 for the pre-assessment task. Fig 5 (DFD) provides secondary evidence for log coverage of CUI data paths.
CM	3.4.1 – 3.4.9	**Fig 3**	VLAN 10 defense layers (Fig 3) documents AppLocker, WSUS, GPO baselines, and software restriction. Supplemented by INV-HW-001 and INV-SW-001 inventory records.
IA	3.5.1 – 3.5.11	**Fig 2, Fig 3**	VPN auth flow (Fig 2) covers MFA and replay-resistant auth. VLAN 10 layers (Fig 3) covers AD RBAC and Entra ID enforcement.
IR	3.6.1 – 3.6.3	** (no diagram)*	Evidenced by IRP-001 (Incident Response Plan), ITL-001 (incident log), and IREAR-2024-001 (tabletop exercise after action report).
MA	3.7.1 – 3.7.6	** (no diagram)*	Evidenced by MTP-001 (maintenance policy), SML-001 (maintenance log), and VMEL-001 (visitor and maintenance escort log).
MP	3.8.1 – 3.8.9	**Fig 5**	CUI data flow diagram (Fig 5) traces media lifecycle: receipt, processing, archival (Veeam/Azure WORM), and destruction (NIST SP 800-88). Supplemented by MSR-001 sanitization records.
PS	3.9.1 – 3.9.2	** (no diagram)*	Evidenced by PSP-001 (personnel security policy), Checkr screening records, and HSC-001 (HR separation checklist).

Family	Practice IDs	Primary figure(s)	Notes
PE	3.10.1 – 3.10.6	**Fig 6, Fig 7**	Facility floor plan (Fig 6) documents all keycard entry points, camera placement, and workstation positions. Server room control layers (Fig 7) documents the two-stage access sequence and secured area controls.
RA	3.11.1 – 3.11.3	** (no diagram)*	Evidenced by RA-2025-001 (risk assessment report), Tenable Nessus scan reports, and VTR-001 (vulnerability tracking register).
CA	3.12.1 – 3.12.4	** (no diagram)*	This crosswalk document itself partially satisfies 3.12.4. Supplemented by SCA-2025-001 (security control assessment), POAM-001 v3.2, and SSP-001 v3.0.
SC	3.13.1 – 3.13.16	**Fig 1, Fig 2, Fig 3, Fig 4, Fig 5**	Most comprehensively evidenced family. Fig 4 (SonicWall stack) is the primary artifact for 3.13.1 and 3.13.6. Fig 2 covers 3.13.7 and 3.13.8. Fig 5 covers 3.13.8 and 3.13.16. Practice 3.13.12 has an active POA&M (2026-01).
SI	3.14.1 – 3.14.7	**Fig 3, Fig 4**	VLAN 10 layers (Fig 3) documents MDE, WSUS, and AppLocker. SonicWall stack (Fig 4) documents gateway AV and IPS. Supplemented by Defender portal reports and WSUS compliance exports.

PLAN OF ACTION AND MILESTONES

POAM-001

Cogswell Cogs, Inc. — CUI Processing Environment

CMMC Level 2 / NIST SP 800-171 Rev 2

Administrative Field	Value	Field	Value
Organization Name	Cogswell Cogs, Inc.	**CAGE Code**	7CG42
System Name	CUI Processing Environment (CPE)	**SSP Reference**	SSP-001 v3.0
Point of Contact	Margaret Cogswell, ISSO	**POC Phone**	(802) 555-0142
IT Technical Lead	Harlan Spacely, IT Administrator	**POC Email**	m.cogswell@cogswellcogs.com
Contract Number	W52P1J-23-C-0088 (Army Contracting Command — ACC-APG)	**Doc Version**	3.2
Facility Address	742 Skypad Boulevard, Orbit City, CA 90210	**Date**	March 20, 2026
SPRS Score (Current)	107 — submitted January 15, 2026 (reflects 1 partially implemented practice)	**Next Review**	September 2026

HANDLING NOTICE — *This document is designated CUI//SP-CTI. It contains security deficiency details for a DoD contractor system. Handle, store, and transmit in accordance with 32 CFR Part 2002 and the Cogswell Cogs CUI Program Policy (CUI-POL-001). Do not distribute without written authorization from the System Owner (Victor Cogswell, CEO).*

1. Purpose and Scope

This Plan of Action and Milestones (POA&M) document (POAM-001) is the official remediation tracking record for the Cogswell Cogs, Inc. CUI Processing Environment (CPE) in support of the organization's CMMC Level 2 certification under 32 CFR Part 170. It is a companion document to System Security Plan SSP-001 (Version 3.0, dated March 20, 2026).

The POA&M serves three functions. First, it documents all security control deficiencies identified through internal assessments, vulnerability scanning, or external review. Second, it establishes binding milestones, resource allocations, and responsible parties for each remediation effort. Third, it serves as the primary evidence artifact that a C3PAO will examine to verify that partially implemented practices are being actively and systematically remediated.

This version of POAM-001 contains one (1) active open item (Section 3) and a historical archive of four (4) successfully closed items from the 2025 remediation cycle (Section 4). All open items have been assessed against the 180-day remediation window requirement of 32 CFR Part 170.

1.1 POA&M Status Summary

Practice	Description	Status	Target Date	Section
3.13.12	Teams Admin Center policy not yet in enforcement mode. Physical compensating controls (camera covers) installed August 2025.	Partially Implemented	June 30, 2026	Section 3
3.1.3	Endpoint DLP for USB output	CLOSED — Remediated	May 2025	Section 4
3.3.5	M365 / on-prem SIEM correlation	CLOSED — Remediated	April 2025	Section 4
3.4.8	AppLocker on servers (FS-01/DC-01)	CLOSED — Remediated	August 2025	Section 4
3.11.1	Annual Risk Assessment update	CLOSED — Remediated	June 2025	Section 4

2. Regulatory and Assessment Context

2.1 Governing Authorities

Authority	Relevance to This POA&M
32 CFR Part 170 (CMMC Rule)	Governs the CMMC program. Section 170.21 permits POA&Ms for Level 2 assessments under defined conditions. POA&M items must be closed within 180 days of the C3PAO assessment date. Failure to close within 180 days results in loss of CMMC certification.
NIST SP 800-171 Rev 2, Practice 3.13.12	Requires organizations to prohibit remote activation of collaborative computing devices and to provide an indication of use to present users. This practice is the subject of the sole open POA&M item in this document.
NIST SP 800-171A (Assessment Procedures)	Provides the assessment methodology and evidentiary standards a C3PAO will apply. The physical camera cover compensating control is assessed under the 'other' assessment method category and must be documented with physical evidence (photographs, installation records).
DFARS 252.204-7021 (CMMC Clause)	Contract W52P1J-23-C-0088 includes DFARS 252.204-7021. CMMC Level 2 certification is a condition of contract continuation. Any gap between certification lapse and re-certification creates contract performance risk.
DFARS 252.204-7012 (Cyber Incident Reporting)	While not directly a POA&M driver, this clause requires 72-hour incident reporting. An open POA&M item affecting communication systems (3.13.12) increases the residual risk profile under this clause and is documented in the Risk Assessment (RA-2025-001).

2.2 POA&M Acceptance Criteria for CMMC Level 2

For a C3PAO to accept a POA&M item at the time of assessment under 32 CFR Part 170, all of the following conditions must be satisfied:

1.	The practice must be assessed as Partially Implemented (not Not Implemented). A Not Implemented finding cannot be carried as a POA&M and will result in a failed assessment.
2.	The organization must demonstrate active, good-faith remediation progress with documented milestones, resources, and responsible parties.
3.	The practice must not be among the practices that are explicitly disqualified from POA&M treatment under the CMMC assessment guide (practices related to MFA, basic access control, and incident reporting are examples of practices that may be treated more strictly).
4.	All POA&M items accepted at assessment must be fully remediated and verified within 180 calendar days of the assessment date. The 180-day clock begins on the date the C3PAO formally issues its assessment findings.

5.	Progress must be affirmatively reported to the C3PAO at defined intervals during the 180-day window. Cogswell Cogs will submit monthly status updates to the C3PAO via the agreed reporting channel beginning 30 days after assessment completion.

3. Active POA&M Item

⚠ 180-DAY REMEDIATION DEADLINE — CRITICAL COMPLIANCE NOTICE

Per 32 CFR Part 170, this POA&M item must be fully remediated and independently verified within 180 calendar days of the C3PAO assessment date. The 180-day deadline is calculated from the formal assessment completion date, not the date of this document. Failure to close this item within the 180-day window will result in automatic loss of CMMC Level 2 certification and may constitute a material breach of Contract W52P1J-23-C-0088 under DFARS 252.204-7021. The ISSO (Margaret Cogswell) is responsible for proactive milestone tracking and must escalate immediately to the System Owner (Victor Cogswell) if any milestone is at risk of slipping.

POA&M ITEM NO. 2026-01 | PRACTICE 3.13.12 | STATUS: PARTIALLY IMPLEMENTED

3.1 Administrative Data

POA&M Item Number	2026-01	**Date Opened**	March 20, 2026
Practice ID	3.13.12	**Date Target**	June 30, 2026
Practice Family	SC — System and Communications Protection	**Priority**	HIGH
ISSO / POC	Margaret Cogswell (m.cogswell@cogswellcogs.com)	**Tech Lead**	Harlan Spacely
System Owner	Victor Cogswell, CEO	**SPRS Impact**	Estimated -3 points (current score: 107)
SSP Reference	SSP-001 v3.0, Section 4.13 (Practice 3.13.12)	**Risk Rating**	Medium (compensating controls in place)
180-Day Deadline	**To be calculated:** *Assessment Date + 180 days. The ISSO must record the actual assessment completion date here immediately upon receipt of the C3PAO's formal findings letter.*	**Assessment Date**	[TO BE ENTERED]

3.2 Deficiency Description

NIST SP 800-171 Requirement	**3.13.12:** Prohibit remote activation of collaborative computing devices and provide indication of use to present users. *Source: NIST SP 800-171 Rev 2, Section 3.13. Assessment method per NIST SP 800-171A: Examine [system and communications protection policy; procedures addressing protection of information at rest; system design documentation; system security plan]; Interview; Test.*
Affected System Components	Microsoft Teams (M365 GCC High tenant — cogswellcogs.onmicrosoft.us); Conference Room A and Conference Room B — Poly Studio X30 collaboration camera systems.
Nature of Deficiency	**The deficiency is limited to software policy enforcement.** The Microsoft Teams Admin Center policy that prevents remote activation of cameras and microphones on room-based collaboration systems is currently operating in audit mode. In audit mode, the policy generates log entries for potential policy violations but does not block or prevent remote activation events. Full enforcement mode has been deferred pending the completion of Teams Phone firmware compatibility testing on the Poly Studio X30 units. **Compensating control status:** Physical privacy covers were installed on all Poly Studio X30 conference room cameras in both Conference Room A and Conference Room B in August 2025. These covers provide a hardware-level indication of non-use and prevent unauthorized visual surveillance even in the absence of software enforcement. This compensating control was documented in SSP-001 v3.0 (Section 4.13) and evaluated by Koran & Associates in January 2026 as providing adequate interim protection for the visual component of the requirement.
Root Cause	Poly Studio X30 firmware version 3.7.1 (current as of March 2026) contains a known compatibility issue with the Teams Admin Center device management API when enforcement-mode policies are applied. Polycom/Poly engineering advisory PA-2025-114 identifies this as a firmware defect resolved in the forthcoming firmware release 3.8.0, targeted for general availability April 2026. Deploying enforcement mode before the firmware update risks rendering the conference room systems inoperable during calls, which carries operational impact to program meetings with ACC-APG.
Risk Acceptance Statement	The System Owner (Victor Cogswell) formally accepts the residual risk associated with this deficiency for the period of the POA&M. This acceptance is based on the following risk reduction factors: 1. Physical camera covers installed on all affected devices eliminate the unauthorized visual surveillance vector. 2. Teams audit-mode policy is actively logging activation events; the ISSO reviews these logs weekly.

	3. Conference rooms are located within the secure facility perimeter (keycard access required) and are not accessible to unauthorized personnel. 4. No CUI is processed or displayed exclusively in conference rooms; CUI access requires workstation authentication. **Risk acceptance is time-limited to the duration of this POA&M (through June 30, 2026) and does not extend beyond that date.**

3.3 Resources Required

Resource	Type	Estimated Effort / Cost	Availability
IT Administrator (Harlan Spacely) — firmware upgrade testing, policy configuration, and verification	Internal Labor	Estimated 12–16 hours total across M1, M2, and M3 milestones. No incremental labor cost (salaried position).	Available — no competing projects scheduled during POA&M window.
ISSO (Margaret Cogswell) — milestone oversight, evidence documentation, and C3PAO reporting	Internal Labor	Estimated 4–6 hours total. No incremental cost.	Available.
Microsoft 365 GCC High — Teams Admin Center (existing subscription)	Existing License	No additional licensing required. Teams Admin Center enforcement-mode policy is included in existing M365 GCC High Plan subscription.	Active — subscription current through December 31, 2026.
Poly Studio X30 Firmware 3.8.0 — vendor-provided update (complimentary)	Vendor Software	No cost. Firmware release 3.8.0 is a complimentary update per Poly support agreement (Contract SVC-POLY-2023).	Targeted GA: April 2026. IT Administrator subscribed to Poly release notifications.
Koran & Associates — independent verification review (optional)	External Consultant	Estimated 2 hours at consultant rate (budgeted under existing retainer). Optional; ISSO may perform verification without external review if schedule permits.	Available per retainer agreement.

3.4 Remediation Milestones

#	Target Date	Responsible Party	Status	% Complete	Milestone Description
M1	April 30, 2026	Harlan Spacely (IT Admin)	**In Progress**		Download and deploy Poly Studio X30 firmware 3.8.0 upon general availability (expected April 2026). Conduct regression testing on conference room audio/video functionality to confirm no operational regressions. Document firmware version, installation date, and test results in Maintenance Log (SML-001). Confirm firmware release notes explicitly resolve compatibility issue identified in Poly advisory PA-2025-114.
M2	May 31, 2026	Harlan Spacely (IT Admin)	**Not Started**		Configure and activate enforcement-mode device policy in Microsoft Teams Admin Center for all conference room systems. Policy must explicitly prohibit remote activation of cameras and microphones from external meeting participants. Capture Teams Admin Center policy configuration screenshot as evidence artifact (EVD-3.13.12-002). Verify policy is applied to both Conference Room A and Conference Room B Poly Studio X30 devices. Review audit-mode logs from January 2026 through April 2026 to confirm no prior unauthorized activation events occurred during the compensating control period.
M3	June 30, 2026	Margaret Cogswell (ISSO)	**Not Started**		Conduct final verification testing: attempt remote camera/microphone activation from an external Teams meeting participant account and confirm the activation is blocked. Document test procedure, tester identity, date, and outcome in

#	Target Date	Responsible Party	Status	% Complete	Milestone Description
					the POA&M Closure Record (EVD-3.13.12-003). Update SSP-001 to reflect 3.13.12 status as Implemented. Update POAM-001 to close Item 2026-01. Submit updated SPRS score to SPRS portal reflecting closure. Submit closure notification to C3PAO per agreed reporting protocol. Obtain System Owner signature on POA&M closure. File all evidence artifacts in SharePoint GCC High / Security / POA&M / 2026-01.

3.5 Evidence Artifacts Required for Closure

Artifact ID	Description	Milestone	Storage Location / Notes
EVD-3.13.12-001	Photographs of installed physical camera covers on both Poly Studio X30 units in Conference Rooms A and B.	Pre-existing (Aug 2025)	SharePoint GCC High / Security / POA&M / 2026-01 / Camera-Covers-Photos.pdf. Verified by ISSO January 2026.
EVD-3.13.12-002	Teams Admin Center policy configuration screenshot showing enforcement-mode activation for both conference room devices.	M2 (May 2026)	SharePoint GCC High / Security / POA&M / 2026-01 / Teams-Policy-Config.pdf
EVD-3.13.12-003	POA&M Closure Record: documented test of remote activation attempt confirming policy blocks activation. Includes tester, date, and outcome.	M3 (Jun 2026)	SharePoint GCC High / Security / POA&M / 2026-01 / Closure-Record.pdf. Must be signed by ISSO.
EVD-3.13.12-004	Poly Studio X30 firmware version confirmation (firmware 3.8.0 installed), extracted	M1 (Apr 2026)	SharePoint GCC High / Security / POA&M / 2026-01 / Firmware-Confirmation.pdf

Artifact ID	Description	Milestone	Storage Location / Notes
	from device management console.		
EVD-3.13.12-005	Maintenance Log (SML-001) entry documenting firmware upgrade date, technician, and post-upgrade test results.	M1 (Apr 2026)	SharePoint GCC High / IT / Maintenance / SML-001. Cross-reference entry in POA&M closure record.
EVD-3.13.12-006	Updated SSP-001 (v3.1 or later) reflecting 3.13.12 status as Implemented.	M3 (Jun 2026)	SharePoint GCC High / Compliance / SSP-001-v3.1.docx. System Owner approval required.
EVD-3.13.12-007	SPRS submission confirmation showing updated score reflecting 3.13.12 closure.	M3 (Jun 2026)	SharePoint GCC High / Security / POA&M / 2026-01 / SPRS-Confirmation.pdf. ISSO to retain screenshot of submission.

3.6 Progress Reporting Schedule

Cogswell Cogs will provide monthly progress updates to the C3PAO throughout the 180-day remediation window. Updates must be submitted by the 15th of each month and must include: current milestone status, percentage of completion, any obstacles encountered, and revised target dates if milestones have slipped (with written System Owner authorization for any date change).

Report Due Date	Reporting Party	Content Required
April 15, 2026	M. Cogswell (ISSO)	M1 status update: firmware availability confirmation, testing initiation. Note if Poly firmware 3.8.0 GA has been delayed.
May 15, 2026	M. Cogswell (ISSO)	M1 closure confirmation (firmware installed and tested) + M2 status update: Teams Admin Center policy configuration progress.
June 15, 2026	M. Cogswell (ISSO)	M2 closure confirmation + M3 progress: verification testing underway. Preliminary evidence artifacts submitted if available.
June 30, 2026	M. Cogswell (ISSO) + V. Cogswell (System Owner)	**FINAL CLOSURE REPORT: All milestones complete. All evidence artifacts on file. SSP updated. SPRS score updated. System Owner signature obtained. Item formally closed.**

4. Historical Archive — Closed POA&M Items (2025 Remediation Cycle)

The following four items were identified during the 2024 internal security control assessment (SCA-2024-001) and remediated during 2025. All items were independently verified by Koran & Associates and confirmed closed during the annual review (SCA-2025-001, completed December 5, 2025). These items are retained in this document for historical continuity and as an auditable record of the organization's remediation track record.

CLOSED ITEM 2025-01 | PRACTICE 3.13.12 | ENDPOINT DATA LOSS PREVENTION — USB OUTPUT GAP | STATUS: REMEDIATED & CLOSED

POA&M Item No.	2025-01	**Practice ID**	3.13.12
Date Opened	November 1, 2024	**Date Closed**	May 31, 2025
Closed By	Margaret Cogswell (ISSO)	**Verified By**	Koran & Associates (June 2025)
SPRS Score Impact	+5 points on closure	**Final Status**	**CLOSED — Remediated**
Deficiency (Historical)	Microsoft Purview Endpoint DLP policy was not deployed to workstations. As a result, CUI exfiltration via USB storage device could not be detected or blocked at the endpoint. The perimeter USB block (GPO-SEC-005) prevented physical USB insertion, but the absence of Endpoint DLP meant any USB exception scenario would lack a detection and audit layer.		
Remediation Action	Microsoft Purview Endpoint DLP license (included in M365 GCC High E3 licensing) was activated and configured. DLP policies were created to detect and block file transfers to USB devices for all users in the CUI-authorized security group. Pilot deployment to 3 workstations completed May 15, 2025. Full deployment to all 12 CUI workstations completed May		

	28, 2025. DLP policy configuration screenshot and test results documented in EVD-3.1.3-001 through EVD-3.1.3-004.
Evidence on File	EVD-3.1.3-001: Microsoft Purview DLP policy configuration (screenshot). EVD-3.1.3-002: Pilot test results — USB transfer attempt blocked, alert generated. EVD-3.1.3-003: Full deployment confirmation (all 12 workstations, Intune compliance report). EVD-3.1.3-004: ISSO sign-off and closure memo (May 31, 2025).

#	Target Date	Responsible	Status	Actual Completion	Description
M 1	April 30, 2025	IT Admin / ISSO	**CLOSED**	Completed April 18, 2025	Evaluated Microsoft Purview Endpoint DLP licensing; confirmed included in existing M365 GCC High E3 license. No additional procurement required.
M 2	May 15, 2025	IT Admin / ISSO	**CLOSED**	Completed May 15, 2025	Deployed DLP policy to pilot group of 3 workstations. Confirmed USB transfer block and alert generation. No operational issues observed.
M 3	May 31, 2025	IT Admin / ISSO	**CLOSED**	Completed May 28, 2025	Full deployment to all 12 CUI workstations. SSP updated. SPRS score updated. Item closed by ISSO.

CLOSED ITEM 2025-02 | PRACTICE 3.3.5 | CROSS-SOURCE AUDIT LOG CORRELATION (M365 TO SIEM) | STATUS: REMEDIATED & CLOSED

POA&M Item No.	2025-02	**Practice ID**	3.3.5
Date Opened	November 1, 2024	**Date Closed**	April 30, 2025

Closed By	Margaret Cogswell (ISSO)	**Verified By**	Koran & Associates (June 2025)
SPRS Score Impact	+5 points on closure	**Final Status**	**CLOSED — Remediated**
Deficiency (Historical)	Wazuh SIEM (SIEM-01) was ingesting on-premises Windows Security Event logs and SonicWall firewall logs but was not correlating these events with Microsoft 365 GCC High audit logs. This meant that cross-platform attack scenarios (e.g., a compromised M365 account being used to access on-premises file shares) would not generate a correlated alert. M365 audit events were available in the M365 compliance center but required manual review separately from SIEM-01.		
Remediation Action	Microsoft Graph API connector for Wazuh was configured using an Azure AD application registration with appropriate audit log read permissions in the GCC High tenant. A custom Wazuh decoder was developed to normalize M365 audit log format into the Wazuh event schema. Cross-source correlation rules were developed and tested against three simulated attack scenarios: (1) M365 account compromise followed by VPN access, (2) unusual SharePoint CUI file access followed by USB insertion attempt, and (3) failed M365 MFA events correlated with concurrent failed VPN authentication. All three scenarios generated correlated alerts in SIEM-01.		
Evidence on File	EVD-3.3.5-001: Graph API connector configuration documentation. EVD-3.3.5-002: Custom Wazuh decoder code and rule definitions. EVD-3.3.5-003: Correlation rule test results (3 scenarios). EVD-3.3.5-004: ISSO		

	sign-off and closure memo (April 30, 2025).

#	Target Date	Responsible	Status	Actual Completion	Description
M 1	April 15, 2025	IT Admin / ISSO	**CLOSED**	Completed April 10, 2025	Configured Microsoft Graph API connector for Wazuh; registered Azure AD application in GCC High tenant with AuditLog.Read.All permissions. Confirmed log ingestion flow from M365 to SIEM-01.
M 2	April 25, 2025	IT Admin / ISSO	**CLOSED**	Completed April 22, 2025	Developed and deployed custom Wazuh decoder for M365 audit log format normalization. Defined and activated three cross-source correlation rules covering the primary attack scenarios of concern.
M 3	April 30, 2025	IT Admin / ISSO	**CLOSED**	Completed April 30, 2025	Validated correlation rules against all three simulated test scenarios. All scenarios generated expected correlated alerts. SSP updated. Item closed by ISSO.

CLOSED ITEM 2025-03 | PRACTICE 3.4.8 | APPLOCKER APPLICATION CONTROL — SERVER GAP (FS-01 / DC-01) | STATUS: REMEDIATED & CLOSED

POA&M Item No.	2025-03	**Practice ID**	3.4.8
Date Opened	November 1, 2024	**Date Closed**	August 31, 2025
Closed By	Margaret Cogswell (ISSO)	**Verified By**	Koran & Associates (September 2025)
SPRS Score Impact	+5 points on closure	**Final Status**	**CLOSED — Remediated**
Deficiency (Historical)	AppLocker application control was deployed and enforced on all 12		

	Windows 11 workstations but was not deployed to the Windows Server 2022 file server (FS-01) or the domain controller (DC-01). Application control on these servers was policy-only (documented in Prohibited Software Policy PSP-001) without a technical enforcement mechanism. An attacker with server access could execute unauthorized binaries without generating an AppLocker block event.
Remediation Action	A complete application inventory was performed on FS-01 and DC-01 to establish the approved execution baseline. AppLocker was deployed in audit mode for 60 days to identify legitimate applications that would need to be whitelisted. Audit mode findings were reviewed and 4 previously undocumented scheduled task executables were added to the approved list. AppLocker enforcement mode was activated on both servers with an allow-list policy. Post-enforcement monitoring confirmed no legitimate operational processes were blocked.
Evidence on File	EVD-3.4.8-001: FS-01 and DC-01 application inventory reports (June 2025). EVD-3.4.8-002: AppLocker audit-mode findings report (July 2025) including the 4 identified unwhitelisted executables. EVD-3.4.8-003: Updated approved software list (ASL-001 v2) incorporating newly identified scheduled task executables. EVD-3.4.8-004: AppLocker enforcement mode activation confirmation (both servers). EVD-3.4.8-005: 30-day post-enforcement monitoring report confirming no operational blocking events. EVD-3.4.8-006: ISSO sign-off and closure memo (August 31, 2025).

#	Target Date	Responsible	Status	Actual Completion	Description
M 1	June 30, 2025	IT Admin / ISSO	CLOSED	Completed June 27, 2025	Performed full application inventory on FS-01 and DC-01. Identified 4 previously undocumented scheduled task executables. Updated Approved Software List (ASL-001 v2).
M 2	July 31, 2025	IT Admin / ISSO	CLOSED	Completed July 15, 2025	Deployed AppLocker in audit mode to both servers. Collected 30 days of audit data. Reviewed findings; confirmed no additional unknown executables beyond the 4 identified in M1.
M 3	August 31, 2025	IT Admin / ISSO	CLOSED	Completed August 25, 2025	Activated AppLocker enforcement mode on FS-01 and DC-01. Monitored for 7 days post-activation; no legitimate processes blocked. SSP updated. Item closed by ISSO.

CLOSED ITEM 2025-04 | PRACTICE 3.11.1 | ANNUAL RISK ASSESSMENT UPDATE (RA-2025-001) | STATUS: REMEDIATED & CLOSED

POA&M Item No.	2025-04	**Practice ID**	3.11.1
Date Opened	November 1, 2024	**Date Closed**	June 30, 2025
Closed By	Margaret Cogswell (ISSO)	**Verified By**	Koran & Associates (July 2025)
SPRS Score Impact	+5 points on closure	**Final Status**	**CLOSED — Remediated**
Deficiency (Historical)	The most recent formal risk assessment (RA-2024-001, completed August 2024) had not been updated to reflect significant system changes made in Q4 2024, specifically the replacement of the Cisco AnyConnect VPN with a FortiGate SSL VPN (December		

	2024). Additionally, the annual update cadence was not met; RA-2024-001 became overdue for its one-year refresh in August 2025 prior to the completion of the update. The absence of a current risk assessment meant the SSP's risk foundation was not reflective of the actual system state.
Remediation Action	Risk Assessment RA-2025-001 was completed using the NIST SP 800-30 Rev 1 methodology. The assessment scope was expanded relative to RA-2024-001 to explicitly cover the FortiGate SSL VPN architecture, the Microsoft Endpoint DLP deployment (3.1.3 remediation), and the Wazuh SIEM M365 integration (3.3.5 remediation). Seven risk scenarios were assessed. Three scenarios received a residual risk rating of Low. Four scenarios received a residual risk rating of Medium, including the 3.13.12 Teams policy gap. No High or Critical residual risks were identified. The System Owner accepted all residual risks on June 30, 2025.
Evidence on File	EVD-3.11.1-001: RA-2025-001 full risk assessment report (NIST SP 800-30 Rev 1 format). EVD-3.11.1-002: Risk treatment decisions and System Owner acceptance sign-off. EVD-3.11.1-003: Koran & Associates independent review memo (July 2025). EVD-3.11.1-004: ISSO closure memo and POAM-001 update record.

#	Target Date	Responsible	Status	Actual Completion	Description
M 1	April 30, 2025	IT Admin / ISSO	**CLOSED**	Completed April 25, 2025	Engaged Koran & Associates to define updated risk assessment scope reflecting FortiGate VPN, Endpoint DLP, and SIEM M365 integration changes. Finalized

#	Target Date	Responsible	Status	Actual Completion	Description
					methodology and interview schedule.
M 2	May 31, 2025	IT Admin / ISSO	**CLOSED**	Completed May 28, 2025	Completed RA-2025-001 draft covering all 14 NIST SP 800-171 practice families and 7 threat scenarios. Submitted draft to Koran & Associates for independent review.
M 3	June 30, 2025	IT Admin / ISSO	**CLOSED**	Completed June 30, 2025	Koran & Associates review completed. Final RA-2025-001 issued. System Owner accepted all residual risks. SSP updated. SPRS score updated. Item closed by ISSO.

5. Document Review and Authorization

This POA&M is reviewed monthly by the ISSO and quarterly with the System Owner. Any changes to milestone dates, responsible parties, or resource allocations require System Owner written approval. The POA&M is provided to the C3PAO upon request and is submitted as part of the CMMC Level 2 assessment package.

Review Date	Reviewer	Version	Changes
March 20, 2026	M. Cogswell (ISSO) / V. Cogswell (System Owner)	3.2	Initial issue of POAM-001 v3.2. Closed items 2025-01 through 2025-04 archived from prior tracking records. Active item 2026-01 (3.13.12) opened with June 30, 2026 target. 180-day deadline notice added per 32 CFR Part 170.
December 5, 2025	M. Cogswell (ISSO)	3.1	Closed items 3.1.3, 3.3.5, 3.4.8, and 3.11.1 following SCA-2025-001 verification. Updated SPRS score to 107. Retained 3.13.12 as partially implemented; extended target to June 30, 2026 following physical camera cover installation.
November 1, 2024	M. Cogswell (ISSO)	2.0	Initial POA&M entries following SCA-2024-001 internal assessment. Opened items 3.1.3, 3.3.5, 3.4.8, 3.11.1, and 3.13.12.

System Owner Authorization

System Owner Name	Victor Cogswell
Signature	
Title	Chief Executive Officer, Cogswell Cogs, Inc.
Date	March 20, 2026
ISSO Signature	
ISSO Name / Date	Margaret Cogswell / March 20, 2026