1. SYSTEM IDENTIFICATION

1.1. System Name/Title: Orchestrated Repository for the Enterprise

1.1.1. System Categorization: MODERATE

1.1.2. System Unique Identifier: ORE

1.2. Responsible Organization:

Name:	
Address:	
Phone:	

1.2.1. Information Owner (Government point of contact responsible for providing and/or receiving CUI**):**

Name:	Fraser, Doug
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	dfraser@2twelvesolutions.com

1.2.1.1. System Owner (assignment of security responsibility)**:**

Name:	Fraser, Doug
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	dfraser@2twelvesolutions.com

1.2.1.2. System Security Officer:

Name:	Tong, Thanh
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	ttong@2twelvesolutions.com

1.3. General Description/Purpose of System: What is the function/purpose of the system?

1.3.1. Number of end users and privileged users:

Roles of Users and Number of Each Type:

Number of Users	Number of Administrators/ Privileged Users
0	0

1.4. General Description of Information: CUI information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at https://www.archives.gov/cui/registry/category-list.

Information Type (Use only information types from NIST SP 800-60, Volumes I and II as amended)	NIST 800-60 identifier for Associated Information Type	Confidentiality	Integrity	Availability

2. SYSTEM ENVIRONMENT

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note: *this does not require depicting every workstation or desktop*, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram.

Description:
Orchestrated Repository for the Enterprise (ORE) is a strategic platform designed to provide governance, risk and compliance through an orchestrated repository ecosystem. The ORE provides highly secure content management, archival platform, and data orchestration system gateway to the modern data repository ecosystem. The zero trust design ensures both the insider and external threats cannot view, manipulate, or download any unauthorized data: a true “insider threat” prevention system.

Purpose:

Environment:

The ORE system will be located both physically and logically within the Navy environment. The ORE is composed of 5 virtual machines. Two for the ORE application, two for the database, and one for block and NFS storage. The ORE application is stateless and can run on any number of hosts. It stores documents on any network storage capable of being made available to the filesystem, such as NFS, SMB, iSCSI, etc. The ORE stores videos on S3 compatible block storage. The ORE persists document and video metadata, policies, configurations in the MySQL database. ORE is a cloud native system and the application is packaged as Docker containers and is running on a container runtime that can support Docker images. The ORE will also leverage the Navy security and firewall features to provide improved access and application protections.

Laws and Regulations:
Federal Information Security Management Act of 2002 (FISMA), 44 USC 3541 et seq., enacted as Title III of the E-Government Act of 2002, Pub L 107-347, 116 Stat 2899Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," revised, November 30, 2000National Institute of Standards and Technology (NIST) Federal Information Processing Standard FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006NIST SP 800-53, Rev 4, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009, with updated errata May 01, 2010The FedRAMP Laws and Regulations can be found on this web page: www.fedramp.gov FedRAMP Laws and Regulations Template ORE Laws and Regulations include additional laws and regulations specific to ORE. List any additional regulations hereand here, etc.

Authorization Boundary:
Placeholder

Network Architecture:

Data Flow:

Ports and Protocols:

Ports (TCP/UDP)*	Protocols	Services	Purpose	Used By
3306	TCP	Oracle MySQL	Database Communications	Oracle MySQL
443	TCP	Orchestrated Repository Enterprise	Secure Web Services	Orchestrated Repository Enterprise
443	TCP	S3 Object Storage	Store video files	S3 Object Storage

Interconnections:

SP* IP Address and Interface	External Organization Name and IP Address of System	External Point of Contact and Phone Number	Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)**	Data Direction (incoming, outgoing, or both)	Information Being Transmitted	Port or Circuit Numbers

2.1. Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component.

Name	Asset Type	Status	Owner

2.2. List all software components installed on the system.

Name	Asset Type	Status	Owner
Orchestrated Repository Enterprise		Active (On Network)	Osafo, Lloyd
Oracle MySQL		Active (On Network)	Osafo, Lloyd
MinIO		Active (On Network)	Osafo, Lloyd
Docker Engine		Active (On Network)	Osafo, Lloyd
Keycloak		Active (On Network)	Osafo, Lloyd

2.3. Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization?

Type	Count
Hardware Internally Managed	0
Software Internally Managed	0
Hardware Externally Managed	0
Software Externally Managed	0

3. REQUIREMENTS

(Note: The source of the requirements is NIST Special Publication 800-171, dated December 2016)

Provide a thorough description of how all of the security requirements are being implemented or planned to be implemented. The description for each security requirement contains: 1) the security requirement number and description; 2) how the security requirement is being implemented or planned to be implemented; and 3) any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the requirement is not applicable to the system, provide rationale.

3.1. Access Control

ac-1 Policy and Procedures

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-2 Account Management

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-2.1 Automated System Account Management

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-2.2 Automated Temporary and Emergency Account Management

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-2.3 Disable Accounts

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-2.4 Automated Audit Actions

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-2.5 Inactivity Logout

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-2.13 Disable Accounts for High-risk Individuals

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-3 Access Enforcement

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-4 Information Flow Enforcement

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-5 Separation of Duties

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-6 Least Privilege

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-6.1 Authorize Access to Security Functions

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-6.2 Non-privileged Access for Nonsecurity Functions

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-6.5 Privileged Accounts

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-6.7 Review of User Privileges

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-6.9 Log Use of Privileged Functions

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-6.10 Prohibit Non-privileged Users from Executing Privileged Functions

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-7 Unsuccessful Logon Attempts

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-8 System Use Notification

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-11 Device Lock

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-11.1 Pattern-hiding Displays

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-12 Session Termination

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-14 Permitted Actions Without Identification or Authentication

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-17 Remote Access

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-17.1 Monitoring and Control

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-17.2 Protection of Confidentiality and Integrity Using Encryption

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-17.3 Managed Access Control Points

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-17.4 Privileged Commands and Access

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-18 Wireless Access

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-18.1 Authentication and Encryption

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-18.3 Disable Wireless Networking

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-19 Access Control for Mobile Devices

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-19.5 Full Device or Container-based Encryption

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-20 Use of External Systems

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-20.1 Limits on Authorized Use

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-20.2 Portable Storage Devices — Restricted Use

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-21 Information Sharing

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ac-22 Publicly Accessible Content

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

3.2. Awareness and Training

at-3 Role-based Training

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

at-4 Training Records

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

at-1 Policy and Procedures

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

at-2 Literacy Training and Awareness

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

at-2.2 Insider Threat

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

at-2.3 Social Engineering and Mining

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

3.3. Audit and Accountability

au-1 Policy and Procedures

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-2 Event Logging

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-3 Content of Audit Records

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-3.1 Additional Audit Information

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-4 Audit Log Storage Capacity

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-5 Response to Audit Logging Process Failures

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-6 Audit Record Review, Analysis, and Reporting

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-6.1 Automated Process Integration

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-6.3 Correlate Audit Record Repositories

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-7 Audit Record Reduction and Report Generation

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-7.1 Automatic Processing

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-8 Time Stamps

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-9 Protection of Audit Information

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-9.4 Access by Subset of Privileged Users

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-11 Audit Record Retention

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

au-12 Audit Record Generation

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

3.4. Configuration Management

cm-1 Policy and Procedures

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-2 Baseline Configuration

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-2.2 Automation Support for Accuracy and Currency

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-2.3 Retention of Previous Configurations

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-2.7 Configure Systems and Components for High-risk Areas

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-3 Configuration Change Control

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-3.2 Testing, Validation, and Documentation of Changes

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-3.4 Security and Privacy Representatives

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-4 Impact Analyses

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-4.2 Verification of Controls

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-5 Access Restrictions for Change

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-6 Configuration Settings

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-7 Least Functionality

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-7.1 Periodic Review

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-7.2 Prevent Program Execution

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-7.5 Authorized Software — Allow-by-exception

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-8 System Component Inventory

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-8.1 Updates During Installation and Removal

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-8.3 Automated Unauthorized Component Detection

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-9 Configuration Management Plan

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-10 Software Usage Restrictions

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-11 User-installed Software

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-12 Information Location

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

cm-12.1 Automated Tools to Support Information Location

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

3.5. Identification and Authentication

ia-1 Policy and Procedures

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-2 Identification and Authentication (Organizational Users)

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-2.1 Multi-factor Authentication to Privileged Accounts

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-2.2 Multi-factor Authentication to Non-privileged Accounts

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-2.8 Access to Accounts — Replay Resistant

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-2.12 Acceptance of PIV Credentials

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-3 Device Identification and Authentication

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-4 Identifier Management

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-4.4 Identify User Status

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-5 Authenticator Management

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-5.1 Password-based Authentication

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-5.2 Public Key-based Authentication

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-5.6 Protection of Authenticators

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-6 Authentication Feedback

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-7 Cryptographic Module Authentication

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-8 Identification and Authentication (non-organizational Users)

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-8.1 Acceptance of PIV Credentials from Other Agencies

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-8.2 Acceptance of External Authenticators

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-8.4 Use of Defined Profiles

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-11 Re-authentication

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-12 Identity Proofing

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-12.2 Identity Evidence

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-12.3 Identity Evidence Validation and Verification

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ia-12.5 Address Confirmation

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

3.6. Incident Response

ir-7 Incident Response Assistance

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-7.1 Automation Support for Availability of Information and Support

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-8 Incident Response Plan

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-1 Policy and Procedures

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-2 Incident Response Training

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-2.1 Simulated Events

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-3 Incident Response Testing

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-3.2 Coordination with Related Plans

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-4 Incident Handling

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-4.1 Automated Incident Handling Processes

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-4.4 Information Correlation

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-5 Incident Monitoring

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-5.1 Automated Tracking, Data Collection, and Analysis

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-6 Incident Reporting

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-6.1 Automated Reporting

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ir-6.3 Supply Chain Coordination

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

3.7. Maintenance

ma-1 Policy and Procedures

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ma-2 Controlled Maintenance

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ma-3 Maintenance Tools

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ma-3.1 Inspect Tools

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ma-3.2 Inspect Media

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ma-3.3 Prevent Unauthorized Removal

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ma-4 Nonlocal Maintenance

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ma-5 Maintenance Personnel

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ma-6 Timely Maintenance

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

3.8. Media Protection

mp-1 Policy and Procedures

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

mp-2 Media Access

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

mp-3 Media Marking

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

mp-4 Media Storage

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

mp-5 Media Transport

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

mp-6 Media Sanitization

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

mp-7 Media Use

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

3.9. Personnel Security

ps-1 Policy and Procedures

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ps-2 Position Risk Designation

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ps-3 Personnel Screening

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ps-4 Personnel Termination

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ps-4.2 Automated Actions

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ps-5 Personnel Transfer

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ps-6 Access Agreements

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ps-7 External Personnel Security

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ps-8 Personnel Sanctions

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ps-9 Position Descriptions

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

3.10. Physical Protection

3.11. Risk Assessment

ra-3 Risk Assessment

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ra-1 Policy and Procedures

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ra-2 Security Categorization

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ra-3.1 Supply Chain Risk Assessment

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ra-5 Vulnerability Monitoring and Scanning

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ra-5.2 Update Vulnerabilities to Be Scanned

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

ra-5.5 Privileged Access

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

ra-5.11 Public Disclosure Program

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ra-7 Risk Response

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

ra-9 Criticality Analysis

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

3.12. Security Assessment

3.13. System and Communications Protection

sc-1 Policy and Procedures

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

sc-2 Separation of System and User Functionality

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-4 Information in Shared System Resources

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-5 Denial-of-service Protection

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-7 Boundary Protection

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

sc-7.3 Access Points

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-7.4 External Telecommunications Services

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-7.5 Deny by Default — Allow by Exception

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-7.7 Split Tunneling for Remote Devices

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-7.8 Route Traffic to Authenticated Proxy Servers

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-8 Transmission Confidentiality and Integrity

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-8.1 Cryptographic Protection

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-10 Network Disconnect

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-12 Cryptographic Key Establishment and Management

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-13 Cryptographic Protection

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-15 Collaborative Computing Devices and Applications

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-17 Public Key Infrastructure Certificates

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-18 Mobile Code

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-20 Secure Name/address Resolution Service (authoritative Source)

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-21 Secure Name/address Resolution Service (recursive or Caching Resolver)

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-22 Architecture and Provisioning for Name/address Resolution Service

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-23 Session Authenticity

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-28 Protection of Information at Rest

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-28.1 Cryptographic Protection

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

sc-39 Process Isolation

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

3.14. System and Information Integrity

si-1 Policy and Procedures

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

si-2 Flaw Remediation

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

si-2.2 Automated Flaw Remediation Status

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

si-3 Malicious Code Protection

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

si-4 System Monitoring

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

si-4.2 Automated Tools and Mechanisms for Real-time Analysis

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

si-4.4 Inbound and Outbound Communications Traffic

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

si-4.5 System-generated Alerts

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

si-5 Security Alerts, Advisories, and Directives

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

si-7 Software, Firmware, and Information Integrity

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

si-7.1 Integrity Checks

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

si-7.7 Integration of Detection and Response

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

si-8 Spam Protection

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

si-8.2 Automatic Updates

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

si-10 Information Input Validation

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

si-11 Error Handling

☐ Implemented ☒ Planned to be Implemented ☐ Not Applicable

si-12 Information Management and Retention

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

si-16 Memory Protection

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

4. RECORD OF CHANGES

Date	Description	Made By: