FedRAMP

SYSTEM SECURITY PLAN

Prepared by

Identification of Organization that Prepared this Document		
	Organization Name	
	Street Address	
	Suite/Room/Building	
	City, State Zip	

Prepared for

Identification of Cloud Service Provider		
	Organization Name	
	Street Address	
	Suite/Room/Building	
	City, State Zip	

TEMPLATE REVISION HISTORY

Date	Description
1/21/2013	Original publication
6/6/2014	Major revision for SP800-53 Revision 4. Includes new template and formatting changes.
6/6/2018	Revised controls for language consistency and updated Attachment 3

Date	Description
6/20/2016	Reformatted to FedRAMP Document Standard, added repeated text schema and content fields to tables that were not Control Tables. Revised cover page, changed document designation to Controlled Unclassified Information (CUI), Removed front matter section How This Document is Organized, Instructions re-written, Corrected section numbering to match SSP v1.0, Revised Section 9 Table 9-1 Personnel Roles and Privileges, Removed Section 10 inventory tables (see Attachment 13 FedRAMP Inventory Workbook). Global verbiage change, Authorizing Official (AO) changed to JAB/AO; e-Authentication, e-authentication and E-authentication changed to E-Authentication. Added attachments 10 FIPS 199, 11 Separation of Duties Matrix, 12 FedRAMP Laws and Regulations, 13 FedRAMP Inventory Workbook. Changes to the following controls: AC-02 (05), AC-05, AC-17 (09), AU-03 (01), AU-05, AU-06, CA-02 (03), CA-7, CM-02 (01), IA-02 (11), MP-03, PL-08, SA-09 (01), SC-15, SI-04 (04)
10/21/2016	Removed tables in Sec 15.12 FedRAMP Laws and Regulations Removed revision history tables in all of Sec 15 Removed Acronyms - see FedRAMP Master Acronyms and Glossary resource document Added PTA to Sec 15.4 PTA and PIA Added E-Authentication to Sec 15.3 Added FIPs to Sec 15.10 FIPS 199 Changed Inventory instruction and guidance Sec 10 and Attachment 13 Removed chapter numbers from Attachments Removed 3 questions from Sec 2.3 E-Authentication Determination
3/6/2017	Document renamed from "FedRAMP System Security Plan (SSP) Moderate Baseline Master Template to "FedRAMP System Security Plan (SSP) Moderate Baseline Template"
6/6/2017	Updated logo
8/28/2018	Revised controls for language consistency, updated section 2.3 and Attachment 3, added guidance to SA -9, updated requirements in RA-5
5/18/2021	Revised SA-4 Additional FedRAMP Requirements and Guidance

DOCUMENT REVISION HISTORY

Date	Description	Version of SSP	Author
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>

How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact *info@FedRAMP.gov*

For more information about the FedRAMP project, see www.FedRAMP.gov

Note that "-1" Controls (AC-1, AU-1, SC-1, etc.)* cannot be inherited and must be described in some way by the service provider.
*Access Control (AC), Audit and Accountability (AU), System and Communications Protection (SC)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

System Security Plan Approvals

Cloud Service Provider Signatures

Name <Enter Name> Date <Select Date>

Title <Enter Title>

Cloud Service Provider CSP Name

Name <Enter Name> Date <Select Date>

Title <Enter Title>

Cloud Service Provider CSP Name

Name <Enter Name> Date <Select Date>

Title <Enter Title>

Cloud Service Provider	CSP Name

1. INFORMATION SYSTEM NAME/TITLE

This System Security Plan provides an overview of the security requirements for the Orchestrated Repository for the Enterprise (ORE) and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the ORE information system.

The security safeguards implemented for the ORE system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Table 1-1. Information System Name and Title

Unique Identifier	Information System Name	Information System
<Enter FedRAMP Application Number>	Orchestrated Repository for the	ORE

2. INFORMATION SYSTEM CATEGORIZATION

The overall information system sensitivity categorization is recorded in Table 2-1. Security Categorization that follows. Directions for attaching the FIPS 199 document may be found in the following section: **Error! Reference source not found.**.

Table 2-1. Security Categorization

System Sensitivity Level:	Moderate

2.1. Information Types

This section describes how the information types used by the information system are categorized for confidentiality, integrity and availability sensitivity levels.

The following tables identify the information types that are input, stored, processed and/or output from ORE. The selection of the information types is based on guidance provided by Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office Business Reference Model 2.0 and FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems which is based on NIST Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

The tables also identify the security impact levels for confidentiality, integrity and availability for each of the information types expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity and availability) discussed in NIST SP 800-60 and FIPS Pub 199.

The potential impact is low if—

- The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
- The potential impact is moderate if—
- The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
- The potential impact is high if—
- The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Example:

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
System Development	C.3.5.1	Low	Moderate	Low

Table 2-2. Sensitivity Categorization of Information Types

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

2.2. Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2-2. Sensitivity Categorization of Information Types, for the ORE, default to the high-water mark for the Information Types as identified in Table 2-3. Security Impact Level below.

Table 2-3. Security Impact Level

Security Objective	Low, Moderate or High
Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate

Through review and analysis, it has been determined that the baseline security categorization for the ORE system is listed in the Table 2-4. Baseline Security Configuration that follows.

Table 2-4. Baseline Security Configuration

ORE Security Categorization	Moderate

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

2.3. Digital Identity Determination

The digital identity information may be found in **Error! Reference source not found.**

Note: NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.

The digital identity level is Choose an item.

Additional digital identity information can be found in Section 15 Attachmentss Digital Identity Level Selection.

3. INFORMATION SYSTEM OWNER

The following individual is identified as the system owner or functional proponent/advocate for this system.

Table 3-1. Information System Owner

Information System Owner Information	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

4. AUTHORIZING OFFICIAL

The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the *Insert AO information as instructed above*.

5. OTHER DESIGNATED CONTACTS

The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

Table 5-1. Information System Management Point of Contact

Information System Management Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Table 5-2. Information System Technical Point of Contact

Information System Technical Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Instruction: Add more tables as needed.

Delete this and all other instructions from your final version of this document.

Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

6. ASSIGNMENT OF SECURITY RESPONSIBILITY

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

Table 6-1. CSP Name Internal ISSO (or Equivalent) Point of Contact

CSP Name Internal ISSO (or Equivalent) Point of Contact	
Name	Tong, Thanh
Title	
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	
Email Address	ttong@2twelvesolutions.com

Table 6-2. AO Point of Contact

AO Point of Contact	
Name	Osafo, Lloyd
Title	
Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	
Email Address	lloyd@2twelvesolutions.com

7. INFORMATION SYSTEM OPERATIONAL STATUS

The system is currently in the life-cycle phase shown in Table 7-1. System Status that follows. (Only operational systems can be granted an ATO).

Table 7-1. System Status

System Status		
□	Operational	The system is operating and in production.
☒	Under Development	The system is being designed, developed, or implemented
□	Major Modification	The system is undergoing a major change, development, or transition.
□	Other	Explain: Click here to enter text.

8. INFORMATION SYSTEM TYPE

The ORE makes use of unique managed service provider architecture layer(s).

8.1. Cloud Service Models

Information systems, particularly those based on cloud architecture models, are made up of different service layers. Below are some questions that help the system owner determine if their system is a cloud followed by specific questions to help the system owner determine the type of cloud.

Question (Yes/No)	Conclusion
Does the system use virtual machines?	A no response means that system is most likely not a cloud.
Does the system have the ability to expand its capacity to meet customer demand?	A no response means that the system is most likely not a cloud.
Does the system allow the consumer to build anything other than servers?	A no response means that the system is an IaaS. A yes response means that the system is either a PaaS or a SaaS.
Does the system offer the ability to create databases?	A yes response means that the system is a PaaS.
Does the system offer various developer toolkits and APIs?	A yes response means that the system is a PaaS.
Does the system offer only applications that are available by obtaining a login?	A yes response means that system is a SaaS. A no response means that the system is either a PaaS or an IaaS.

The layers of the ORE defined in this SSP are indicated in Table 8-1. Service Layers Represented in this SSP that follows.

Table 8-1. Service Layers Represented in this SSP

Service Provider Architecture Layers		
□	Software as a Service (SaaS)	Major Application
□	Platform as a Service (PaaS)	Major Application
□	Infrastructure as a Service (IaaS)	General Support System
□	Other	Explain: Click here to enter text.

Note: Refer to NIST SP 800-145 for information on cloud computing architecture models.

8.2. Cloud Deployment Models

Information systems are made up of different deployment models. The deployment models of the ORE that are defined in this SSP and are not leveraged by any other FedRAMP Authorizations, are indicated in Table 8-2. Cloud Deployment Model Represented in this SSP that follows.

Table 8-2. Cloud Deployment Model Represented in this SSP

Service Provider Cloud Deployment Model		
□	Public	Cloud services and infrastructure supporting multiple organizations and agency clients
□	Private	Cloud services and infrastructure dedicated to a specific organization/agency and no other clients
□	Government Only Community	Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations
□	Hybrid	Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data) Click here to enter text.

8.3. Leveraged Authorizations

The ORE Choose an item leverages a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by this ORE are listed in Table 8-3. Leveraged Authorizations that follows.

Table 8-3. Leveraged Authorizations

Leveraged Information System Name	Leveraged Service Provider Owner	Date Granted
<Enter Leveraged information system name1>	<Enter service provider owner1>	<Date>
<Enter Leveraged information system name2>	<Enter service provider owner2>	<Date>
<Enter Leveraged information system name3>	<Enter service provider owner3>	<Date>

9. GENERAL SYSTEM DESCRIPTION

This section includes a general description of the ORE.

9.1. System Function or Purpose

9.2. Information System Components and Boundaries

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9-1 Authorization Boundary Diagram below.

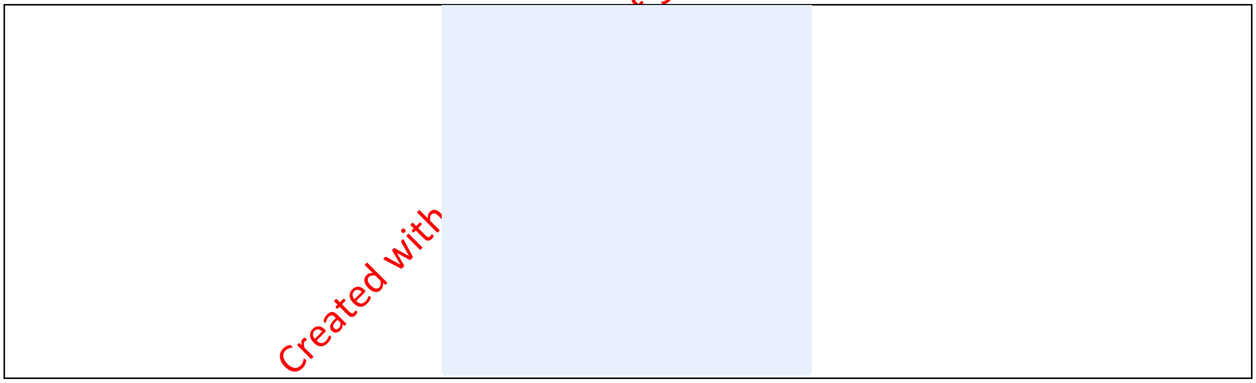

Figure 9-1 Authorization Boundary Diagram

9.3. Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 9-1. Personnel Roles and Privileges that follows.

Table 9-1. Personnel Roles and Privileges

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
UNIX System Administrator	Internal	P	Moderate	Full administrative access (root)	Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups
Client Administrator	External	NP	N/A	Portal administration	Add/remote client users. Create, modify and delete client applications
Program Director	Internal	NLA	Limited	N/A	Reviews, approves and enforces policy
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed

There are currently <number> internal personnel and <number> external personnel. Within one year, it is anticipated that there will be <number> internal personnel and <number> external personnel.

9.4. Network Architecture

Assessors should be able to easily map hardware, software and network inventories back to this diagram.

The logical network topology is shown in Figure 9-2 Network Diagram mapping the data flow between components.

The following Figure 9-2 Network Diagram(s) provides a visual depiction of the system network components that constitute ORE.

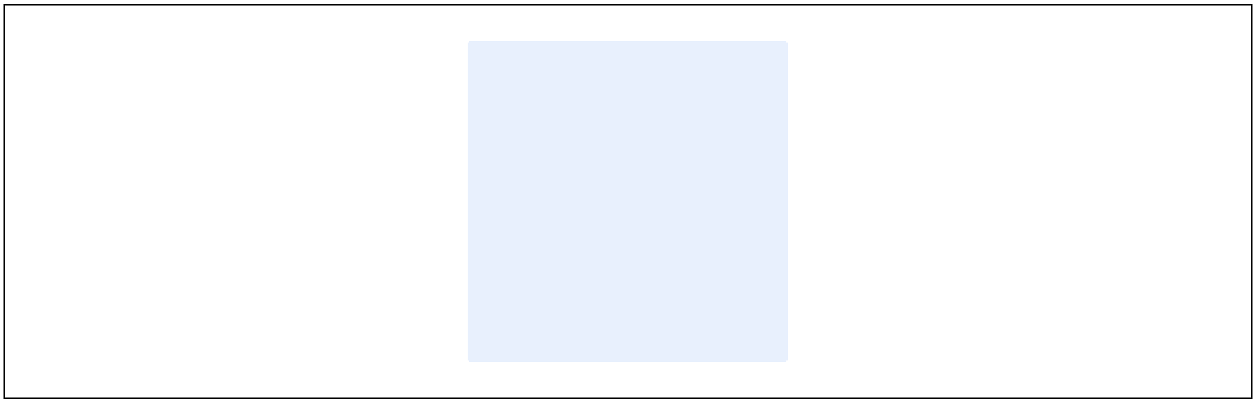

Figure 9-2 Network Diagram

10. SYSTEM ENVIRONMENT AND INVENTORY

Directions for attaching the FedRAMP Inventory Workbook may be found in the following section: **Error! Reference source not found.**.

10.1. Data Flow

The data flow in and out of the system boundaries is represented in Figure 10-1 Data Flow Diagram below.

Figure 10-1 Data Flow Diagram

10.2. Ports, Protocols and Services

Table 10-1 Ports, Protocols and Services below lists the ports, protocols and services enabled in this information system.

Table 10-1 Ports, Protocols and Services

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

* Transmission Control Protocol (TCP), User Diagram Protocol (UDP)

11. SYSTEM INTERCONNECTIONS

The Table 11-1. System Interconnections below is consistent with Table 13-3. CA-3 Authorized Connections.

Table 11-1. System 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

*Service Processor

**Internet Protocol Security (IPSec), Virtual Private Network (VPN), Secure Sockets Layer (SSL)

This document details the System Security Plan (SSP) for the Orchestrated Repository for the Enterprise (ORE) security controls. This System Security Plan was written in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Revision 1, Guide for Developing Security Plans for Information Technology Systems.&nbsp; Completion of this SSP, which describes how U.S. federal information will be safeguarded, is a requirement of the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, the Computer Security Act of 1987., 02/18/2023 18:00:00

12. LAWS, REGULATIONS, STANDARDS AND GUIDANCE

A summary of FedRAMP Laws and Regulations is included in **Error! Reference source not found.**.

12.1. Applicable Laws and Regulations

The FedRAMP Laws and Regulations can be found on this web page: Templates.

Table 12-1. Orchestrated Repository for the Enterprise Laws and Regulations includes additional laws and regulations specific to Information System Name.

Table 12-1. Orchestrated Repository for the Enterprise Laws and Regulations

Identification Number	Title	Date	Link

12.2. Applicable Standards and Guidance

The FedRAMP Standards and Guidance be found on this web page: Templates

Table 12-2. Orchestrated Repository for the Enterprise Standards and Guidance includes in this section any additional standards and guidance specific to Orchestrated Repository for the Enterprise.

Table 12-2. Orchestrated Repository for the Enterprise Standards and Guidance

Identification Number	Title	Date	Link

13. MINIMUM SECURITY CONTROLS

Security controls must meet minimum security control baseline requirements. Upon categorizing a system as Low, Moderate, or High sensitivity in accordance with FIPS 199, the corresponding security control baseline standards apply. Some of the control baselines have enhanced controls which are indicated in parentheses.

Security controls that are representative of the sensitivity of {{SSP.SECURITYPLAN.OTHERIDENTIFIER}} are described in the sections that follow. Security controls that are designated as “Not Selected” or “Withdrawn by NIST” are not described unless they have additional FedRAMP controls. Guidance on how to describe the implemented standard can be found in NIST 800-53, Rev 4. Control enhancements are marked in parentheses in the sensitivity columns.

Systems that are categorized as FIPS 199 Low use the controls designated as Low, systems categorized as FIPS 199 Moderate use the controls designated as Moderate and systems categorized as FIPS 199 High use the controls designated as High. A summary of which security standards pertain to which sensitivity level is found in Table 13-1. Summary of Required Security Controls that follows.

Table 13-1. Summary of Required Security Controls

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
AC	**Access Control**			
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12)	AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (11) (12) (13)
AC-3	Access Enforcement	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	Not Selected	AC-4 (21)	AC-4 (8) (21)
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (7) (8) (9) (10)
AC-7	Unsuccessful Logon Attempts	AC-7	AC-7	AC-7 (2)
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-10	Concurrent Session Control	Not Selected	AC-10	AC-10
AC-11	Session Lock	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	Not Selected	AC-12	AC-12 (1)
AC-14	Permitted Actions Without Identification or Authentication	AC-14	AC-14	AC-14
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4) (9)	AC-17 (1) (2) (3) (4) (9)
AC-18	Wireless Access	AC-18	AC-18 (1)	AC-18 (1) (3) (4) (5)
AC-19	Access Control For Mobile Devices	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	AC-22	AC-22	AC-22
AT	**Awareness and Training**			
AT-1	Security Awareness and Training	AT-1	AT-1	AT-1

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
	Policy and Procedures			
AT-2	Security Awareness Training	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	AT-3	AT-3	AT-3 (3) (4)
AT-4	Security Training Records	AT-4	AT-4	AT-4
AU	**Audit and Accountability**			
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Audit Events	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis and Reporting	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (4) (5) (6) (7) (10)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9 (2) (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	AU-11	AU-11	AU-11
AU-12	Audit Generation	AU-12	AU-12	AU-12 (1) (3)
CA	**Security Assessment and Authorization**			
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2 (1)	CA-2 (1) (2) (3)	CA-2 (1) (2) (3)
CA-3	System Interconnections	CA-3	CA-3 (3) (5)	CA-3 (3) (5)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Authorization	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7 (1)	CA-7 (1) (3)
CA-8	Penetration Testing	Not Selected	CA-8 (1)	CA-8 (1)
CA-9	Internal System Connections	CA-9	CA-9	CA-9
CM	**Configuration Management**			
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1) (2) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	Not Selected	CM-3 (2)	CM-3 (1) (2) (4) (6)
CM-4	Security Impact Analysis	CM-4	CM-4	CM-4 (1)

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
CM-5	Access Restrictions For Change	Not Selected	CM-5 (1) (3) (5)	CM-5 (1) (2) (3) (5)
CM-6	Configuration Settings	CM-6	CM-6 (1)	CM-6 (1) (2)
CM-7	Least Functionality	CM-7	CM-7 (1) (2) (5)*	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	CM-10	CM-10 (1)	CM-10 (1)
CM-11	User-Installed Software	CM-11	CM-11	CM-11 (1)
*FedRAMP does not include CM-7 (4) in the Moderate Baseline. NIST supplemental guidance states that CM-7 (4) is not required if (5) is implemented.				
CP	**Contingency Planning**			
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1) (2) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1) (3)	CP-9 (1) (2) (3) (5)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10 (2)	CP-10 (2) (4)
IA	**Identification and Authentication**			
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	IA-2 (1) (12)	IA-2 (1) (2) (3) (5) (8) (11) (12)	IA-2 (1) (2) (3) (4) (5) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4 (4)	IA-4 (4)
IA-5	Authenticator Management	IA-5 (1) (11)	IA-5 (1) (2) (3) (4) (6) (7) (11)	IA-5 (1) (2) (3) (4) (6) (7) (8) (11) (13)
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)
IR	**Incident Response**			
IR-1	Incident Response Policy and	IR-1	IR-1	IR-1

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
	Procedures			
IR-2	Incident Response Training	IR-2	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1) (2) (3) (4) (6) (8)
IR-5	Incident Monitoring	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1) (2)	IR-7 (1) (2)
IR-8	Incident Response Plan	IR-8	IR-8	IR-8
IR-9	Information Spillage Response	Not Selected	IR-9 (1) (2) (3) (4)	IR-9 (1) (2) (3) (4)
MA	**Maintenance**			
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools	Not Selected	MA-3 (1) (2) (3)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	MA-4	MA-4 (2)	MA-4 (2) (3) (6)
MA-5	Maintenance Personnel	MA-5	MA-5 (1)	MA-5 (1)
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6
MP	**Media Protection**			
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2	MP-2
MP-3	Media Marking	Not Selected	MP-3	MP-3
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization	MP-6	MP-6 (2)	MP-6 (1) (2) (3)
MP-7	Media Use	MP-7	MP-7 (1)	MP-7 (1)
PE	**Physical and Environmental Protection**			
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3 (1)
PE-4	Access Control For Transmission Medium	Not Selected	PE-4	PE-4
PE-5	Access Control For Output Devices	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (4)
PE-8	Visitor Access Records	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and Cabling	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
PE-11	Emergency Power	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14 (2)	PE-14 (2)
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	Not Selected	PE-18
PL	**Planning**			
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2 (3)	PL-2 (3)
PL-4	Rules of Behavior	PL-4	PL-4 (1)	PL-4 (1)
PL-8	Information Security Architecture	Not Selected	PL-8	PL-8
PS	**Personnel Security**			
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Risk Designation	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3 (3)	PS-3 (3)
PS-4	Personnel Termination	PS-4	PS-4	PS-4 (2)
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8
RA	**Risk Assessment**			
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-5	Vulnerability Scanning	RA-5	RA-5 (1) (2) (3) (5) (6) (8)	RA-5 (1) (2) (3) (4) (5) (6) (8) (10)
SA	**System and Services Acquisition**			
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	SA-3	SA-3	SA-3

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
SA-4	Acquisition Process	SA-4 (10)	SA-4 (1) (2) (8) (9) (10)	SA-4 (1) (2) (8) (9) (10)
SA-5	Information System Documentation	SA-5	SA-5	SA-5
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8
SA-9	External Information System Services	SA-9	SA-9 (1) (2) (4) (5)	SA-9 (1) (2) (4) (5)
SA-10	Developer Configuration Management	Not Selected	SA-10 (1)	SA-10 (1)
SA-11	Developer Security Testing and Evaluation	Not Selected	SA-11 (1) (2) (8)	SA-11 (1) (2) (8)
SA-12	Supply Chain Protection	Not Selected	Not Selected	SA-12
SA-15	Development Process, Standards and Tools	Not Selected	Not Selected	SA-15
SA-16	Developer-Provided Training	Not Selected	Not Selected	SA-16
SA-17	Developer Security Architecture and Design	Not Selected	Not Selected	SA-17
SC	**System and Communications Protection**			
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected	SC-3
SC-4	Information In Shared Resources	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Availability	Not Selected	SC-6	SC-6
SC-7	Boundary Protection	SC-7	SC-7 (3) (4) (5) (7) (8) (12) (13) (18)	SC-7 (3) (4) (5) (7) (8) (10) (12) (13) (18) (20) (21)
SC-8	Transmission Confidentiality and Integrity	Not Selected	SC-8 (1)	SC-8 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-12	Cryptographic Key Establishment and Management	SC-12	SC-12 (2) (3)	SC-12 (1) (2) (3)
SC-13	Cryptographic Protection	SC-13	SC-13	SC-13
SC-15	Collaborative Computing Devices	SC-15	SC-15	SC-15
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	SC-19
SC-20	Secure Name / Address Resolution Service (Authoritative Source)	SC-20	SC-20	SC-20

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name / Address Resolution Service	SC-22	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23	SC-23 (1)
SC-24	Fail in Known State	Not Selected	Not Selected	SC-24
SC-28	Protection of Information At Rest	Not Selected	SC-28 (1)	SC-28 (1)
SC-39	Process Isolation	SC-39	SC-39	SC-39
SI	**System and Information Integrity**			
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2 (2) (3)	SI-2 (1) (2) (3)
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2) (7)	SI-3 (1) (2) (7)
SI-4	Information System Monitoring	SI-4	SI-4 (1) (2) (4) (5) (14) (16) (23)	SI-4 (1) (2) (4) (5) (11) (14) (16) (18) (19) (20) (22) (23) (24)
SI-5	Security Alerts, Advisories and Directives	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	Not Selected	SI-6	SI-6
SI-7	Software, Firmware and Information Integrity	Not Selected	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Spam Protection	Not Selected	SI-8 (1) (2)	SI-8 (1) (2)
SI-10	Information Input Validation	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Handling and Retention	SI-12	SI-12	SI-12
SI-16	Memory Protection	SI-16	SI-16	SI-16

Note: The -1 Controls (AC-1, AU-1, SC-1, etc.) cannot be inherited and must be provided in some way by the service provider.

The definitions in Table 13-2. Control Origination and Definitions indicate where each security control originates.

Table 13-2. Control Origination and Definitions

Control Origination	Definition	Example
Service Provider Corporate	A control that originates from the CSP Name corporate network.	DNS from the corporate network provides address resolution services for the information system and the service offering.
Service Provider System Specific	A control specific to a particular system at the CSP Name and the control is not part of the standard corporate controls.	A unique host-based intrusion detection system (HIDs) is available on the service offering platform but is not available on the corporate network.
Service Provider Hybrid	A control that makes use of both corporate controls and additional controls specific to a particular system at the CSP Name.	There are scans of the corporate network infrastructure; scans of databases and web-based application are system specific.
Configured by Customer	A control where the customer needs to apply a configuration in order to meet the control requirement.	User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http* or https, etc.), entering an IP range specific to their organization are configurable by the customer.
Provided by Customer	A control where the customer needs to provide additional hardware or software in order to meet the control requirement.	The customer provides a SAML SSO solution to implement two-factor authentication.
Shared	A control that is managed and implemented partially by the CSP Name and partially by the customer.	Security awareness training must be conducted by both the CSPN and the customer.
Inherited from pre-existing FedRAMP Authorization	A control that is inherited from another CSP Name system that has already received a FedRAMP Authorization.	A PaaS or SaaS provider inherits PE controls from an IaaS provider.

*Hyper Text Transport Protocol (http)

Responsible Role indicates the role of CSP employee who can best respond to questions about the particular control that is described.

13.1. Access Control (AC)

AC-1 Access Control Policy and Procedures Requirements (L) (M)

The organization:

(a) Develops, documents and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

Reviews and updates the current:

(1) Access control policy [*FedRAMP Assignment: at least every 3 years*]; and

(2) Access control procedures [*FedRAMP Assignment: at least annually*].

AC-1	Control Summary Information
Responsible Role: Fraser, Doug	
ac-01_odp.01:	
ac-01_odp.02:	
ac-01_odp.03:	
ac-01_odp.04:	
ac-01_odp.05:	
ac-01_odp.06:	
ac-01_odp.07:	
ac-01_odp.08:	
Parameter AC-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

AC-1 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. ORE Information Security Policy directs the activities within the ORE Digital Identity Plan. The plan addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements to meet the control implementation requirements for the access control family of a moderate baseline.& The Access Management Plan specifically addresses procedures or processes related to: • Information Access Restriction& • The Request Fulfillment Process for Provisioning Account Access& • Managing the Administrative privileges in Agile • The Periodic Review of Access& • The Revocation of Access& • The Separation of Duties& • Access Control to Program Source Code& • Authenticator Device Management • Encryption& (Section 9.0, page 6-7) & All ORE procedures that are captured in ORE's document repository management system, are reviewed at least annually by the document owner and the Architecture Review Board (ARB). The ARB is responsible for notifying stakeholder when changes are made and approved by the ARB. This may require the creation of new documentation or reviewing and updating current procedures, annually or as needed; and policies every 3 years or as needed. & The Engineering and Operations teams are responsible for reviewing policies and procedures. The team composition includes the following: • Engineering (Product development and engineering, Product management); • Operations (Operations for Applications, Databases, Services); and • ORE Leadership (System Owner; Product Owner;); The ORE ARB is responsible for reviewing and approving the policies and procedures for the ORE environment.
Part a1	
Part a1a	
Part a1b	
Part a2	

Part b	
Part c	
Part c1	
Part c2	

AC-2 Account Management (L) (M)

The organization:

(a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];

(b) Assigns account managers for information system accounts;

(c) Establishes conditions for group and role membership;

(d) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

(e) Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;

(f) Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];

(g) Monitors the use of information system accounts;

(h) Notifies account managers:

(1) When accounts are no longer required;

(2) When users are terminated or transferred; and

(3) When individual information system usage or need-to-know changes;

(i) Authorizes access to the information system based on:

(1) A valid access authorization;
(2) Intended system usage; and
(3) Other attributes as required by the organization or associated missions/business

functions;

(j) Reviews accounts for compliance with account management requirements [*FedRAMP Assignment: at least annually*]; and

(k) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

AC-2	Control Summary Information
Responsible Role: Fraser, Doug	
ac-02_odp.01:	
ac-02_odp.02:	
ac-02_odp.03:	
ac-02_odp.04:	
ac-02_odp.05:	
ac-02_odp.06:	
ac-02_odp.07:	
ac-02_odp.08:	
ac-02_odp.09:	
ac-02_odp.10:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-2 What is the solution and how is it implemented?

<table>
<tr>
<td><b>Part a</b></td>
<td>Part A:

This control is reviewed at least annually or as needed by the ISSO and SO.

<b><u>ORE Responsibility:</u></b>
ORE has identified two account types for the ORE environment, one for each role – Operations team and Engineering team members. Operations team has full administrative access to the ORE environment. Engineering team accounts have limited administrative access within the ORE environment.
&
<u>Application</u>: ORE Application accesses are specific to each company. ORE admins do not have access to customer company. ORE admins only need access through the OS layer. Applications can only be accessed through the SSO through OIDC and/or SAML 2.0 and employs a identity provider architecture that enforces MFA or CAC/PIV authentication.
&

Access to security scanning results for the ORE are limited to ORE Operations and Engineering team members. Security scanning results are automatically generated on a continuous basis as part of the secure software development practices used by the ORE Engineering team. The ORE Engineering team makes use of CI/CD to perform vulnerability scanning and code quality scanning of the ORE applications whenever ORE code updates are pushed.

<u>Database</u>: The ORE users a MySQL database accessible only through the application. The operations team do not have& direct access to the ORE applications nor the data in the database.& They have admin access to the OS level and can see the database files, therefore able to perform backups and restore data, however they have no accounts or access to the database and cannot access any data. Customers of the ORE do not have accounts in the database. Databases are built as part of the ORE application package. Patches and updates are accomplished through automation.
&
<u>Operating System</u>: TBD
<table>
<tr><th>Account type</th><th>Functionality</th></tr>
<tr><td>Operations team</td><td>• Configures and manage user privileges
• Add, change, remove/disable user accounts
• Monitor and maintain boundary access points
• Review audit logs</td></tr>
<tr><td>Engineering Team</td><td>• Review user privileges
• Consult Operations on access requirements
• Configure application security scans</td></tr>
</table>
</td>
</tr>
</table>

2 Twelve Solutions Leadership	• Review procedures annually • Approve procedures at least annually or when there's been a major change

Customer Responsibility:

Customers are responsible for identifying account types and roles within the ORE application.

Part B:

This control is reviewed at least annually or as needed by the ISSO and SO.

&
2 Twelve Solutions Responsibility:
Operations team and the Engineering team are privileged users in ORE environment. Engineering team is dedicated account manager with limited privilege and Operations team has full privilege. Operations team implements account changes within the ORE infrastructure; Engineering team implements account changes through configuration management process. Requesting managers submit access requests through Agile system as Change Requests.& When the ARB approves a request, Agile system notifies system administrators to perform user account setup.
&
Application:& Operations team and the Engineering team are designated as account managers for infrastructure tool. The customer is responsible for the account management actions for their ORE Application instances. All ORE infrastructure remote access is provided through SSH connections to the bastion host.&
&
Database:& Each customer environment has a dedicated MySQL database accessible only through the application. ORE admins do not have direct access to customer applications nor the data in the database. Database is accessed through application where customer makes request to application and application request goes to database. On the back end, database is tied to S3 buckets for backup. 2 Twelve Solutions admins have access to the OS, instance that holds database to perform backup, apply patches and make updates through automation, but do not have direct access to database. Nessus is used to conduct vulnerability scan of the database within the ORE environment.
&
Operating System:& TBD
&
Customer Responsibility:
Customers are responsible for assigning account managers for ORE application accounts.

Part C:

This control is reviewed at least annually or as needed by the ISSO and SO.

&

2 Twelve Solutions Responsibility:

2 Twelve Solutions has established two groups for ORE system accounts – Operations team and Engineering team. Users who require administrative privileges within the ORE environment are designated as Operations team. Members of the Engineering team are defined to have administrative access to Qualys and Nessus, with read-only access within the ORE environment.

&

Application, Database, Operating System:& User permissions are granted on the principle of least privilege and role based access needs, as depicted in the 2 Twelve Solutions FedRAMP ORE Access and Identity Management Plan. Agile system ticketing system is used to document and enforce the defined workflow for all account changes. The conditions for group and role membership are dictated by the function of the individual’s role to ensure those accounts only perform the functions commensurate with business needs. There are no user accounts in database and 2 Twelve Solutions admins do not have direct access to database.

&

Customer Responsibility:

Customers are responsible for establishing roles and groups within the ORE application and the requirements for membership in such roles and groups.& The requesting manager emails itservice.2 Twelve Solutions.com or initiate a Agile system ticket to begin the approval process. The Compliance & Governance Analyst ensures that the appropriate access form is completed.& The Compliance & Governance Analyst will attach the approved clearance form to a Agile system change request.

Part D:

This control is reviewed at least annually or as needed by the ISSO and SO.

&

2 Twelve Solutions Responsibility:

2 Twelve Solutions has established two groups for ORE system accounts – Operations team and Engineering team. Users who require administrative privileges within the ORE environment are designated as Operations team. Members of the Engineering team are defined to have administrative access to Qualys and read-only access within the ORE environment.

&

Application:& ORE Application accesses are specific to each customer. ORE admins do not have access to

	customer application. After the creation of a tenant admin account during the customer onboard process, ORE administrators have no access to the customer application. 2 Twelve Solutions admins can only access the OS layer of those instances. Applications can only be accessed through the front portal through MFA or SSO through SAML 2.0. AWS Security Groups are used to define access to the ORE Application. & Access to Qualys SaaS, Nessus and Splunk is limited to the Operations team and Engineering team members. Multifactor authentication is enabled for Qualys SaaS. Qualys have agents on the instance that can scan the application monthly. Qualys agents are managed through the Qualys SaaS, which is FedRAMP approved service. Access to Nessus and Splunk must go through the SSH Bastion host.& Authentication& through the Bastion host is required for all infrastructure access to the ORE environment. The Bastion host is whitelist to only accept limited ranges of IP addresses. For the authentication process, the first step requires the user's private SSH key to authenticate against the public SSH key on the host, access to the private key is protected through a secret passphrase. The next step requires a one-time password from YubiKey. Finally the last step requires the users to supply a correct system password. & Database:& There are no user accounts in database and 2 Twelve Solutions admins do not have direct access to database. & Operating System:& For operating system access, 2 Twelve Solutions has established two groups for ORE system accounts – Operations team and Engineering team. All account changes are requested through Agile system, requiring approval from ARB. Change Management process described in CM-3 is followed to set up user account through Agile system. Users who require administrative privileges within the ORE environment are designated as Operations team. Members of the Engineering team are defined to have administrative access to Qualys and Nessus, with read-only access within the ORE environment. & **Customer Responsibility:** Customers are responsible for establishing roles and groups within the ORE application and the requirements for membership in such roles and groups. Part E: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:** The FedRAMP Security Manager must approve requests to create information system accounts. Approval are documented and tracked through Agile system tickets. Configuration management process is being followed through Agile system and documented in 2 Twelve Solutions FedRAMP ORE Access and Identity Management Plan. &

	Application:& The FedRAMP Security Manager must approve requests to create accounts on Qualys, Nessus, and Splunk. Approval are documented and tracked through Agile system tickets. Access requests require multiple levels of approvals from Operations engineers, a Security analyst, and a Privacy analyst. & Database:& Each customer environment has a dedicated PostgreSQL database accessible only through the application. ORE admins do not have direct access to customer applications nor the data in the database. Database is accessed through application where customer makes request to application and application request goes to database. On the back end, database is tied to S3 buckets for backup. 2 Twelve Solutions admins have on the system level to apply patches and make updates through automation, but do not have the ability to read data from the database. Nessus is used to conduct vulnerability scan of the database within the ORE environment. & Operating System:& The FedRAMP Security Manager must approve requests to create information system accounts. This includes access to the ORE infrastructure. Approval are documented and tracked through Agile system tickets. Agile system workflow set to enforce verification/approval process as documented in CM-3. & **Customer Responsibility:** Customers are responsible for designating approvers for ORE application accounts. Part F: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:** Application, Database, Operating System:& ORE accounts are created, enabled, modified, disabled, and removed following 2 Twelve Solutions FedRAMP ORE Access and Identity Management Plan. Once the ticket is approved by the FedRAMP manager, the Operations team will create the account(s), modify access rights, or disable accounts.& & **Customer Responsibility:** Customers are responsible for creating, enabling, modifying, disabling, and removing ORE application accounts according to their respective account management procedures. Part G:

This control is reviewed at least annually or as needed by the ISSO and SO.

&

2 Twelve Solutions Responsibility:

2 Twelve Solutions monitors the use of system accounts through the use of audit logs. Activities on the bastion host, are monitored and logged via Splunk. 2 Twelve Solutions monitors activity for AWS user accounts and account activity. Audit logs are forwarded to Splunk for review.

&

The following processes are in place to support account activity monitoring.

- All 2 Twelve Solutions ORE account activity is logged by the logging facilities defined in the response to AU-2, and events are automatically sent to a SIEM tool
- The 2 Twelve Solutions Engineering team monitors (using a SIEM tool) for system-wide account activity for application, database and operating system.
- Account creation, modification, and deletion events generate an alert in the SIEM tool for investigation.
- Account additions, modifications, or deletions require a ticket before execution.
- If any abnormal account activity is identified, the Engineering Team is immediately notified through email.
- After triage by the Engineering Team, activities are tracked using a ticketing system.

&

Reference AU-2 for additional details on audit events generated in the 2 Twelve Solutions ORE environment.

&

Application:& 2 Twelve Solutions monitors the use of system accounts through the use of audit logs. Activities on the bastion host, are monitored and logged via Splunk. 2 Twelve Solutions monitors activity for AWS user accounts and account activity. Audit logs are forwarded to Splunk for review. Account activities including account creation, deletion, modification, new instances are captured through AWS Cloudtrail and fed into Splunk. Alerts are generated through Agile system, email will be generated to Operations team, or Splunk dashboard upon login. Admin can also open and see trail for every single event, and export event as a report (pdf,doc).

&

Database:& There are no user accounts in database. The activity itself is forwarded from Postgres SQL to Splunk.

&

Operating System:& 2 Twelve Solutions monitors the use of system accounts through instance itself. Logs from ClamAV, OSSEC, rkhunter , and system events are fed into Splunk. Pre-configured thresholds and search events are set up in Splunk and will generate alert if certain threshold is exceeded. Operations and Engineering team will receive an alert via email or Agile system ticketing system.

	& **Customer Responsibility:** Customers are responsible for the review of their user actions. Application logs are available through the platform to privileged customer users. Part H: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:** Operations team is notified through Agile system when a 2 Twelve Solutions user account requires modification or disablement due to change in role (change in privileges) or termination. 2 Twelve Solutions's Human Resources is responsible to notify Engineering and Operations team of the terminated employee in order to revoke access to FedRAMP environment the same day of the termination. Operations is responsible for revoking terminated personnel's user's token immediately in conjunction with any Yubikey and/or SSH keys. & Application, Database, Operating System:& 2 Twelve Solutions utilizes the Agile system ticketing system to manage the entire lifecycle of accounts.& Changes to the accounts are initiated by Engineering or the user's manager. When the change is approved, the Engineering team and Operations team are notified via email when accounts are no longer needed due to termination, transfer or system usage change.& When users are terminated, a notification is sent to HR and the respective manager. This also triggers a notification to additional groups with information concerning the employee's last working day. That specific date is entered into the HR system to ensure accounts tied to the individual's corporate credentials are disabled on the correct day. As a result, any associated user accounts get disabled on network information systems upon the identified last working day. HR is responsible for collecting all assigned assets, according to the termination checklist.& When users are promoted or transferred to another group, user role and access rights are automatically reviewed by the new manager and any permission not required in the new role is revoked. The user's permissions are changed after proper approvals and authorization from the respective group owners is received. The ticketing system retains the tickets associated with changes to accounts and includes approvals for the changes. Personnel termination process described in PS-3. & **Customer Responsibility:** Customers are responsible for notifying their account managers when accounts are no longer required, when users are terminated or transferred, or when system usage or need-to-know changes. Part I:

This control is reviewed at least annually or as needed by the ISSO and SO.

&

2 Twelve Solutions Responsibility:

ORE users are authorized by role; specifically users are assigned either to the Operations team group or the Engineering team. Operations team is responsible for administrative activities on ORE. Engineering team is responsible for security control implementation and oversight.

&

Application, Operating System:& 2 Twelve Solutions ORE users are authorized access to the ORE environment based on valid access authorization (Operations vs Engineering) or intended usage (administrative activities vs security control implementation and/or oversights). Authorization of access assignments, valid access authorization, and intended system usage are initiated by each employee's manager who ensures that:

- Access being requested is appropriate to the individual's role and validates that the employee has completed the appropriate technical and security training for the access type being requested.
- Tickets are created in the ticketing system relating to each request
- All access (including permissions, membership to roles and groups, etc.) is required to follow the 'need to know' and 'least privilege' principles
- User permissions are granted on the principle of least privilege and role based access needs, as depicted in the 2 Twelve Solutions FedRAMP ORE Access and Identity Management Plan.

&

Database: There are no user accounts in database and 2 Twelve Solutions admins do not have direct access to database.

&

Customer Responsibility:

Customers are responsible for authorizing user access to the ORE application based on their intended system usage.

Part J:

This control is reviewed at least annually or as needed by the ISSO and SO.

&

2 Twelve Solutions Responsibility:

The CISO and Cloud Operations Manager review all 2 Twelve Solutions ORE user accounts annually to ensure compliance with account management requirements.

&

Application, Operating System:& 2 Twelve Solutions ORE user accounts are reviewed for compliance by

	the FedRAMP Manager and Engineering at least annually. Account permissions and privileges are being reviewed at least quarterly by Engineering as described in CM-5(5). Only accounts with valid access authorizations for the ORE application are permitted. Any accounts determined to be unnecessary due to prior termination or transfer are removed or disabled in accordance with account management policies and procedures. & Database:& There are no user accounts in database and 2 Twelve Solutions admins do not have direct access to database. & **Customer Responsibility:** Customers are responsible for reviewing user access to the ORE application. Part K: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Shared/group credentials are not employed within the ORE environment; all users authenticate to individual accounts used for ORE activities. & Application, Database, Operating System:& There are no shared or group accounts as part of the ORE environment. Default root accounts are considered emergency account. No group account is used for day to day operations. Operations have access to it only used for emergency. & **Customer Responsibility:** Customers are responsible for issuing and reissuing shared/group account credentials when individuals are removed from security groups for the ORE application.
Part b	
Part c	
Part d	
Part d1	
Part d2	
Part d3	
Part e	
Part f	

Part g	
Part h	
Part h1	
Part h2	
Part h3	
Part i	
Part i1	
Part i2	
Part i3	
Part j	
Part k	
Part l	

AC-2 (1) CONTROL ENHANCEMENT (M) (H)

The organization employs automated mechanisms to support the management of information system accounts.

AC-2 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
ac-02.01_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-2 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions employs Agile system tickets to track account management activities. Privileged user accounts within the ORE environment is deployed using automation scripts. SIEM is leveraged to monitor user accounts within the ORE environment. & Application, Operating System:& 2 Twelve Solutions uses automated mechanisms to support the management of accounts for the ORE application.& Agile system tickets are used for the tracking and approval of information system account creation. Account creations for the infrastructure are completed through automation. Account activities are monitored through SIEM. Management of infrastructure accounts is tracked and documented through Agile system ticketing system. The ticketing system provides automated workflow for managing the following aspects of account management: • Requests for accounts. • Approvals for account creation, modification, and removal - Permission changes. • Notifications to account owners and manager for various account management tasks. & Database: ORE admins do not have direct access to customer applications nor the data in the database. Database is accessed through application where customer makes request to application and application request goes to database. & **Customer Responsibility**: The Customer is responsible for employing automated mechanisms to support the management of ORE application accounts including: • Permission changes • Requests for accounts. • Provisioning endpoints and new users. • Approvals for account creation, modification, and removal

AC-2 (2) CONTROL ENHANCEMENT (M)

The information system automatically [*Selection: removes; disables*] temporary and emergency accounts after [*FedRAMP Assignment: no more than 30 days for temporary and emergency account types*].

AC-2 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
ac-02.02_odp.01:	
ac-02.02_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-2 (2) What is the solution and how is it implemented?
2 Twelve Solutions Responsibility: 2 Twelve Solutions does not regularly use temporary or emergency accounts. If deployed, 2 Twelve Solutions disables all temporary and emergency accounts within 30 days. & Application, Operating System:& 2 Twelve Solutions does not regularly use temporary or emergency accounts for the ORE application. If deployed, 2 Twelve Solutions disables all temporary and emergency accounts within 30 days. All accounts must go through the processes defined in AC-2. & Database: ORE admins do not have direct access to customer applications nor the data in the database. Database is accessed through application where customer makes request to application and application request goes to database. & **Customer Responsibility:** Customers are responsible for reviewing user access to the ORE application.

AC-2 (3) CONTROL ENHANCEMENT (M)

The information system automatically disables inactive accounts after [*FedRAMP Assignment: ninety (90) days for user accounts*].

AC-2 (3) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the Joint Authorization Board (JAB)/AO. Where user management is a function of the service, reports of activity of consumer users shall be made available.

AC-2 (3)	Control Summary Information
Responsible Role: Fraser, Doug	
ac-02.03_odp.01:	
ac-02.03_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-2 (3) What is the solution and how is it implemented?	
Part a	**2 Twelve Solutions Responsibility:** & Application:& Account inactivity is enforced through password expiration. Account passwords are configured to expire after 60 days. & Operating System:& Account inactivity is enforced through account expiration. Accounts on hosts are configured to expire after 60 days. & **Customer Responsibility:** Customers are responsible for monitoring the usage of user accounts and disabling after a period of inactivity.
Part b	
Part c	
Part d	

AC-2 (4) CONTROL ENHANCEMENT (M)

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [*Assignment: organization-defined personnel or roles*].

AC-2 (4)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-2 (4) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Application, Operating System:& For the ORE application, all account management activities, such as creation, modification, enabling, disabling and/or removing accounts is captured by log collector and forwarded to SIEM for review.& All account changes such as request; approval, creation, modification, and deletion of access to resources in the environment are tracked, documented, and retained in Agile system. The Operations and Engineering teams are notified via email of all account management activities. & Database:& ORE admins do not have direct access to customer applications nor the data in the database. Database is accessed through application where customer makes request to application and application request goes to database. & **Customer Responsibility:&** The Customer is responsible for automatically auditing account creation, modification, enabling, disabling, and removal actions, and notify organization personnel.

AC-2 (5) CONTROL ENHANCEMENT (M)

The organization requires that users log out when [*Assignment: organization-defined time-period of expected inactivity or description of when to log out*].

AC-2 (5) Additional FedRAMP Requirements and Guidance:

Guidance: Should use a shorter timeframe than AC-12

AC-2 (5)	Control Summary Information
Responsible Role: Fraser, Doug	
ac-02.05_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-2 (5) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE requires users to terminate sessions at the completion of task, end of the work day, and when extended period of inactivity is expected. In addition, the bastion host is configured to end user sessions after a period of 300 seconds of inactivity. & Application, Database, Operating system:& Access to the ORE tools must authenticate through the bastion host. Bastion host are configured to terminate any inactive sessions 300 seconds or longer. For infrastructure access, bastion host and instances within ORE are configured to terminate inactive sessions after 300 seconds. Infrastructure configuration settings are deployed through automation. & **Customer Responsibility:&** The Customer is responsible for requiring that users log out after 15 minutes of inactivity.

AC-2 (7) CONTROL ENHANCEMENT (M)

The organization:

(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;

Monitors privileged role assignments; and

Takes [*Assignment: organization-defined actions*] when privileged role assignments are no longer appropriate.

{{CONTROL|AC-2.7}}

AC-2 (9) CONTROL ENHANCEMENT (M)

The organization only permits the use of shared/group accounts that meet [*Assignment: organization-defined conditions for establishing shared/group accounts*].

AC-2 (9) Additional FedRAMP Requirements and Guidance: Required if shared/group accounts are deployed.

{{CONTROL|AC-2.9}}

AC-2 (10) CONTROL ENHANCEMENT (M) (H)

The information system terminates shared/group account credentials when members leave the group.

AC-2 (10) Additional FedRAMP Requirements and Guidance: Required if shared/group accounts are deployed.

{{CONTROL|AC-2.10}}

AC-2 (12) CONTROL ENHANCEMENT (M)

The organization:

(a) Monitors information system accounts for [*Assignment: organization-defined atypical use*]; and

Reports atypical usage of information system accounts to [*Assignment: organization-defined personnel or roles*].

AC-2 (12) (a) and AC-2 (12) (b) Additional FedRAMP Requirements and Guidance: Required for privileged accounts.

{{CONTROL|AC-2.12}}

AC-3 Access Enforcement (L) (M) (H)

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AC-3	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-3 What is the solution and how is it implemented?

This control is reviewed at least annually or as needed by the ISSO and SO.

&
2 Twelve Solutions Responsibility:
User permissions are granted on the principle of least privilege and role based access needs, as depicted in the 2 Twelve Solutions FedRAMP ORE Access and Digital Identity Plan. Agile system ticketing system is used to document and enforce the defined workflow for all account changes. Approved users will be added to automation playbook and granted access into the environment. The bastion host is the used to enforce privilege access into ORE. Users must provide a valid SSH key and a valid one time password from Yubikey or HSPD-12 compliant hardware to authenticate through the bastion host.
&
Application: Application accesses are specific to each customer. Firewall rules are leveraged to enforce access flow and provide logical separation such that customers only have access to their own environment. Application front end users must authenticate through MFA or SAML 2.0 token. Reverse Proxy enforces TLS1.2 encryption to protect the communication session. 2 Twelve Solutions administrators do not have access to client applications. Access to Qualys, Splunk, Nessus is limited to authorized personnel based on role based access on the principle of least privilege.
&

Database: Each customer environment has a dedicated MySQL database accessible only through the application. 2 Twelve Solutions administrators do not have access to client data. Patches and updates are accomplished through Anisble playbooks.

Operating System: Authorized 2 Twelve Solutions administrators access operating systems by authenticating through the bastion host. All users must have a valid SSH key and a one-time password from Yubikey or HSPD-12 compliant hardware token. After authenticate through the bastion host, users must have a matching public SSH key on the instance to establish connection with that host. Connections are enforced through whitelisting by Firewall rules. Creation, modification, and deletion of security groups must go through the defined CM process and requested through Agile system for ARB approval.
&
Customer Responsibility:&

The Customer is responsible for enforcing approved authorizations for logical access to ORE application and system resources in accordance with applicable access control policies

AC-4 Information Flow Enforcement (M) (H)

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [*Assignment: organization-defined information flow control policies*].

{{CONTROL|AC-4}

AC-4 (21) CONTROL ENHANCEMENT (M) (H)

The information system separates information flows logically or physically using [*Assignment: organization-defined mechanisms and/or techniques*] to accomplish [*Assignment: organization-defined required separations by types of information*].

{{CONTROL|AC-4.21}}

AC-5 Separation of Duties (M) (H)

The organization:

(a) Separates [*Assignment: organization-defined duties of individuals*];

(b) Documents separation of duties of individuals; and

(c) Defines information system access authorizations to support separation of duties.

AC-5 Additional FedRAMP Requirements and Guidance:

Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP. Directions for attaching the Separation of Duties Matrix document may be found in Section **Error! Reference source not found. Error! Reference source not found.**.

AC-5	**Control Summary Information**
Responsible Role: Fraser, Doug	
ac-05_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-5 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions separates administrator activities conducted by the Operations team from the oversight and enforcement functions conducted by the Engineering team. Operations team is provided privileges to launch automation scripts to configure the ORE environment, while the Engineering team has read only privileges in ORE. Operations team has administrative access to SIEM and read only to Qualys/Nessus and Engineering team has read only access to SIEM and administrative access to Qualys/Nessus. Please refer to AC-2(b) for more information on account management and the approval and use of security groups in the role-based access schemes. Separation of Duties is further defined through attachment 11 – 2 Twelve Solutions ORE Separation of Duties Matrix. & Application:& 2 Twelve Solutions separates administrator activities conducted by the Operations team from the oversight and enforcement functions conducted by the Engineering team. Operations team is provided privileges to launch automation scripts to configure the ORE environment, while the Engineering team has read only privileges in ORE. The Engineering team has administrator privileges for the Qualys and Nessus to scan and ensure policy compliance, while the Operations team has read only access to Qualys. & Database: Each customer environment has a dedicated MySQL database accessible only through the application. ORE admins do not have& direct access to customer applications nor the data in the database.& They have admin access to the OS level and can see the database files, therefore able to perform backups and restore data; however they have no accounts or access to the database and cannot access any data. Customers do not have accounts in the database.& Databases are built as part of the ORE application package. Patches and updates are accomplished through automation. Nessus is used to conduct vulnerability scan of the database within the ORE environment, thus separate user account. & Operating System: 2 Twelve Solutions separates administrator activities conducted by the Operations team from the oversight and enforcement functions conducted by the Engineering team. Operations team is provided privileges to launch automation scripts to configure the ORE environment, while the Engineering team has read only privileges in ORE. Operations team has administrative access to the ORE environment, but read-only to Qualys and Nessus. Engineering team accounts have read-only access within the ORE environment, but administrative access to Qualys and Nessus. & **Customer Responsibility:&** The Customer is responsible for developing and maintaining a separation of duties for privileged and non-privileged users.

Part b:

This control is reviewed at least annually or as needed by the ISSO and SO.

&

2 Twelve Solutions Responsibility:

2 Twelve Solutions separates administrator activities conducted by the Operations team from the oversight and enforcement functions conducted by the Engineering team. Operations team is provided privileges to launch automation scripts to configure the ORE environment, while the Engineering team has read only privileges in ORE. Operations team has administrative access to SIEM and read only to Qualys/Nessus and Engineering team has read only access to SIEM and administrative access to Qualys/Nessus. Please refer to AC-2(b) for more information on account management and the approval and use of security groups in the role-based access schemes. Separation of Duties is further defined through attachment 11 – 2 Twelve Solutions ORE Separation of Duties Matrix.

&

Application:& 2 Twelve Solutions separates administrator activities conducted by the Operations team from the oversight and enforcement functions conducted by the Engineering team. Operations team is provided privileges to launch automation scripts to configure the ORE environment, while the Engineering team has read only privileges in ORE. The Engineering team has administrator privileges for the Qualys and Nessus to scan and ensure policy compliance, while the Operations team has read only access to Qualys.

&

Database: Each customer environment has a dedicated MySQL database accessible only through the application. ORE admins do not have& direct access to customer applications nor the data in the database.& They have admin access to the OS level and can see the database files, therefore able to perform backups and restore data; however they have no accounts or access to the database and cannot access any data. Customers do not have accounts in the database.& Databases are built as part of the ORE application package. Patches and updates are accomplished through automation. Nessus is used to conduct vulnerability scan of the database within the ORE environment, thus separate user account.

&

Operating System: 2 Twelve Solutions separates administrator activities conducted by the Operations team from the oversight and enforcement functions conducted by the Engineering team. Operations team is provided privileges to launch automation scripts to configure the ORE environment, while the Engineering team has read only privileges in ORE. Operations team has administrative access to the ORE environment, but read-only to Qualys and Nessus. Engineering team accounts have read-only access within the ORE environment, but administrative access to Qualys and Nessus.

&

Customer Responsibility:&

The Customer is responsible for developing and maintaining a separation of duties for privileged and non-privileged users.

Part c:

This control is reviewed at least annually or as needed by the ISSO and SO.

&

2 Twelve Solutions Responsibility:

2 Twelve Solutions separates administrator activities conducted by the Operations team from the oversight and enforcement functions conducted by the Engineering team. Operations team is provided privileges to launch automation scripts to configure the ORE environment, while the Engineering team has read only privileges in ORE. Operations team has administrative access to SIEM and read only to Qualys/Nessus and Engineering team has read only access to SIEM and administrative access to Qualys/Nessus. Please refer to AC-2(b) for more information on account management and the approval and use of security groups in the role-based access schemes. Separation of Duties is further defined through attachment 11 – 2 Twelve Solutions ORE Separation of Duties Matrix.

&

Application:& 2 Twelve Solutions separates administrator activities conducted by the Operations team from the oversight and enforcement functions conducted by the Engineering team. Operations team is provided privileges to launch automation scripts to configure the ORE environment, while the Engineering team has read only privileges in ORE. The Engineering team has administrator privileges for the Qualys and Nessus to scan and ensure policy compliance, while the Operations team has read only access to Qualys.

&

Database: Each customer environment has a dedicated MySQL database accessible only through the application. ORE admins do not have& direct access to customer applications nor the data in the database.& They have admin access to the OS level and can see the database files, therefore able to perform backups and restore data; however they have no accounts or access to the database and cannot access any data. Customers do not have accounts in the database.& Databases are built as part of the ORE application package. Patches and updates are accomplished through automation. Nessus is used to conduct vulnerability scan of the database within the ORE environment, thus separate user account.

&

Operating System: 2 Twelve Solutions separates administrator activities conducted by the Operations team from the oversight and enforcement functions conducted by the Engineering team. Operations team is provided privileges to launch automation scripts to configure the ORE environment, while the Engineering team has read only privileges in ORE. Operations team has administrative access to the ORE environment, but read-only to Qualys and Nessus. Engineering team accounts have read-only access within the ORE environment, but administrative access to Qualys and Nessus.

&

Customer Responsibility:&

The Customer is responsible for developing and maintaining a separation of duties for privileged and non-privileged users.

Part b	

AC-6 Least Privilege (M) (H)

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

AC-6	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-6 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: ORE privileged users are assigned roles and privileges only sufficient to complete their assigned responsibilities. Operations team is assigned access to the bastion host with privileges to launch automation scripts for the configuration and maintenance of the ORE environment. Operations team are assigned read only access to the Qualys and Nessus. Engineering team members are assigned read-only privileges for ORE instances and administrative privileges for Qualys and Nessus. & <u>Application, Operating System</u>:& ORE privileged users are assigned roles and privileges only sufficient to complete their assigned responsibilities. Operations team has administrative access to the ORE environment, but read-only to Qualys and Nessus. Engineering team accounts have read-only access within the ORE environment, but administrative access to Qualys and Nessus. ORE employs both the 'need to know' and 'least privilege' principles, only allowing employee access to information systems necessary to accomplish assigned tasks, in accordance with organizational missions and business functions and explicitly authorizing access to specific information and information systems. Account activity is monitored through SIEM. All activities associated with granting, modifying and revoking privileged access to accounts and resources within the ORE environment must: • Have the request(s) tied to a ticket in the approved Agile system ticketing and tracking system • Have appropriate, documented approval from the data or resource owner • Follow approved change management procedures & Please refer to related controls AC-2, AC-3, and CM-7 for additional information. & <u>Database</u>:& There are no user accounts in database. The activity itself is forwarded from Postgres SQL to SIEM. ORE admins do not have direct access to customer applications nor the data in the database.& They have admin access to the OS level and can see the database files, therefore able to perform backups and restore data; however they have no accounts or access to the database and cannot access any data. Customers do not have accounts in the database. & **<u>Customer Responsibility:</u>&** The customer is responsible for employing the principle of least privilege for all access to the ORE application.

AC-6 (1) CONTROL ENHANCEMENT (M)

The organization explicitly authorizes access to [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information*].

AC-6 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
ac-06.01_odp.01:	
ac-06.01_odp.02:	
ac-06.01_odp.03:	
ac-06.01_odp.04:	
ac-06.01_odp.05:	
ac-6.1_prm_2:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-6 (1) What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions explicitly authorizes access to Operations team for the purpose of deploying automation scripts to configure and maintain the ORE environment from the bastion host. 2 Twelve Solutions also authorizes access to the AWS Console for specific individuals. The Qualys cloud for Operations team (read only) and Engineering team (administrative access), Nessus for Operations team (read only) and Engineering team (administrative access). Operations team has administrative access to SIEM and Engineering have read only access to SIEM. & Application, Operating System:& All access to systems in the ORE environment is deny by default and must be explicitly authorized following the principle of “need to know” and “least privilege”. Authorization includes access to security related functions such as establishing system accounts and configuring access authorizations (permissions, privileges). & Database:& There are no user accounts in database. The activity itself is forwarded from Postgres SQL to SIEM. ORE admins do not have direct access to customer applications nor the data in the database.& They have admin access to the OS level and can see the database files, therefore able to perform backups and restore data; however they have no accounts or access to the database and cannot access any data. Customers do not have accounts in the database. & **Customer Responsibility:&** The Customer is responsible for explicitly authorizing access to the ORE application and defined security functions.
Part b	

AC-6 (2) CONTROL ENHANCEMENT (M) (H)

The organization requires that users of information system accounts, or roles, with access to [*FedRAMP Assignment: all security functions*], use non-privileged accounts or roles, when accessing non-security functions.

> **AC-6 (2) Additional FedRAMP Requirements and Guidance:** Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting

intrusion detection parameters, system programming, system and security administration, other privileged functions.

AC-6 (2)	**Control Summary Information**
Responsible Role: Fraser, Doug	
ac-06.02_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-6 (2) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Privileged users only access the ORE environment to conduct system security functions and use their sole ORE accounts for this access. & Application, Database, Operating System:& Only privileged users, such as members of the Operations and Engineering teams have access to the ORE tool accounts (Nessus, SIEM, Qualys) for the purpose of performing administrative or security control implementation functions. ORE application access is restricted to customer account only. Infrastructure access is restricted to Operations and Engineering team. Separation of Duties matrix defines privileged and non-privileged access for users performing specific function. At this time, both Operations and Engineering accounts are considered as privileged accounts. & **Customer Responsibility:&** The Customer is responsible for requiring users of information system accounts, or roles, with access to the ORE application security functions, use non-privileged accounts or roles, when accessing non-security functions.

AC 6 (5) CONTROL ENHANCEMENT (M) (H)

The organization restricts privileged accounts on the information system to [*Assignment: organization-defined personnel or roles*].

AC-6 (5)	Control Summary Information
Responsible Role: Fraser, Doug	
ac-06.05_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-6 (5) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Only Operations team and Engineering team members are provided privileged accounts in the ORE environment. Engineering team members have read-only access, while Operations team is provided administrative privileges for the environment. & Application, Operating System:& Privileged accounts are restricted to members of the Operations and Engineering team. Engineering team members have read-only access, while Operations team is provided administrative privileges for the environment.& Through the “least privilege” and “need to know” principles, 2 Twelve Solutions ORE restricts access to privileged accounts to a very limited number of personnel with approved roles and responsibilities. Individuals with the following roles and responsibilities are given access to privileged accounts: • System Owner, ORE Leadership • VP, 2 Twelve Solutions Chief Information Security Officer , ORE Leadership • ORE Technical Director , Operations Team • Network Administrator, Operations Team • System Administrator , Operations Team • Database Administrator, Operations Team • Enginering Manager , Engineering Team • Analyst, Engineering Team • Development Manager, Engineering Team • Developer, Engineering& Team & Note: All access that is not specifically granted to a user is denied by default.& & Database:& There are no user accounts in database. The activity itself is forwarded from MySQL to SIEM. ORE admins do not have direct access to customer applications nor the data in the database.& They have admin access to the OS level and can see the database files, therefore able to perform backups and restore data; however they have no accounts or access to the database and cannot access any data. Customers do not have accounts in the database. & **Customer Responsibility:&** The customer is responsible for restricting privileged accounts on the information system to defined roles for the ORE application.

AC-6 (9) CONTROL ENHANCEMENT (M) (H)

The information system audits the execution of privileged functions.

AC-6 (9)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-6 (9) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Privileged functions are captured and forwarded to SIEM for review and monitoring by the Engineering and Operations team. All privileged actions through the AWS console are captured by the log collector and forwarded to SIEM. & Application:& All privileged functions from the ORE application are captured by log collector and forwarded SIEM for review by the Engineering team. Tenants can review their activities and events through the ORE console. When pre-defined events or triggers are detected, appropriate team are notified of the event through email. The information systems produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. & Database:& There are no user accounts in database. The activity itself is forwarded from MySQL to SIEM. ORE admins do not have direct access to customer applications nor the data in the database.& They have admin access to the OS level and can see the database files, therefore able to perform backups and restore data; however they have no accounts or access to the database and cannot access any data. Customers do not have accounts in the database. & Operating system: All privileged actions such as sudo and yum update are captured and forwarded to SIEM for near real time monitoring and alerting. Actions from Bastion hosts and all other instances are configured to feed all activities to SIEM. When pre-defined events or triggers are detected, appropriate team are notified of the event through email. The information systems produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. & **Customer Responsibility:&** The Customer is responsible for ensuring the information system audits the execution of privileged functions.

AC-6 (10) CONTROL ENHANCEMENT (M) (H)

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

AC-6 (10)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-6 (10) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Non-privileged users in the ORE application are controlled by role-based assignments to prevent execution of privileged functions. No non-privileged users have any other access to the ORE environment. & Application, Operating system:& Non-privileged users in the ORE environment are controlled by role-based assignments to prevent execution of privileged functions. No non-privileged users have any other access to the ORE environment. Separation of Duties matrix defines privileged and non-privileged access for users performing specific function. & Database:& Customers do not have accounts in the database and 2 Twelve Solutions admins also do have direct access to database. & **Customer Responsibility:&** The Customer is responsible for ensuring the ORE application prevents non-privileged users from executing privileged functions.

AC-7 Unsuccessful Login Attempts (L) (M)

The organization:

(a) Enforces a limit of [*FedRAMP Assignment: not more than three (3)*] consecutive invalid logon attempts by a user during a [*FedRAMP Assignment: fifteen (15) minutes*]; and

Automatically [*Selection: locks the account/node for a* [FedRAMP Assignment: thirty (30) *minutes*]; *delays next logon prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded.

AC-7	Control Summary Information
Responsible Role: Fraser, Doug	
ac-07_odp.01:	
ac-07_odp.02:	
ac-07_odp.03:	
ac-07_odp.04:	
ac-07_odp.05:	
ac-07_odp.06:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-7 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: & Application: For Nessus and Qualys, account lockouts are set to maximum of 3 tries, after the third unsuccessful attempt, the user account is locked until unlocked by an administrator. For SIEM, accounts are locked after 3 unsuccessful attempts within 15 minutes, the account will remain locked for 30 minutes. User can request the account to be unlocked sooner through a Agile system ticket. & Database:& There are no user accounts in database. The activity itself is forwarded from MySQL to SIEM. ORE admins do not have direct access to customer applications nor the data in the database.& They have admin access to the OS level and can see the database files, therefore able to perform backups and restore data; however they have no accounts or access to the database and cannot access any data. Customers do not have accounts in the database. & Operating System: 2 Twelve Solutions ORE personnel use multifactor authentication through bastion host and Yubikey or HSPD-12 compliant hardware to access ORE environment and locks out after three (3) failed login attempts are implemented on the bastion host and all ORE instances. Once the threshold is met, the account will be locked.& The only way to unlocking the account is to submit a ticket to have an administrator unlock the account. & **Customer Responsibility:&** The customer is responsible for enforcing a limit of 3 consecutive invalid login attempts within a 15 minute period Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: & Application: For Nessus and Qualys, account lockouts are set to maximum of 3 tries, after the third unsuccessful attempt, the user account is locked until unlocked by an administrator. For SIEM, accounts are locked after 3 unsuccessful attempts within 15 minutes, the account will remain locked for 30 minutes. User can request the account to be unlocked sooner through a Agile system ticket.

	& Database:& There are no user accounts in database. The activity itself is forwarded from MySQL to SIEM. ORE admins do not have direct access to customer applications nor the data in the database.& They have admin access to the OS level and can see the database files, therefore able to perform backups and restore data; however they have no accounts or access to the database and cannot access any data. Customers do not have accounts in the database. & Operating System: 2 Twelve Solutions ORE personnel use multifactor authentication through bastion host and Yubikey or HSPD-12 compliant hardware to access ORE environment and locks out after three (3) failed login attempts are implemented on the bastion host and all ORE instances. Once the threshold is met, the account will be locked.& The only way to unlocking the account is to submit a ticket to have an administrator unlock the account. & **Customer Responsibility:&** The customer is responsible for ensuring that the account is locked from attempting to login for at least 30 minutes once the threshold has been met.
Part b	

AC-8 System Use Notification (L) (M) (H)

The information system:

(a) Displays to users [*Assignment: organization-defined system use notification message or banner (FedRAMP Assignment: see additional Requirements and Guidance)*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

(1) Users are accessing a U.S. Government information system;
(2) Information system usage may be monitored, recorded, and subject to audit;
(3) Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
(4) Use of the information system indicates consent to monitoring and recording;

(b) Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system;

and

For publicly accessible systems:

Displays system use information [*Assignment: organization-defined conditions (FedRAMP Assignment: see additional Requirements and Guidance)*], before granting further access;

Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

Includes a description of the authorized uses of the system.

AC-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO.

Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

AC-8	Control Summary Information
Responsible Role: Fraser, Doug	
ac-08_odp.01:	
ac-08_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-8 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: As all ORE privileged users must access ORE through the bastion host and do not directly access any other system components, the system warning banner is applied at the bastion host and all other hosts on the system level. & Application, Database, Operating System:& As all ORE privileged users must access ORE through the bastion host and do not directly access any other system components, the system warning banner is applied at the bastion host and all instances within the ORE environment. The system use notifications contain explicit action language that must be taken to accept the notification before continuing to access systems. & **Customer Responsibility:&** It is the customer responsibility to determine elements of the cloud environment that require the System Use Notification control. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The warning banner is defined as part of the configuration, which is deployed through automation. Any deviation from the automation settings will be re-applied at each deployment. In addition, the banner display and content is check manually by the Operations and Engineering during each infrastructure access. The warning banner is be reviewed at least annually by the Engineering team. & **Customer Responsibility:&** It is the customer responsibility to determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. Part c:

	This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: The warning banner is defined as part of the configuration, which is deployed through automation. Any deviation from the automation settings will be re-applied at each deployment. In addition, the banner display and content is check manually by the Operations and Engineering during each infrastructure access. The warning banner is be reviewed at least annually by the Engineering team. & **<u>Customer Responsibility:</u>&** It is the customer responsibility to ensure users are presented with a warning banner prior to accessing ORE application.
Part a1	
Part a2	
Part a3	
Part a4	
Part b	
Part c	
Part c1	
Part c2	
Part c3	

Additional FedRAMP Requirements and Guidance

Requirement 1: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement 2: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO. If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement 3: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

AC-8 Req.	**Control Summary Information**
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AC-8 What is the solution and how is it implemented?	
Req. 1	
Req. 2	
Req. 3	

AC-10 Concurrent Session Control (M) (H)

The information system limits the number of concurrent sessions for each [*Assignment: organization-defined account and/or account type*] to [*FedRAMP Assignment: three (3) sessions for privileged access and two (2) sessions for non-privileged access*].

{{CONTROL|AC-10}}

AC-11 Session Lock (M) (H)

The information system:

(a) Prevents further access to the system by initiating a session lock after [*FedRAMP Assignment: fifteen (15) minutes*] of inactivity or upon receiving a request from a user; and

(b) Retains the session lock until the user reestablishes access using established identification and authentication procedures.

AC-11	Control Summary Information
Responsible Role: Fraser, Doug	
ac-11_odp.01:	
ac-11_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-11 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The bastion host disconnects the user SSH session automatically after 5 minutes, or upon request from the user. Timeout settings for all hosts within the boundary are configured through automation to 300 seconds. After 300 seconds of inactivity, the user is disconnected from ORE. & Application, Operating System:& For all infrastructure access, the bastion host disconnects the user SSH session automatically after 5 minutes, or upon request from the user. This is enforced by “ClientAliveInterval 300” and “Client AliveCountMax 0” configured on each host within the boundary including the bastion host. Access to Splunk and Nessus requires authentication through the bastion host and is identical to operating system access. Qualys is FedRAMP approved SaaS service inherited on ORE environment. & Database:& Access to database is through ORE application and 2 Twelve Solutions admins do not have direct access to database. Nessus scans are performed at least monthly on MySQL database. & **Customer Responsibility:&** It is the customer responsibility to ensure the ORE application further access to the system by initiating a session lock after 15 minutes. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The bastion host requires the user to initiate a new session and authenticate to establish a new user session. The ORE application requires the user to re-authenticate to resume the user session after the lock. & Application, Operating System:& The bastion host requires the user to initiate a new session and authenticate to establish a new user session. & Database:& Access to database is through ORE application and 2 Twelve Solutions admins do not have direct access to database. Nessus scans are performed at least monthly on MySQL database. &

	<u>Customer Responsibility:</u>& It is the customer responsibility to ensure the ORE Application retains the session lock until the user reestablishes access to the information system.
Part b	

AC-11 (1) CONTROL ENHANCEMENT (M) (H)

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

AC-11 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-11 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE enforces a session lock after fifteen minutes of inactivity for all account access.& When the session lock occurs, the login page will replace the previous displayed information. User must reestablish access using proper identification and authentication procedures. & Application, Operating System:& ORE enforces a session lock after fifteen minutes of inactivity for all account access.& When the session lock occurs, the login page will replace the previous displayed information. User must reestablish access using proper identification and authentication procedures. Timeout settings for all hosts within the boundary are configured through automation to 300 seconds. After 300 seconds of inactivity, the user is disconnected from ORE. & Database:& Access to database is through ORE application and 2 Twelve Solutions admins do not have direct access to database. Nessus scans are performed at least monthly on MySQL database. & **Customer Responsibility:&** It is the customer responsibility to ensure the ORE application conceals, via the session lock, information previously visible on the display.

AC-12 Session Termination (M) (H)

The information system automatically terminates a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

AC-12	Control Summary Information
Responsible Role: Fraser, Doug	
ac-12_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-12 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The bastion host disconnects the user SSH session automatically after 5 minutes, or upon request from the user. Timeout settings for all hosts within the boundary are configured through automation to 300 seconds. After 300 seconds of inactivity, the user is disconnected from ORE. & Application, Operating System:& For all infrastructure access, the bastion host disconnects the user SSH session automatically after 5 minutes, or upon request from the user. This is enforced by “ClientAliveInterval 300” and “Client AliveCountMax 0” configured on each host within the boundary including the bastion host. Access to Splunk and Nessus requires authentication through the bastion host and is identical to operating system access. Qualys is FedRAMP approved SaaS service inherited on ORE environment. & Database:& Access to database is through ORE application and 2 Twelve Solutions admins do not have direct access to database. Nessus scans are performed at least monthly on MySQL database. & **Customer Responsibility:&** It is the customer responsibility to ensure the ORE Application automatically terminates a user session after at least 15 minutes of inactivity.

AC-14 Permitted Actions without Identification or Authentication (L) (M) (H)

The organization:

(a) Identifies [*Assignment: organization-defined user actions*] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and

(b) Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

AC-14	Control Summary Information
Responsible Role: Fraser, Doug	
ac-14_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-14 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: All actions in the ORE environment require user authentication. Users are required to authenticate through the bastion host prior to conducting any activities in the system backend. Users are required to authenticate with Splunk and Nessus again prior to conducting any activities in those application. & Application, Operating System:& All actions in the ORE environment require user authentication. Users are required to authenticate through the bastion host prior to conducting any activities in the system backend. Users are required to authenticate with Splunk and Nessus again prior to conducting any activities in those application. No action is allowed prior to authentication through the bastion host. In addition, the bastion host is whitelisted to limited the IP range that can establish connection. & Database:& Each customer environment has a dedicated MySQL database accessible only through the application. Databases are not public facing and cannot be accessed directly. & **Customer Responsibility:&** It is the customer responsibility to ensure actions are identified that can be performed within the ORE application without identification or authentication Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: No actions are allowed in the ORE environment without authentication. The requirements for identification and authentication are documented within this SSP. For further details of the identification and authentication requirements, review IA-2 for user identification and IA-3 for device authentication. & Application, Database, Operating System:& No actions are allowed in the ORE environment without authentication. The requirements for identification and authentication to the application, database and operating system are documented within this SSP. Customer applications accessed must through the front portal via MFA or SSO through SAML 2.0. All ORE/Provider infrastructure access to 2 Twelve Solutions admins to perform administrative activities is provided through SSH connections to the bastion host. &

	Customer Responsibility:& It is the customer responsibility to ensure that all actions that can be performed without identification or authentication are fully documented.&
Part b	

AC-17 Remote Access (L) (M) (H)

The organization:

(a) Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

(b) Authorizes remote access to the information system prior to allowing such connections.

AC-17	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-17 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE privileged users are required to remotely access ORE through SSH connection to the bastion host from a 2 Twelve Solutions-defined range of IP addresses using 2 Twelve Solutions-issued laptops. The IP addresses of the 2 Twelve Solutions-issued laptops are whitelisted within the ORE environment. Attempts from any other device or IP address will be denied access. The requirements and implementation guidance for remote access is documented throughout this SSP and within access management policies and procedures and ORE Access and Digital Identity Plan. Requests and authorizations for access to the environment are managed through the following: • Ticketing system: a ticket must be submitted by the user or accounts manager. • Approval: the ticket must have the appropriate level of management approval if any of the noted activities are needed. • Change control: any activities must follow an approved change management process. Authorized individuals may connect to the environment only after they have successfully authenticated through the bastion host using valid SSH keys and Yubikey or HSPD-12 compliant hardware. There are no other access paths permitted into the ORE& infrastructure. & Application, Database, Operating System:& All access to the ORE environment and associated resources is restricted to only those assigned and approved administrators that require access and only after successful multi-factor authentication in conjunction with bastion host. ORE tools and network access is limited to Engineering and Operations team. It is the responsibility of the customer to define the usage restrictions for any partner or provisioning user accounts in their environment. Customer applications can only be accessed through the front portal through MFA or SSO through SAML 2.0. Please see AC-2 for more information on application account types and permissions. & **Customer Responsibility:&** It is the customer responsibility to establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access permitted for the ORE application. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**:

	2 Twelve Solutions authorizes remote connections to the ORE environment through the use of Agile system ticket system and system design documentation that identifies the ports and protocols in use for all communication across the system boundary. & Application, Database, and Operating System:& Approval to the ORE infrastructure is requested and approved through the established workflow within Agile system.& The requirements for identification and authentication to the application, database and operating system are documented within this SSP. ORE privileged users are required to remotely access ORE through SSH connection to the bastion host from a 2 Twelve Solutions-defined range of IP addresses using 2 Twelve Solutions-issued laptops. Customer applications accessed must through the front portal via MFA or SSO through SAML 2.0. All ORE/Provider infrastructure access to 2 Twelve Solutions admins to perform administrative activities is provided through SSH connections to the bastion host. & **Customer Responsibility:&** It is the customer responsibility to authorize remote access to the information system prior to allowing any remote access connections.
Part b	

AC-17 (1) CONTROL ENHANCEMENT (M) (H)

The information system monitors and controls remote access methods.

AC-17 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-17 (1) What is the solution and how is it implemented?

Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Remote sessions with proper authentication and identification are the only approved methods for gaining remote administrative access to the ORE environment. ORE monitors the use of remote access methods through audit logging and review. Remote sessions to the bastion host are logged on the host and forwarded to SIEM for near real time monitoring. For more detailed implementation of the monitoring in place, refer to AU-2 and AU-3 of this SSP. & Application: Logging agents running on the hosts captures audit log events and send to SIEM server. 2 Twelve Solutions ORE auditable events are selected using a risk-based approach that takes into account their information security standards. The following are deemed to be auditable events: • All administrator privileged functions • Authentication checks • Authorization checks • Data deletions, data access, data changes, and permission changes & Databases: ORE generates audit records for the following events which are then transported to a centralized audit processing tool. • Database events • SQL statements • Privileges • Schemas • Objects & Operating System: Events captured in IDS/IPS are forwarded to SIEM. 2 Twelve Solutions ORE monitors industry-wide security threats and has defined the following events as auditable events that should be captured in system audit logs based on mission/business needs: • Failed logon attempts • File integrity monitoring • Account and/or profile changes and deletions • Changes to system security settings and parameters

	• System shutdowns/restarts • Use of privileged accounts and/or activities & **Customer Responsibility:&** It is the customer responsibility to monitor and control remote access methods.

AC-17 (2) CONTROL ENHANCEMENT (M) (H)

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AC-17 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-17 (2) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Application:& ORE admins must authenticate through the bastions host via OpenSSH. All other services access is through the web browser. For customer access to the ORE application, custom certificate can be used over HTTPS in the web browser. By default, the Reverse Proxy only accepts TLS 1.2 and Digicert is leveraged as the root certificate for HTTPs connections & Database: ORE databases are not public facing and only accessible internally through ORE components. ORE databases can be accessed through the ORE application by the customer or by automation thought SSH. & Operating System:& Authorized 2 Twelve Solutions administrators access operating systems by authenticating through the bastion host.& All users must have a valid SSH key and a one-time password from Yubikey or HSPD-12 compliant hardware token. For admins, ORE accepts only remote SSH connections to the bastion host. 2 Twelve Solutions utilizes SSH key pairs generated using RSA 2048 bit size key. & **Customer Responsibility:&** It is the customer responsibility to implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions for the ORE application.

AC-17 (3) CONTROL ENHANCEMENT (M) (H)

The information system routes all remote accesses through [*Assignment: organization-defined number*] managed network access control points.

AC-17 (3)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-17 (3) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions routes all remote access through one Bastion host. ORE accepts only remote SSH connections to the bastion host.& Firewall rules restrict connections both internally between components and externally with outside networks. & Application:& ORE admins must authenticate through the bastions host via OpenSSH. All other services access is through the web browser. For customer access to the ORE application, custom certificate can be used over HTTPS in the web browser. By default, the Reverse Proxy only accepts TLS 1.2 and Digicert is leveraged as the root certificate for HTTPs connections & Database: ORE databases are not public facing and only accessible internally through ORE components. ORE databases can be accessed thought the ORE application by the customer or by automation thought SSH. & Operating System:& 2 Twelve Solutions routes all infrastructure remote access through one Bastion host. ORE accepts only remote SSH connections to the bastion host.& Firewall rules restrict connections both internally between components and externally with outside networks.& & **Customer Responsibility:&** It is the customer responsibility to route all remote accesses through a managed controlled access point.

AC-17 (4) CONTROL ENHANCEMENT (M) (H)

The organization:

(a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [*Assignment: organization-defined needs*]; and

(b) Documents the rationale for such access in the security plan for the information system.

AC-17 (4)	Control Summary Information
Responsible Role: Fraser, Doug	
ac-17.04_odp.01:	
ac-17.04_odp.02:	
Parameter AC-17(4)(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-17 (4) What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: As described in section 9 and 10 of this SSP, ORE is built entirely upon the Provider. All access to the information system is remote access. As such all privileged command usage and access to security-relevant information must be performed via remote access. & Application, Database and Operating System:& All infrastructure access to the information system is remote access. As such all privileged command usage and access to security-relevant information must be performed via remote access.& All remote access to the system is routed through bastion host for administrative access. Before ORE personnel can connect to ORE environment, they must first be approved for remote access by an authorized manager following the configuration management process and submit request through Agile system. & **Customer Responsibility:&** It is the customer responsibility to authorize the execution of privileged commands and access to security-relevant information via remote access only for administrative functions only. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: As described in section 9 and 10 of this SSP the only way to perform privileged command usage and access to security-relevant information on ORE& is via remote access since it is a cloud native service built on the Provider. The security roles and access rights are documented within this SSP, separation of duty matrix, and the access control policies and procedures. & **Customer Responsibility:&** It is the customer responsibility to document the rationale for such access in the security plan of the ORE application.
Part b	

AC-17 (9) CONTROL ENHANCEMENT (M) (H)

The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [*FedRAMP Assignment: fifteen (15) minutes*].

{{CONTROL|AC-17.9}}

AC-18 Wireless Access Restrictions (L) (M) (H)

The organization:

(a) Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

(b) Authorizes wireless access to the information system prior to allowing such connections.

AC-18	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-18 What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: As described in section 9 and 10 of this SSP, ORE is built entirely upon the Provider. All access to the information system is remote access. There is no wireless access within the ORE authorization boundary. This control is Inherited from the [Insert policy document of related control for the provider] & **Customer Responsibility:&** There is no wireless access within the authorization boundary. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: As described in section 9 and 10 of this SSP, ORE is built entirely upon the Provider. All access to the information system is remote access. There is no wireless access within the ORE authorization boundary.& This control is Inherited from the [Insert policy document of related control for the provider] & **Customer Responsibility:&** There is no wireless access within the authorization boundary.
Part b	

AC-18 (1) CONTROL ENHANCEMENT (M) (H)

The information system protects wireless access to the system using authentication of [*Selection (one or more): users; devices*] and encryption.

AC-18 (1)	**Control Summary Information**
Responsible Role: Fraser, Doug	
ac-18.01_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-18 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: As described in section 9 and 10 of this SSP, ORE is built entirely upon the Provider. All access to the information system is remote access. There is no wireless access within the ORE authorization boundary.& This control is Inherited from the [Insert policy document of related control for the provider] & **Customer Responsibility:&** There is no wireless access within the authorization boundary.

AC-19 Access Control for Portable and Mobile Systems (L) (M) (H)

The organization:

(a) Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and

(b) Authorizes the connection of mobile devices to organizational information systems.

AC-19	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-19 What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The usage of mobile devices is prohibited in ORE infrastructure. Only 2 Twelve Solutions-issued laptops may access the bastion host from a defined range of IP addresses, no other mobile devices are allowed access to the ORE environment. It should be noted that 2 Twelve Solutions laptops, similar to a customer's workstation, is not part of the authorized boundary. 2 Twelve Solutions does not have any physical assets within its authorized boundary. & **Customer Responsibility:&** It is the customer responsibility to establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The usage of mobile devices is prohibited in ORE infrastructure. Only 2 Twelve Solutions-issued laptops may access the bastion host from a defined range of IP addresses, no other mobile devices are allowed access to the ORE environment. It should be noted that 2 Twelve Solutions laptops, similar to a customer's workstation, is not part of the authorized boundary. 2 Twelve Solutions does not have any physical assets within its authorized boundary. & **Customer Responsibility:&** It is the customer responsibility to authorize the connection of mobile devices to the ORE Application.
Part b	

AC-19 (5) CONTROL ENHANCEMENT (M) (H)

The organization employs [*Selection: full-device encryption; container encryption]* to protect the confidentiality and integrity of information on [*Assignment: organization-defined mobile devices*].

AC-19 (5)	Control Summary Information
Responsible Role: Fraser, Doug	
ac-19.05_odp.01:	
ac-19.05_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-19 (5) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The usage of mobile devices is prohibited in ORE infrastructure. Only 2 Twelve Solutions-issued laptops may access the bastion host from a defined range of IP addresses, no other mobile devices are allowed access to the ORE environment. It should be noted that 2 Twelve Solutions laptops, similar to a customer's workstation, is not part of the authorized boundary. 2 Twelve Solutions does not have any physical assets within its authorized boundary. & **Customer Responsibility:&** There are no mobile devices within the authorization boundary.

AC-20 Use of External Information Systems (L) (M) (H)

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

(a) Access the information system from external information systems; and

(b) Process, store, or transmit organization-controlled information using external information systems.

AC-20	Control Summary Information
Responsible Role: Fraser, Doug	
ac-20_odp.01:	
ac-20_odp.02:	
ac-20_odp.03:	
ac-20_odp.04:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-20 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The ARB authorizes connections from ORE to other information systems through the use of Interconnection Security Agreements which documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated such as: - Authorized Connections Information System Name - Name of Organization 2 Twelve Solutions System Connects To - Role and Name of Person Who Signed Connection Agreement - Name and Date of Interconnection Agreement - SP IP Address and Interface - Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer etc.) - Data Direction (incoming, outgoing, or both) - Information Being Transmitted - Ports or Circuit # & 2 Twelve Solutions ORE Information Security Policy require that the ARB: - Reviews and updates Interconnection Security Agreements *a*t least annually and on input from program office ; and - that ORE prohibits the direct connection of defined unclassified, non-national security system& to an external network without the use of boundary protections which meet Trusted Internet Connection (TIC) requirements documented within& Appendix H – Cloud Considerations of the TIC 2.0 Reference Architecture document; https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf. ORE employs deny-all, permit by exception policy for allowing ORE to connect to external information systems & Application, Database, Operating System: The ARB authorizes connections from ORE to other information systems through the use of Interconnection Security Agreements which documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.& 2 Twelve Solutions ORE has an ISA or an agreement in place with the Provider. & **Customer Responsibility:&** It is the customer responsibility to establishes terms and conditions, consistent with any trust relationships

	established with other organizations with access to the ORE Application. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The ARB authorizes connections from ORE to other information systems through the use of Interconnection Security Agreements which documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated such as: • Authorized Connections Information System Name • Name of Organization 2 Twelve Solutions System Connects To • Role and Name of Person Who Signed Connection Agreement • Name and Date of Interconnection Agreement • SP IP Address and Interface • Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer etc.) • Data Direction (incoming, outgoing, or both) • Information Being Transmitted • Ports or Circuit # & 2 Twelve Solutions ORE Information Security Policy require that the ARB: • Reviews and updates Interconnection Security Agreements *a*t least annually and on input from FedRAMP; and • that ORE prohibits the direct connection of defined unclassified, non-national security system& to an external network without the use of boundary protections which meet Trusted Internet Connection (TIC) requirements documented within& Appendix H – Cloud Considerations of the TIC 2.0 Reference Architecture document; https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf. ORE employs deny-all, permit by exception policy for allowing ORE to connect to external information systems & Application, Database, Operating System: The ARB authorizes connections from ORE to other information systems through the use of Interconnection Security Agreements which documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.& 2 Twelve Solutions ORE has an ISA or an agreement in place with the Provider. & **Customer Responsibility:&** It is the customer responsibility to establishes terms and conditions, consistent with any trust relationships

	established with other organizations with access to the ORE Application.
Part a1	
Part a2	
Part b	

AC-20 (1) CONTROL ENHANCEMENT (M) (H)

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

(a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or

(b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

AC-20 (1)	**Control Summary Information**
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-20 (1) What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE establishes terms and conditions with other organizations in partnership. During the planning phase of the interconnection, 2 Twelve Solutions along with the intended connecting party examine all relevant technical, security and administrative issues prior to formalizing an agreement. 2 Twelve Solutions and the intended connecting firm will develop and establish a connection plan for implementing or configuring appropriate security controls once 2 Twelve Solutions has had a chance to review the connecting actor's security posture. & Application, Database, Operating System:& ORE establishes terms and conditions with other organizations in partnership. During the planning phase of the interconnection, 2 Twelve Solutions along with the intended connecting party examine all relevant technical, security and administrative issues prior to formalizing an agreement. All connections must be approved by the ARB prior to establishing connections. & **Customer Responsibility:&** It is the customer responsibility to permit authorized individuals to use an external information system to access the information system or to process, store, or transmit data or information for the ORE Application and verifies the implementation of required security controls with the external service provider. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Once the connection is established ORE relies upon and maintains interconnections through security agreements to enforce approved authorizations for controlling the flow of information within the system and between interconnected systems. For a list of approved interconnections, see Section 11, System Interconnections and CA-3 for more information. & Application, Database, Operating System:& Once the connection is established ORE relies upon and maintains interconnections through security agreements to enforce approved authorizations for controlling the flow of information within the system and between interconnected systems. All external connections are protected through encryption, enforced through AWS security group, monitored through

	SIEM, and reviewed at least annually as part of the FedRAMP assessment. & **<u>Customer Responsibility:</u>&** It is the customer responsibility to permit authorized individuals to use an external information system to access the information system or to process, store, or transmit data or information for the ORE Application and retains approved information system connection or processing agreements.
Part b	

AC-20 (2) CONTROL ENHANCEMENT (M) (H)

The organization [*Selection: restricts; prohibits*] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

AC-20 (2)	**Control Summary Information**
Responsible Role: Fraser, Doug	
ac-20.02_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-20 (2) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE prohibits the usage of portable storage devices by any authorized individual on external information systems. & The approved ORE Interconnection Security Agreements (ISA's) for all interconnections with external systems prohibit where possible, and restricts where required the use of organization controlled portable storage devices. If not prohibited, the restrictions on the use of organization controlled portable storage devices will be specified in the ISA & **Customer Responsibility:&** It is the customer responsibility to restrict or prohibit the use of organization-controlled portable storage devices connected to the ORE application or external information systems.&

AC-21 Information Sharing (M) (H)

The organization:

(a) Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and

(b) Employs [*Assignment: organization-defined automated mechanisms or manual processes*] to assist users in making information sharing/collaboration decisions.

{{CONTROL|AC-21}}

AC-22 Publicly Accessible Content (L) (M) (H)

The organization:

(a) Designates individuals authorized to post information onto a publicly accessible information system;

(b) Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

(c) Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and

(d) Reviews the content on the publicly accessible information system for nonpublic information [*FedRAMP Assignment: at least quarterly*] and removes such information, if discovered.

AC-22	Control Summary Information
Responsible Role: Fraser, Doug	
ac-22_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AC-22 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Per the NIST SP 800-53 revision 4 supplemental guidance: This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. ORE does not have publicly accessible content and requires users to authenticate before interacting with the system. & Application, Database, Operating System:& Per the NIST SP 800-53 revision 4 supplemental guidance: ORE does not have publicly accessible content and requires users to authenticate before interacting with the system. ORE is not accessible to the general public without identification or authentication. Access is only permitted to registered, authorized users with valid login credentials. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The control is not applicable. Per the NIST SP 800-53 revision 4 supplemental guidance: This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. ORE does not have publicly accessible content and requires users to authenticate before interacting with the system. & Application, Database, Operating System:& Per the NIST SP 800-53 revision 4 supplemental guidance: ORE does not have publicly accessible content and requires users to authenticate before interacting with the system. ORE is not accessible to the general public without identification or authentication. Access is only permitted to registered, authorized users with valid login credentials Part c: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**

	The control is not applicable. Per the NIST SP 800-53 revision 4 supplemental guidance: This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. ORE does not have publicly accessible content and requires users to authenticate before interacting with the system. & Application, Database, Operating System:& Per the NIST SP 800-53 revision 4 supplemental guidance: ORE does not have publicly accessible content and requires users to authenticate before interacting with the system. ORE is not accessible to the general public without identification or authentication. Access is only permitted to registered, authorized users with valid login credentials. Part d: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility** The control is not applicable. Per the NIST SP 800-53 revision 4 supplemental guidance: This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. ORE does not have publicly accessible content and requires users to authenticate before interacting with the system. & Application, Database, Operating System:& Per the NIST SP 800-53 revision 4 supplemental guidance: ORE does not have publicly accessible content and requires users to authenticate before interacting with the system. ORE is not accessible to the general public without identification or authentication. Access is only permitted to registered, authorized users with valid login credentials.
Part b	
Part c	
Part d	

13.2. Awareness and Training (AT)

AT-1 Security Awareness and Training Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

  (1) A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

  (2) Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and

(b) Reviews and updates the current:

  (1) Security awareness and training policy [*FedRAMP Assignment: at least every 3 years*]; and

  (2) Security awareness and training procedures [*FedRAMP Assignment: at least annually*].

AT-1	Control Summary Information
Responsible Role: Tong, Thanh	
at-01_odp.01:	
at-01_odp.02:	
at-01_odp.03:	
at-01_odp.04:	
at-01_odp.05:	
at-01_odp.06:	
at-01_odp.07:	
at-01_odp.08:	
Parameter AT-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

This document details the System Security Plan (SSP) for the Orchestrated Repository for the Enterprise (ORE) security controls. This System Security Plan was written in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Revision 1, Guide for Developing Security Plans for Information Technology Systems.&nbsp; Completion of this SSP, which describes how U.S. federal information will be safeguarded, is a requirement of the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, the Computer Security Act of 1987., 02/18/2023 18:00:00

AT-1 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

AT-2 Security Awareness (L) (M) (H)

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

(a) As part of initial training for new users;

(b) When required by information system changes; and

(c) [*FedRAMP Assignment: at least annually*] thereafter.

AT-2	Control Summary Information
Responsible Role: Tong, Thanh	
at-02_odp.01:	
at-02_odp.02:	
at-02_odp.03:	
at-02_odp.04:	
at-02_odp.05:	
at-02_odp.06:	
at-02_odp.07:	
Parameter AT-2(c)):	
at-2_prm_2:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AT-2 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a2	
Part b	
Part c	
Part d	
Part a1	

AT-2 (2) CONTROL ENHANCEMENT (M) (H)

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

AT-2 (2)	**Control Summary Information**
Responsible Role: Tong, Thanh	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AT-2 (2) What is the solution and how is it implemented?

AT-3 Role-Based Security Training (L) (M) (H)

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

(a) Before authorizing access to the information system or performing assigned duties;

(b) When required by information system changes; and

(c) [*FedRAMP Assignment: at least annually*] thereafter.

AT-3	Control Summary Information
Responsible Role: Tong, Thanh	
at-03_odp.01:	
at-03_odp.02:	
at-03_odp.03:	
at-03_odp.04:	
at-03_odp.05:	
Parameter AT-3(c)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AT-3 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a2	
Part b	
Part c	

AT-4 SECURITY TRAINING RECORDS (L) (M)

The organization:

(a) Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

(b) Retains individual training records for [*FedRAMP Assignment: at least one year*].

AT-4	Control Summary Information
Responsible Role: Tong, Thanh	
at-04_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AT-4 What is the solution and how is it implemented?	
Part a	
Part b	

13.3. Audit and Accountability (AU)

AU-1 Audit and Accountability Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

(b) Reviews and updates the current:

(1) Audit and accountability policy [*FedRAMP Assignment: at every 3 years*]; and

(2) Audit and accountability procedures [*FedRAMP Assignment: at least annually*].

AU-1	Control Summary Information
Responsible Role: Fraser, Doug	
au-01_odp.01:	
au-01_odp.02:	
au-01_odp.03:	
au-01_odp.04:	
au-01_odp.05:	
au-01_odp.06:	
au-01_odp.07:	
au-01_odp.08:	
Parameter AU-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

AU-1 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>** 2 Twelve Solutions ORE Information Security Policy directs the activities within the ORE System Event Logging and Alert Management Plan. The plan addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements to meet the FedRAMP control implementation requirements for the Audit and Accountability control family of a moderate baseline.& The plan specifically addresses procedures or processes related to: • Security Information and Event Management (SIEM) Tool Architecture; and • Audit Events Sources, Logging, and Alerts & All ORE procedures that are captured in Thanos document management system, 2 Twelve Solutions's document repository management system, are reviewed at least annually by the document owner and the ORE Architecture Review Board (ARB). The ARB consists of Engineering and Operations. The ARB is responsible for notifying stakeholder when changes are made and approved by the ARB. This may require the creation of new documentation or reviewing and updating current procedures, annually or as needed; and policies every 3 years or as needed. & The Operations and Engineering team are responsible for reading the document on an annual basis. The team composition includes the following: • Engineering (Development Manager and Developrs and Analysts); • Operations (Operations, Databases, and Network); and ORE Leadership (SVP, System Owner; VP, CISO; and VP, Operations); Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>** ORE policies are managed by the ISSO and SO. Part c:

	This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility** ORE policies are reviewed and updated every three years by the Operations team. The Engineering team updates the procedure annually. The ORE Leadership team approves all changes.
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

AU-2 Audit Events (L) (M) (H)

The organization:

(a) Determines that the information system is capable of auditing the following events: [*FedRAMP Assignment:* [*Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes*];

Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

Determines that the following events are to be audited within the information system:

[*FedRAMP Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited continually for each identified event*].

AU-2 Additional FedRAMP Requirements and Guidance:

Requirement: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO.

AU-2	Control Summary Information
Responsible Role: Fraser, Doug	
au-02_odp.01:	
au-02_odp.02:	
au-02_odp.03:	
au-02_odp.04:	
Parameter AU-2(d)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-2 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:** All events are logged and forwarded to SIEM, centralized logging platform. As documented in ORE& System Event Logging and Alert Management Plan, and based on the mission/business processes identified in the ORE Business Impact Analysis, ORE audits: ORE environment auditable events: & • Successful and unsuccessful account logon events • Account management events • Object access • Policy change • Privilege functions • Process tracking • System events & Application:& log collector within AWS captures audit log events and send to SIEM server. 2 Twelve Solutions ORE auditable events are selected using a risk-based approach that takes into account their information security standards. The following are deemed to be auditable events: • All administrator privileged functions • Authentication checks • Authorization checks • Data deletions, data access, data changes, and permission changes & Databases: ORE generates audit records for the following events which are then transported to a centralized audit processing tool. • Database events • SQL statements • Privileges • Schemas • Objects & Operating System: Events captured in OSSEC, ClamAV and rkhunter are forwarded to SIEM. 2 Twelve Solutions ORE monitors industry-wide security threats and has defined the following events as auditable events that should be captured in system audit logs based on mission/business needs: • Failed logon attempts

- File integrity monitoring
- Account and/or profile changes and deletions
- Changes to system security settings and parameters
- System shutdowns/restarts
- Use of privileged accounts and/or activities

&

Customer Responsibility:&

Since application access will use accounts on customer identity management solutions, auditing successful and unsuccessful logon events and account management events is a customer responsibility for customer identity management solutions. ORE will audit users accessing the system with SAML tokens and assignment of ORE roles to customer accounts including addition of roles to an account, changes of roles to an account and removal of roles from an account.

Part b:

This control is reviewed at least annually or as needed by the ISSO and SO.

&

2 Twelve Solutions Responsibility:&

Application, Database, Operating System: Engineering researches and monitors industry-wide security threats and provides the results of their assessments to other organizational entities requiring audit related information, including the 2 Twelve Solutions ORE support teams Development team if needed can be involved too to help guide the selection of auditable events. ORE uses SIEM to aggregate and generate audit log reports and alert on significant events. Event alerts and configuration of SIEM, including queries and alerts are coordinated by Engineering, jointly, through the ORE ARB.& Operations leverages the data captured in the logs to perform investigations of events within the system and determines source, vulnerability and effective remediation actions to avert future compromises.&

&

Customer Responsibility:&

Customers are responsible to coordinates the security audit function with other customer organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

Part c:

This control is reviewed at least annually or as needed by the ISSO and SO.

&

2 Twelve Solutions Responsibility:&
Application, Database, Operating System:& Audit events logged by ORE include sufficient information to support after-the-fact investigations of security incidents. The selection of auditable events is coordinated by Engineering, jointly, through the ORE& ARB.& If the auditable events defined for the system do not provide sufficient detail for investigations, additional events will be added to the list in the SSP and the audit configuration on ORE components to capture the new audit events.&
&
Customer Responsibility:&
Customers are responsible to provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

Part d:

This control is reviewed at least annually or as needed by the ISSO and SO.

&
2 Twelve Solutions Responsibility:&
ORE generates audit logs when the following events occur:

- Requests to create, read, update or delete restricted information are performed.
- A network connection is initiated or accepted.
- Access rights are granted, modified or revoked including the addition of a new user or group.
- User privileges, file permissions, firewall rules, user passwords or database object permissions are changed.
- Network, application, system or service configurations are changed.
- Installation and software patches and other software changes.
- An application is started, shutdown or restarted.
- An application is ended abnormally.
- Intrusion Prevention System, antivirus, or antispyware system detects suspicious activity.

&
Application: Events captured and described in part a and below:

- & Account and/or profile changes and deletions
- Successful and unsuccessful account login events
- Changes to system security settings and parameters
- System shutdowns/restarts
- Use of privileged accounts and/or activities
- All administrator privileged functions
- Authentication checks
- Authorization checks
- Data deletions, data access, data changes, and permission changes
- Command-line interface access and use

	& Database: Database events are captured and logged as described in part a above and below: • Database events • SQL statements • SQL injection attempts • Signature DB update failure • Privileges • Schemas • Objects • Authorization checks & Operating System: System events are audited and captured below: • Failed logon attempts • File integrity monitoring • Account and/or profile changes and deletions • Changes to system security settings and parameters • System shutdowns/restarts • Use of privileged accounts and/or activities • Authorization checks & **Customer Responsibility:**& Customers are responsible to define events that are to be audited for application access.
Part b	
Part c	
Part d	
Part e	
Part f	
Part b	

AU-2 (3) CONTROL ENHANCEMENT (M) (H)

The organization reviews and updates the audited events [*FedRAMP Assignment: annually or whenever there is a change in the threat environment*].

AU-2 (3) Additional FedRAMP Requirements and Guidance:

Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the JAB/AO.

{{CONTROL|AU-2.3}}

AU-3 Content of Audit Records (L) (M) (H)

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

AU-3	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-3 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & Application, Database, Operating System:& ORE generates audit records that contain the following information: what type of event occurred, a date/time stamp, where the event occurred in the form of IP address or hostname, the source of the event, the outcome of the event, the user ID, and the action taken. Logs captured from log collector, OSSEC, rkhunter, ClamAV, and system events are forwarded to centralized log aggregation tool, SIEM.& For other event sources the outcome of the event is implicit in the description of the action taken.& Auditing systems within the ORE environment records and maintains audit records that are sufficient to answer: • What type of activity was performed: event type and log message fields showing the component affected and whether the activity was related to authorizing, creating, reading, updating, deleting, or accepting a network connection • When the activity was performed: a timestamp showing time and date • What tools were used to perform the activity: this includes a process or transaction name or identifier. • Whether the event was a success or failure • What individuals were associated with this event: information that identifies the subject requesting the action such as a user name, computer name, IP address, and MAC address. • Where the event occurred:& information that identifies the object the action was performed on includes the resource or file names accessed and unique identifiers of records accessed in a database. **Customer Responsibility:**& Customers are responsible to generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.&
Part b	
Part c	
Part d	
Part e	
Part f	

AU-3 (1) CONTROL ENHANCEMENT (M)

The information system generates audit records containing the following additional information: [*Assignment: organization-defined additional, more detailed information*].

AU-3 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines audit record types [*FedRAMP Assignment: session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon*]. The audit record types are approved and accepted by the JAB.

Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.

AU-3 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
au-03.01_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-3 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & Application, Database, Operating System:& ORE utilizes Apache web servers to generate audit records containing the following additional information: session, connection, transaction, or activity duration; for client-server transactions,; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon. ORE utilizes Datadog to track the number of bytes received and bytes sent. & **Customer Responsibility:** & Customers are responsible to generate audit records containing the following additional information: session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon.

AU-4 Audit Storage Capacity (L) (M) (H)

The organization allocates audit record storage capacity in accordance with [*Assignment: organization-defined audit record storage requirements*].

AU-4	Control Summary Information
Responsible Role: Fraser, Doug	
au-04_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-4 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & Application, Database, Operating System:& 2 Twelve Solutions has allocated enough storage so that all ORE auditable events can be stored indefinitely. The audit log capacity for all SIEM Enterprise indexer has storage of 500 GB and can be increased as needed. Daily snapshots of the instance serve as the long term storage. When required, more storage can be added to this as it is tied to EBS volume. SIEM is configured to send out alerts and create an auto Agile system ticket when disk hits 90% threshold. Additionally, they are also backed to S3 storage through backup jobs. & **Customer Responsibility** Customers are responsible to allocates audit record storage capacity in accordance with organizational requirement

AU-5 Response to Audit Processing Failures (L) (M) (H)

The information system:

(a) Alerts [*Assignment: organization-defined personnel or roles*] in the event of an audit processing failure; and

(b) Takes the following additional actions: [*FedRAMP Assignment: organization-defined actions to be taken; (overwrite oldest record)*].

AU-5	Control Summary Information
Responsible Role: Fraser, Doug	
au-05_odp.01:	
au-05_odp.02:	
au-05_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-5 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & <u>Application, Database, Operating System:</u>& In the event that there is an audit processing failure within ORE, the Operations team will be alerted& through SIEM. Uptime monitoring will send an alert if SIEM instance goes down and logs are not being forwarded to SIEM. SIEM& is configured to send out alerts when disk is 90% full.& Operations will then confirm the disk utilization and either provision more storage or write over old space. & **<u>Customer Responsibility</u>** Customers are responsible to alert appropriate personnel in the event of an audit processing failure. Customers are responsible to define appropriate actions in the event of an audit processing failure. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & <u>Application, Database, Operating System:</u>& If audit processing fails on a ORE component, SIEM is configured to alert the Operations and Engineering team if logs are not being forwarded and if SIEM instance itself goes down. These personnel will take the action to correct the audit failure or if that is not possible, to shut down problematic server instances as needed. New instances will be instantiated as needed to resolve the audit processing failure. Depending upon the level and type of failure, the event monitoring tool sends notices to the appropriate 2 Twelve Solutions ORE administrators. These alerts are forwarded to the service operations team and the following actions are taken: • An attempt will be made to restart the audit collection. • The centralized logging platform and load balancers are inspected to determine the source of the issue. • The proper teams are followed up with depending on the error message being produced as a result of the audit processing failure. Application audit failures are remediated by the Engineering team. Appropriate action including shutting down the system component, if necessary, increasing space allocated for audit logs, and ensuring that log allocation is being performed properly. While a given component may be shut down due to audit processing failure, the entire system does not get shutdown and the environment continues to operate. & **<u>Customer Responsibility:</u>**&

	Customers are responsible to define appropriate actions in the event of an audit processing failure.
Part b	

AU-6 Audit Review, Analysis, and Reporting (L) (M) (H)

The organization:

(a) Reviews and analyzes information system audit records [*FedRAMP Assignment: at least weekly*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*]; and

(b) Reports findings to [*Assignment: organization-defined personnel or roles*].

AU-6 Additional FedRAMP Requirements and Guidance:

Requirement: Coordination between service provider and consumer shall be documented and accepted by the Authorizing Official. In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer shall be documented.

AU-6	Control Summary Information
Responsible Role: Fraser, Doug	
au-06_odp.01:	
au-06_odp.02:	
au-06_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-6 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:**& 2 Twelve Solutions DC environment has automated tools in place for the monitoring, logging, alerting, reporting and auditing the logs in real-time for indications of inappropriate or unusual activity on all virtual asset types. A centralized logging platform and SIEM tool are used to identify events and address alerts in the 2 Twelve Solutions ORE environment. All audit events are sent in near real-time to SIEM for log aggregation, analysis, and alerting on significant events. Logs are collected from the operating system, database, AWS log collector, web servers and applications.& These logs are processed in near real-time by SIEM with alerts generated for indications of inappropriate and unusual activity. The near real-time processing exceeds the DoD requirement for at least weekly review. Alerts include but are not limited to: • Successful and unsuccessful logon events • Account management events • Object access • Policy change • Privilege function • Process Tracking • System events • All Administrator activity • Authentication Checks • Authorization Checks • Data Deletion • Data Access • Data Changes • Permission Changes • Actions related to privilege change • Privilege user creation • Privileged required Deletion • Attempts to log in at the Root level & Application: log collector in AWS forwards logs to SIEM. Audit logs are reviewed in real time upon detection of suspicious activity. & Database: Database events are forwarded to SIEM. If an event triggers review, Operations and Engineering teams are alerted and Agile system ticket is created to investigate and track the event. & Operating System:& ClamAV, OSSEC, rkhunter logs are forwarded to SIEM and reviewed upon

	identification of malware or suspicious event. & **Customer Responsibility:**& Customers are responsible to review and analyze information system audit records for indications of inappropriate or unusual activity Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & Application, Database, Operating System:& Findings discovered through the analysis and review process will be reported to the Engineering team and Operations team via a Agile system ticket in accordance with the procedures of the incident response process, following the Incident Reporting Procedures. & **Customer Responsibility:** & Customers are responsible to report findings to appropriate personnel.
Part b	
Part c	

AU-6 (1) CONTROL ENHANCEMENT (M) (H)

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

AU-6 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
au-06.01_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-6 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:**& Application, Database, Operating System:& ORE utilizes SIEM to aggregate and correlate audit information and alert on significant events. SIEM integrates the audit review and reporting process, and assists in the analysis and correlation of audit records for investigation and response to suspicious activities by providing near real-time alerts to appropriate ORE personnel.& & • Centralized Logging Platform: supports the collection of the audit log data for application, infrastructure, and network devices within 2 Twelve Solutions ORE.& • SIEM tool: supports analysis of authentication and infrastructure logs to identify and alert on atypical environment activity and potential incidents. • Application Performance Monitoring Tools: used to monitor application performance activity (e.g. bandwidth, service status) and events, and to provide reporting capabilities on items such as SLAs, resource utilization, voice quality, and capacity utilization. • Intrusion Prevention System (IPS): used to detect external malicious activity affecting the 2 Twelve Solutions ORE& environment. Monitoring is performed to detect malicious events originating from the network perimeter. & **Customer Responsibility:**& Customers are responsible to employs automated mechanisms to integrate audit review, analysis, and reporting processes to support customer processes for investigation and response to suspicious activities.

AU-6 (3) CONTROL ENHANCEMENT (M) (H)

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

AU-6 (3)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-6 (3) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:**& Application, Database, Operating System:& ORE maintains a single audit log repository in SIEM with logs from server OS, Web servers, Database audit records, AWS log collector and applications being processed by SIEM in near real-time to gain organization-wide situational awareness.& The rule sets in SIEM and security alerts aggregated from& ClamAV, rkhunter& OSSEC triggers an alert and notify Engineering in near real time.& & **Customer Responsibility:**& Customers are responsible to analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

AU-7 Audit Reduction and Report Generation (M) (H)

The information system provides an audit reduction and report generation capability that:

(a) Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and

(b) Does not alter the original content or time ordering of audit records.

AU-7	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-7 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO.& **2 Twelve Solutions Responsibility:**& Application, Database, Operating System: ORE utilizes SIEM to aggregate audit information and alert on significant events, and serves as the tool for audit reduction and reporting. SIEM is implemented to analyze, reduce, and generate reports of auditable system events. SIEM allows administrators to automatically process audit record events of interest based upon selectable search criteria and supports after-the-fact investigations of security incidents. The SIEM system: • Aggregates and correlates information gathered from the components of the system • Provides single pane-of-glass management, reporting and administration. • Incorporates 5:1 compression allowing more history to be stored • Has integrated search that allows data of interest to be easily located. • Identifies data patterns, provides metrics, diagnoses problems in real-time, facilitates decision-making for application management, security, and compliance activities & **Customer Responsibility:**& Customers are responsible to audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. **2 Twelve Solutions Responsibility:**& Application, Database, Operating System:& SIEM supports on demand and after-the-fact investigations of security incidents without altering original audit records. Audit logs are protected in SIEM from modification or deletion until the defined retention period is exceeded according to ORE Record Retention Policy. Audit events are captured at local servers throughout the ORE system and are forwarded to SIEM near real time for analysis and review. Users have read-only permissions to review logs so logs cannot be altered in SIEM. Access to SIEM audit data is strictly controlled and access is provided on a need to know basis. The actual log data of the SIEM is stored on S3 compatible storage that is external to the SIEM and cannot be altered. Finally, the configuration of the SIEM forwarder agent, including which log files to forward from the server instances, is defined in /etc/grafana-agent.yaml. Data integrity check is enabled in SIEM for ORE environment.& & **Customer Responsibility:&** Customers are responsible to audit reduction and report generation capability that does not alter the

	original content or time ordering of audit records.
Part b	

AU-7 (1) CONTROL ENHANCEMENT (M) (H)

The information system provides the capability to process audit records for events of interest based on [*Assignment: organization-defined audit fields within audit records*].

AU-7 (1)	**Control Summary Information**
Responsible Role: Fraser, Doug	
au-07.01_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-7 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. **2 Twelve Solutions Responsibility:**& Application, Database, Operating System:& ORE utilizes SIEM to process audit records for events of interest based on the type of event that occurred, the date/time stamp, where the event occurred in the form of IP address or hostname, the source of the event, the outcome of the event, the user ID, and the action taken.& & **Customer Responsibility** Customers are responsible to provide the capability to process audit records for events of interest based on customer defined events.

AU-8 Time Stamps (L) (M) (H)

The information system:

(a) Uses internal system clocks to generate time stamps for audit records; and

(b) Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [*Assignment: one second granularity of time measurement*].

AU-8	Control Summary Information
Responsible Role: Fraser, Doug	
au-08_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-8 What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:**& Application, Database, Operating System:& ORE components, including server instances, use internal system clocks to generate time stamps for audit records. The ORE components' internal clocks are synchronized hourly with NIST time servers via Network Time Protocol (NTP), to provide an accurate time source for audit records.& The NIST time server used for time synchronization is http://tf.nist.gov/tf-cgi/servers.cgi. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. **2 Twelve Solutions Responsibility:**& Application, Database, Operating System:& Audit record time stamps are mapped to Coordinated Universal Time (UTC) and record date/time stamps with a granularity of one second.
Part b	

AU-8 (1) CONTROL ENHANCEMENT (M) (H)

The information system:

(a) Compares the internal information system clocks with [*FedRAMP Assignment: authoritative time source:* [*http://tf.nist.gov/tf-cgi/servers.cgi*] *[at least hourly]*]; and

(b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [*Assignment: organization-defined time period*].

AU-8 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server.

Requirement: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.

Guidance: The service provider selects primary and secondary time servers used by the NIST Internet time service, or by a Stratum-1 time server. The secondary server is selected from a different geographic region than the primary server.

If using Windows Active Directory, all servers should synchronize time with the time source for the Windows Domain Controller. If using some other directory services (e.g., LDAP), all servers should synchronize time with the time source for the directory server. Synchronization of system clocks improves the accuracy of log analysis.

{{CONTROL|AU-8.1}}

AU-9 Protection of Audit Information (L) (M) (H)

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

AU-9	Control Summary Information
Responsible Role: Fraser, Doug	
au-09_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-9 What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:**& Application, Database, Operating System:& 2 Twelve Solutions ORE uses a role-based access control model to ensure that access is commensurate with job responsibilities and approved and provisioned through the procedures documented in AC-2.& In SIEM, authentication.conf defines SIEM user roles and user groups assigned to those roles.& The authorization.conf file defines the permissions and rights assigned to each SIEM role.& ORE protects audit information and audit tools from unauthorized access, modification, and deletion. ORE utilizes SIEM as the audit record repository. As data is written to audit files, the SIEM forwarder agent on the server instances log entries to the SIEM indexer for ingestion in near real time. The Data_integrity_control is enforced by the S3 compatible storage backend. Users have web based access to the SIEM and there are no opportunities for the user to alter the data from the web interface of the SIEM. The S3 storage backend that is used to store the actual logs is separate from the SIEM and so the SIEM administrators do not have the opportunity to alter the actual log data. Only users defined in SIEM can access audit log records. Only Cloud Operations SIEM Administrators have access to the administrative capabilities of SIEM such as changing the configuration of SIEM. Typical Cloud Operations personnel and Application Support users have read only access to the SIEM audit logs. SIEM is configured with a 90 day audit log retention period before transferring to S3 storage and prevents the deletion of audit records before the retention period has expired for the records in question.& SIEM is configured to use the data integrity control option, which computes SHA-256 hashes of every slice of newly indexed raw audit data and stores the hashes within SIEM. SIEM administrators can perform an integrity check to validate that the data in an index or bucket has not been modified. Audit logs are stored in three separate location: local instance, SIEM instance and backups. Local instances are being backed up by the IaaS provider. The SIEM instances are encrypted at rest using Amazon EBS (Amazon Elastic Block Store) logical volume encryption AES-256.& Events can be recovered even if it was deleted from one instance. & **Customer Responsibility:**& Customers are responsible to protects audit information and audit tools from unauthorized access, modification, and deletion.
Part b	

AU-9 (2) CONTROL ENHANCEMENT (M) (H)

The information system backs up audit records [*FedRAMP Assignment: at least weekly*] onto a physically different system or system component than the system or component being audited.

{{CONTROL|AU-9.2}}

AU-9 (4) CONTROL ENHANCEMENT (M) (H)

The organization authorizes access to management of audit functionality to only [*Assignment: organization-defined subset of privileged users*].

AU-9 (4)	Control Summary Information
Responsible Role: Fraser, Doug	
au-09.04_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-9 (4) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:**& Application, Database, Operating System:**&** ORE limits access to management of the SIEM instance to only a small group of 2 Twelve Solutions personnel. Typical Operations personnel and Application Support users have read only access to the SIEM audit logs. The Operations team is responsible for administration of SIEM in the ORE system. The Operations team would are responsible for any changes to audit configuration in log collector and SIEM. In addition, they're responsible for managing SIEM configuration and data retention. Refer to the AC control family for additional information regarding the security and protection of audit information, specifically the authorized access by subset of privileged users. & **Customer Responsibility:**& Customers are responsible to authorizes access to management of customer audit functionality to only a defined subset of privileged users.

AU-11 Audit Record Retention (M)

The organization retains audit records for [*FedRAMP Assignment: at least ninety (90) days*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

AU-11 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements

AU-11	Control Summary Information
Responsible Role: Fraser, Doug	
au-11_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-11 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility:</u>**& <u>Application, Database, Operating System:</u>& 2 Twelve Solutions stores all ORE audit logs at least 90 days online in SIEM and three years or more offline through EBS snapshots based on customer requirement. This provides sufficient information for investigations after security incidents occur. & **<u>Customer Responsibility</u>** Customers are responsible to retains audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

AU-12 Audit Generation (L) (M) (H)

The information system:

(a) Provides audit record generation capability for the auditable events defined in AU-2 a. at [*FedRAMP Assignment: all information system components where audit capability is deployed/available*];

(b) Allows [*Assignment: organization-defined personnel or roles*] to select which auditable events are to be audited by specific components of the information system; and

(c) Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

AU-12	Control Summary Information
Responsible Role: Fraser, Doug	
au-12_odp.01:	
au-12_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

AU-12 What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:**& Application, Database, Operating System:& ORE provides for auditing on system components and generates the auditable events defined in AU-2 part a for all information system components where audit capability is deployed/available. SIEM is capable of generating events are required to generate audit events as defined by AU-2 and AU-3. System admins provide audit record generation capability for auditable events for all information system components capable of generating audit records.& Operations and Engineering can generate reports within SIEM.& Reports can be generated/exported through pre-configured searched within SIEM. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:**& Application, Database, Operating System:& ORE uses SIEM to aggregate and generate audit log reports and alert on significant events. Event alerts and configuration of SIEM, including queries and alerts are coordinated by Engineering, jointly, through Operations to enhance mutual support. The additional coordination enhances the selection of auditable events as directed by the Engineering and Operations. ISTWG and ATWG. Part c: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:**& Application, Database, Operating System:& ORE generates audit records for the events defined in AU-2 (d), with the content as defined in AU-3.& All logs are then aggregated to the SIEM for further processing and analysis.
Part a	

Part b	
Part c	
Part c	
Part d	

13.4. Security Assessment and Authorization (CA)

CA-1 Certification, Authorization, Security Assessment Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and

(a) Reviews and updates the current:

(1) Security assessment and authorization policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Security assessment and authorization procedures [*FedRAMP Assignment: at least annually*].

CA-1	Control Summary Information
Responsible Role: Fraser, Doug	
ca-01_odp.01:	
ca-01_odp.02:	
ca-01_odp.03:	
ca-01_odp.04:	
ca-01_odp.05:	
ca-01_odp.06:	
ca-01_odp.07:	
ca-01_odp.08:	
Parameter CA-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

CA-1 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed annually by the ISSO and SO. & **2 Twelve Solutions Responsibility:** 2 Twelve Solutions ORE Security Assessment and Authorization Policies and Procedures have been established to ensure applicable Security Assessment and Authorization controls and requirements are implemented. The purpose of this document is to establish policies and procedures for Security Assessment and Authorization within the ORE environment. 2 Twelve Solutions has adopted security assessment and authorization principles established within NIST 800-53 control tailored to the ORE and DoD& defined parameters.& 2 Twelve Solutions management has committed in coordinating among organizational entities, and compliance requirements to meet the DoD control implementation requirements for the system assessment and authorization control family of a moderate baseline. 2 Twelve Solutions Security Assessment and Authorization Policies and Procedure apply to all employees, management, contractors, and other users who operate within the ORE environment, including systems and devices within 2 Twelve Solutions Orchestrated Repository for the Enterprise (ORE) information system boundary. System users, groups, services, protocols and other functions are also applicable to this document. Security assessment and authorization plan addresses: & • Policies and Procedures • Security Assessments • System Interconnections • Plan of Action and Milestones • Security Authorization • Continuous Monitoring • Penetration Testing • Internal System Connections & All ORE procedures that are captured in Thanos document management system, 2 Twelve Solutions's document repository management system, are reviewed on an annual basis by the document owner and the ORE Architecture Review Board (ARB). The ARB consists of the Operations and Engineering team. The ARB is responsible for notifying stakeholders of procedures and policies when changes are made and approved by the ARB. This may require the creation of new documentation or reviewing and updating current procedures, annually or as needed; and policies every 3 years or as needed. & The Operations and Engineering team are responsible for reading the document on an annual basis. The team composition includes the following: • Engineering (Development Manager and Developrs and Analysts);

	• Operations (Operations, Databases, and Network); and • ORE Leadership (SVP, System Owner; VP, CISO; and VP, Operations); Part b: This control is reviewed annually by the ISSO and SO. **2 Twelve Solutions Responsibility:** 2 Twelve Solutions security assessment and authorization policies are reviewed at least every three years or due to major changes in the ORE environment. Security assessment and authorization procedures are reviewed and updated at least annually or due to major changes within the ORE environment. All policies and procedures reviewed and updated are approved by the Engineering team.
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

CA-2 Security Assessments (L) (M) (H)

The organization:

(a) Develops a security assessment plan that describes the scope of the assessment including:

(1) Security controls and control enhancements under assessment;
(2) Assessment procedures to be used to determine security control effectiveness; and
(3) Assessment environment, assessment team, and assessment roles and responsibilities;

(b) Assesses the security controls in the information system and its environment of operation

[*FedRAMP Assignment: at least annually*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

(c) Produces a security assessment report that documents the results of the assessment; and

(d) Provides the results of the security control assessment to [*FedRAMP Assignment: individuals or roles to include the FedRAMP Program Management Office (PMO)*].

CA-2 Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Annual Assessment Guidance https://www.fedramp.gov/documents/

CA-2	Control Summary Information
Responsible Role: Fraser, Doug	
ca-02_odp.01:	
ca-02_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CA-2 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed annually by the ISSO and SO & **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions works with the PEO Digital security assement team as part of the DoD assessment performed. The SAP aligns with DoD requirements and is approved by AO prior to testing. The SAP addresses the following: • Scope of the assessment • Assessment Procedures • Assessment environment • Rules Of Engagement • Assessment Schedule • Security controls and control enhancements under assessment Personnel roles and responsibilities within the assessment team Part b: This control is reviewed annually by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions team works with the PEO Digital security assement team on an annual basis. The security assement team& assesses all the security controls implemented for ORE for the initial authorization and tests one-third of the controls annually to determine the extent to whether the controls are implementing correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirement. The one-third of the control testing is performed with guidance from DoD Continuous Monitoring Strategy Guide.& The assessment procedure are documented and followed by 2 Twelve Solutions in NIST SP 800-37 and& & NIST SP 800-53A rev 1 requirement and provides assessment scope and frequency. Part c: This control is reviewed annually by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility:</u>** The PEO Digital security assessment team develops a security assessment report that documents risks,

	vulnerabilities, findings, identified during the assessment. And provides recommendations and remediation for 2 Twelve Solutions ORE. The SAR is consistent with DoD reporting guidelines and templates. Part d: This control is reviewed annually by the ISSO and SO. & **2 Twelve Solutions Responsibility:** The PEO Digital security assessment team presents results of the SAR to 2 Twelve Solutions ORE Leadership (System Owner, CISO, and VP, Operations) upon completion. The PEO Digital security assessment team will address any comments from the Agency Authorizing Official/DoD PMO and provide updates to the SAR for final submission. 2 Twelve Solutions will review and sign each version of the SAR prior to submission on MAX.gov. This procedure is part of the initial accreditation and annual continuous monitoring and reaccreditation activities.
Part b	
Part b1	
Part b2	
Part b3	
Part c	
Part d	
Part e	
Part f	

CA-2 (1) CONTROL ENHANCEMENT (L) (M) (H)

The organization employs assessors or assessment teams with [*Assignment: organization-defined level of independence*] to conduct security control assessments.

CA-2 (1) Additional FedRAMP Requirements and Guidance:

Requirement: For JAB Authorization, must use an accredited Third Party Assessment Organization (3PAO).

CA-2 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CA-2 (1) What is the solution and how is it implemented?
This control is reviewed annually by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions Security Manager is responsible for contracting an accredited PEO DIgital Security Assessment Team to conduct security control assessment of the 2 Twelve Solutions information system and all controls, policies, and procedures within the ORE environment. The accredited third-party assessor is responsible for developing and completing the SAR as part of the initial accreditation annual continuous monitoring assessment activities, as appropriate.

CA-2 (2) CONTROL ENHANCEMENT (M) (H)

The organization includes as part of security control assessments, [*FedRAMP Assignment: at least annually*], [*Selection: announced; unannounced*], [*Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing;* [*Assignment: organization-defined other forms of security assessment*]].

CA-2 (2) Additional FedRAMP Requirements and Guidance:

Requirement: To include *'announced'*, *'vulnerability scanning' to occur at least annually*.

{{CONTROL|CA-2.2}}

CA-2 (3) CONTROL ENHANCEMENT (M) (H)

The organization accepts the results of an assessment of [*FedRAMP Assignment: organization-defined information system*] performed by [*FedRAMP Assignment: any FedRAMP Accredited 3PAO*] when the assessment meets [*FedRAMP Assignment: the conditions of the* JAB/AO *in the FedRAMP Repository*].

{{CONTROL|CA-2.3}}

CA-3 System Interconnections (L) (M) (H)

The organization:

(a) Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;

(b) Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and

(c) Reviews and updates Interconnection Security Agreements [*FedRAMP Assignment: at least annually and on input from FedRAMP*].

Table 13-3. CA-3 Authorized Connections

Authorized Connections Information System Name	Name of Organization CSP Name System Connects To	Role and Name of Person Who Signed Connection Agreement	Name and Date of Interconnection Agreement
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>

CA-3	Control Summary Information
Responsible Role: Fraser, Doug	
ca-03_odp.01:	
ca-03_odp.02:	
ca-03_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CA-3 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed annually by the ISSO and SO. & **2 Twelve Solutions Responsibility:** 2 Twelve Solutions ORE maintains six external interconnections which support the Infrastructure, security, and compliance monitoring within the ORE platform. 2 Twelve Solutions system interconnection agreements documents characteristics and security requirements to identify and protect the confidentiality, integrity, and availability of the information. The requirements and purpose of the information system being connected between third parties is documented in the SSP by the Engineering team. The ARB and AO is responsible for approving and/ or denying all interconnection agreements. All new connection will then be reviewed and approved by the Authorizing official. Part b: This control is reviewed annually by the ISSO and SO. & 2 Twelve Solutions's responsibility: 2 Twelve Solutions Engineering team& is responsible for reviewing the ISA for& each interconnections, the interface characteristics, security requirements, and the nature of the information communicated agreements which includes • Services offered • Sensitivity of Data • User Community ORE Engineering, ARB, and the AO will review each ISA before the connection is approved. This procedure is done to prevent unauthorized access to sensitive data, contracts and agreements. Agreements include security consideration for services offered, data sensitivity, user community, information exchange security, trusted behavior expectation/rules of behavior, incident reporting, audit trails responsibilities, training and awareness, security documentation, and escalation procedures. Part c: This control is reviewed annually by the ISSO and SO. & **2 Twelve Solutions Responsibility:**

	2 Twelve Solutions Engineering team is responsible for reviewing and updating of ORE Interconnections Security Agreements during the annual assessment or when there is a significant change in the system. Once the Interconnection Security Agreement (ISA) is updated, it needs to be re-resigned.
Part b	
Part c	
Part a	

CA-3	**Control Summary Information**
Responsible Role:	

CA-3	Control Summary Information
Responsible Role: Fraser, Doug	
ca-03_odp.01:	
ca-03_odp.02:	
ca-03_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CA-3	Control Summary Information

CA-3 What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed annually by the ISSO and SO. & **2 Twelve Solutions Responsibility:** 2 Twelve Solutions ORE maintains six external interconnections which support the Infrastructure, security, and compliance monitoring within the ORE platform. 2 Twelve Solutions system interconnection agreements documents characteristics and security requirements to identify and protect the confidentiality, integrity, and availability of the information. The requirements and purpose of the information system being connected between third parties is documented in the SSP by the Engineering team. The ARB and AO is responsible for approving and/ or denying all interconnection agreements. All new connection will then be reviewed and approved by the Authorizing official. Part b: This control is reviewed annually by the ISSO and SO. & 2 Twelve Solutions's responsibility: 2 Twelve Solutions Engineering team& is responsible for reviewing the ISA for& each interconnections, the interface characteristics, security requirements, and the nature of the information communicated agreements which includes • Services offered • Sensitivity of Data • User Community ORE Engineering, ARB, and the AO will review each ISA before the connection is approved. This procedure is done to prevent unauthorized access to sensitive data, contracts and agreements. Agreements include security consideration for services offered, data sensitivity, user community, information exchange security, trusted behavior expectation/rules of behavior, incident reporting, audit trails responsibilities, training and awareness, security documentation, and escalation procedures. Part c:

CA-3	Control Summary Information
	This control is reviewed annually by the ISSO and SO. & **2 Twelve Solutions Responsibility:** 2 Twelve Solutions Engineering team is responsible for reviewing and updating of ORE Interconnections Security Agreements during the annual assessment or when there is a significant change in the system. Once the Interconnection Security Agreement (ISA) is updated, it needs to be re-resigned.
Part b	
Part c	
Part a	
Parameter CA-3(c): {{PARAMETER|CA-3(c)|VALUE}}	
Implementation Status (check all that apply): {{CHECKBOXES|CA-3|STATUS}}	

Control Origination (check all that apply):
{{CHECKBOXES|CA-3|RESPONSIBILITY-1}}
{{CHECKBOXES|CA-3|RESPONSIBILITY-2}}	

CA-3 What is the solution and how is it implemented?	
Part a	See § 11 for information about implementation.
Part b	See Table 13-2. Control Origination and Definitions and Table 11-1. System Interconnections for information about implementation.

<table>
<tr><th colspan="2">CA-3 What is the solution and how is it implemented?</th></tr>
<tr><td><b>Part c</b></td><td>
<table>
<tr><th>CA-3</th><th>Control Summary Information</th></tr>
<tr><td colspan="2">Responsible Role: Fraser, Doug</td></tr>
<tr><td colspan="2">ca-03_odp.01:</td></tr>
<tr><td colspan="2">ca-03_odp.02:</td></tr>
<tr><td colspan="2">ca-03_odp.03:</td></tr>
<tr><td colspan="2">Implementation Status (check all that apply):
☒Implemented
☐Partially implemented
☐Planned
☐Alternative implementation
☐Not applicable</td></tr>
<tr><td colspan="2">Control Origination (check all that apply):
☒Service Provider Corporate
☒Service Provider System Specific
☒Service Provider Hybrid (Corporate and System Specific)
☒Configured by Customer (Customer System Specific)
☒Provided by Customer (Customer System Specific)
☒Shared (Service Provider and Customer Responsibility)
☒Inherited from pre-existing FedRAMP Authorization</td></tr>
</table>
</td></tr>
</table>

CA-3 What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed annually by the ISSO and SO. & **2 Twelve Solutions Responsibility:** 2 Twelve Solutions ORE maintains six external interconnections which support the Infrastructure, security, and compliance monitoring within the ORE platform. 2 Twelve Solutions system interconnection agreements documents characteristics and security requirements to identify and protect the confidentiality, integrity, and availability of the information. The requirements and purpose of the information system being connected between third parties is documented in the SSP by the Engineering team. The ARB and AO is responsible for approving and/ or denying all interconnection agreements. All new connection will then be reviewed and approved by the Authorizing official. Part b: This control is reviewed annually by the ISSO and SO. & 2 Twelve Solutions's responsibility: 2 Twelve Solutions Engineering team& is responsible for reviewing the ISA for& each interconnections, the interface characteristics, security requirements, and the nature of the information communicated agreements which includes • Services offered • Sensitivity of Data • User Community ORE Engineering, ARB, and the AO will review each ISA before the connection is approved. This procedure is done to prevent unauthorized access to sensitive data, contracts and agreements. Agreements include security consideration for services offered, data sensitivity, user community, information exchange security, trusted behavior expectation/rules of behavior, incident reporting, audit trails responsibilities, training and awareness, security documentation, and escalation procedures. Part c:

CA-3 What is the solution and how is it implemented?		
		This control is reviewed annually by the ISSO and SO. & **2 Twelve Solutions Responsibility:** 2 Twelve Solutions Engineering team is responsible for reviewing and updating of ORE Interconnections Security Agreements during the annual assessment or when there is a significant change in the system. Once the Interconnection Security Agreement (ISA) is updated, it needs to be re-resigned.
	Part b	
	Part c	
	Part a	

CA-3 (3) CONTROL ENHANCEMENT (M) (H)

The organization prohibits the direct connection of an [*Assignment: organization-defined unclassified, non-national security system*] to an external network without the use of [*FedRAMP Assignment: boundary protections which meet Trusted Internet Connection (TIC) requirements*].

CA-3 (3) Additional FedRAMP Requirements and Guidance:

Guidance: Refer to Appendix H – Cloud Considerations of the TIC Reference Architecture document. Link: https://www.dhs.gov/publication/tic-reference-architecture-22

{{CONTROL|CA-3.3}}

CA-3 (5) CONTROL ENHANCEMENT (M)

The organization employs [*Selection: allow-all, deny-by-exception, deny-all, permit by exception*] policy for allowing [*Assignment: organization-defined information systems*] to connect to external information systems.

CA-3 (5) Additional FedRAMP Requirements and Guidance:

Guidance: For JAB Authorization, CSPs shall include details of this control in their architecture briefing.

{{CONTROL|CA-3.5}}

CA-5 Plan of Action and Milestones (L) (M) (H)

The organization:

(a) Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

(b) Updates existing plan of action and milestones [*FedRAMP Assignment: at least monthly*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-5 Additional FedRAMP Requirements and Guidance:

Requirement: Plan of Action & Milestones (POA&M) must be provided at least monthly.

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Plan of Action and Milestones (POA&M) Template Completion Guide
https://www.FedRAMP.gov/documents/

CA-5	Control Summary Information
Responsible Role: Fraser, Doug	
ca-05_odp:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CA-5 What is the solution and how is it implemented?	
Part a	Part a: The control is reviewed annually by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions has developed a Plan of Action and Milestones (POA&M) based on the format of the *FedRAMP Plan of Action and Milestones (POA&M) Template* and the instructions provided in the *FedRAMP Plan of Action and Milestones (POA&M) Template Completion Guide*. It is the responsibility of Engineering team to document ORE Plan Of Action and Milestone (POA&M). 2 Twelve Solutions ORE document finding description of vulnerabilities, remediation plan, and date planned to remediate vulnerabilities, weaknesses, and deficiencies found during the assessments of security controls within the ORE environment. The POA&M is updated to include any findings from the SAR following the PEO Digital security assessment team FedRAMP assessment. Part b: This control is reviewed annually by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions Engineering and Operations team is responsible for the update of the Plan of Action and Milestones (POA&M). The POA&M is reviewed and updated at least monthly based on the findings from: • Security Control Assessment • Security Impact Analysis • Remediation Activities • Results of Vulnerability Scans • Continuous Monitoring Activities (when vulnerability scan are run and any new vulnerabilities are identified) POA&M updates will be provided monthly to AO for review.
Part b	

CA-6 Security Authorization (L) (M) (H)

The organization:

(a) Assigns a senior-level executive or manager as the authorizing official for the information system;

(b) Ensures that the authorizing official authorizes the information system for processing before commencing operations; and

(c) Updates the security authorization [*FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs*].

CA-6c Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F (SP 800-37). The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the JAB/AO.

CA-6	Control Summary Information
Responsible Role: Fraser, Doug	
ca-06_odp:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CA-6 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed annually by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility:</u>** As part of the security authorization process, a senior-level executive of the authorizing agency reviews the 2 Twelve Solutions ORE security authorization package to determine if vulnerabilities identified in the information system pose an acceptable level of risk to customer agency operations, assets, and individuals before granting an ATO. The explicit acceptance of risk is the responsibility of the authorizing agency and other customer organizations. The authorizing agency must consider many factors, balancing security considerations with mission and operational needs. The authorizing agency issues an authorization decision for the information system after reviewing the authorization package submitted by the 2 Twelve Solutions ORE system owner. The authorization package provides the authorizing agency and other customers with the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system. Part b: This control is reviewed annually by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility:</u>** The authorizing official authorizes the information system for processing before commencing operations. Additionally, the authorizing official determines if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals. Agencies must also determine whether the risk to the agency is acceptable. Following review of the security authorization package and consultation with key agency officials, the authorizing agency renders an authorization decision to: • Authorize system operation without any restrictions or limitations on its operation; • Authorize system operation with restriction or limitation on its operation. The POA&M must be included and contain detailed corrective actions to correct deficiencies. An updated authorization package will be resubmitted upon completion of required POA&M actions to move to authorization to operate w/out any restrictions; or • Not authorize for operation. Part c:

	This control is reviewed annually by the ISSO and SO. & **2 Twelve Solutions Responsibility:** 2 Twelve Solutions Engineering team works with the Authorizing Official and the PEO DIgital Security Assessment Team to update the security authorization. Security authorization is reviewed and updated at least three years or when there is a significant change in the system as defined in NIST SP 800-37.
Part b	
Part c	
Part c1	
Part c2	
Part d	
Part e	

CA-7 Continuous Monitoring (L) (M) (H)

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

(a) Establishment of [*Assignment: organization-defined metrics*] to be monitored;

(b) Establishment of [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessments supporting such monitoring;

(c) Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

(d) Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;

(e) Correlation and analysis of security-related information generated by assessments and monitoring;

(f) Response actions to address results of the analysis of security-related information; and

(g) Reporting the security status of organization and the information system to [*FedRAMP*

Assignment: to meet Federal and FedRAMP requirements] [*Assignment: organization-defined frequency*].

CA-7 Additional FedRAMP Requirements and Guidance:

Requirement: Operating System Scans: at least monthly. Database and Web Application Scans: at least monthly. All scans performed by Independent Assessor: at least annually.

Guidance: CSPs must provide evidence of closure and remediation of a high vulnerability within the timeframe for standard POA&M updates.

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Continuous Monitoring Strategy Guide

https://www.fedramp.gov/documents/

CA-7	Control Summary Information
Responsible Role: Fraser, Doug	
ca-07_odp.01:	
ca-07_odp.02:	
ca-07_odp.03:	
ca-07_odp.04:	
ca-07_odp.05:	
ca-07_odp.06:	
ca-07_odp.07:	
Parameter CA-7(g)-1):	
Parameter CA-7(g)-2):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CA-7 What is the solution and how is it implemented?

Part a	This control is reviewed annually by the ISSO and SO. Part a:& **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions ORE implements continuous monitoring in accordance with NIST 800-37 Rev. 1, A Guide for Applying the Risk Management Framework to Federal Information Systems.& As part of the continuous monitoring process, 2 Twelve Solutions ORE will monitor the following metrics: • OS Event Monitoring (as defined in AU-2) • Integrity Monitoring (as defined in SI-7(1)) • Incident Reporting (as defined in IR-6) • Vulnerability Scanning of components within boundary, OS, WebApp, Databases (as defined in RA-5) • Baseline Configuration scanning for components within boundary (OS, WebApps, Databases) (as defined in SI-7(1)) • Analysis, correlation and aggregation of logs from monitoring tools (as defined in SI-4(2)) – Tracking of Issues resolved and reported (as defined in IR-6) • POA&M Updates (as defined in CA-5) • Contingency Plan & Testing (as defined in CP-3) • Incident Response Plan & Testing (as defined in IR-3) • System Security Plan Updates (as defined in CA-2) • Security Awareness Training Records (as defined in AT-4) Part b: **<u>2 Twelve Solutions Responsibility:</u>** As a part of the 2 Twelve Solutions' continuous monitoring strategy, the team conducts ongoing security status monitoring of all systems, system components, processes, and network devices within the ORE boundary in accordance with provided guidance. Part c: **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions has implemented a security assessment program to evaluate the ongoing effectiveness of security controls outlined in this SSP. The security assessment program includes the assessment of management, operational, and technical controls identified in the moderate controls baseline of NIST SP 800-53, Rev.5, *Recommended Security Controls for Information Systems and Organizations*. Additionally,

technical testing including penetration testing and vulnerability scans is performed to meet the continuous monitoring requirements identified by NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to a Federal Information System*.

Part d:

2 Twelve Solutions Responsibility:

As a part of the 2 Twelve Solutions' continuous monitoring strategy, the team conducts ongoing security status monitoring of all systems, system components, processes, and network devices within the ORE boundary in accordance with provided guidance.

Part e:

2 Twelve Solutions Responsibility:

The team reviews, analyzes, and correlates vulnerabilities and risks identified during vulnerability scanning, security assessments, and metrics defined in part 'a' above and tracks issues in the POA&M.

Part f:

2 Twelve Solutions Responsibility:

Deficiencies within the system are documented in the POA&M that is included in the Security Authorization package. As part of continuous monitoring, 2 Twelve Solutions ORE POA&M is updated to reflect any newly identified or remediated security issues. For more information regarding updates to POA&M see CA-5.&

Part g:

2 Twelve Solutions Responsibility:

2 Twelve Solutions will provide a report of the 2 Twelve Solutions ORE boundary on a defined basis.& Deliverables may include:

- Vulnerability Scans
  - Raw Scan Files (native scanner files – usually XML or CSV)
  - Exported summary reports (PDF, MS Word, or other readable documents)
  - Scan Summary
- Plan of Action and Milestones (POA&M)

	• Current and accurate system inventory • Deviation Requests (Risk Adjustments, False Positives, Operationally Required) • Closure Evidence
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part g	
Part a	
Part b	
Part c	
Part a	
Part f	
Part d	
Part c	
Part b	
Part a	
Part a	
Part d	
Part b	
Part e	
Part c	
Part b	
Part a	
Part b	
Part b	

Part b	

CA-7 Additional FedRAMP Requirements and Guidance:

Requirement 1: Operating System Scans: at least monthly

Requirement 2: Database and Web Application Scans: at least monthly

Requirement 3: All scans performed by Independent Assessor: at least annually

CA-7 Req.	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

CA-7 What is the solution and how is it implemented?	
Req. 1	
Req. 2	
Req. 3	

CA-7 (1) CONTROL ENHANCEMENT (M) (H)

The organization employs assessors or assessment teams with [*Assignment: organization-defined level of independence*] to monitor the security controls in the information system on an ongoing basis.

CA-7 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CA-7 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE will utilize an independent assessment team that the platform provider uses. The same team that performs assessment and authorization will monitor the security controls for a system on an ongoing basis through the POA&M and Continuous Monitoring programs. The ORE ISSO is responsible for working closely with the independent assessment team as needed to include updates and artifacts as required. The ORE ISSO reviews this control implementation on a continuous basis as part of a Continuous Monitoring program.

CA-8 Penetration Testing (M) (H)

The organization conducts penetration testing [*FedRAMP Assignment: at least annually*] on [*Assignment: organization-defined information systems or system components*].

CA-8 Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Penetration Test Guidance

https://www.fedramp.gov/documents/

{{CONTROL|CA-8}}

CA-8 (1) CONTROL ENHANCEMENT (M) (H)

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

{{CONTROL|CA-8.1}}

CA-9 Internal System Connections (L) (M) (H)

The organization:

(a) Authorizes internal connections of [*Assignment: organization-defined information system components or classes of components*] to the information system; and

(b) Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

CA-9	Control Summary Information
Responsible Role: Fraser, Doug	
ca-09_odp.01:	
ca-09_odp.02:	
ca-09_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CA-9 What is the solution and how is it implemented?

Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Part a: **<u>2 Twelve Solutions Responsibility</u>**: Establish an authorization process to approve and authorize internal connections of organization-defined system components or classes of components to the system. This process will involve assessing the security and privacy requirements of the internal connections and ensuring they align with the organization's policies and risk tolerance. Part b: **<u>2 Twelve Solutions Responsibility</u>**: For each authorized internal connection, the organization will document the interface characteristics, security and privacy requirements, and the nature of the information communicated. This documentation will provide a comprehensive understanding of the internal connections and serve as a reference for future assessments, audits, or system modifications. Part c: **<u>2 Twelve Solutions Responsibility</u>**: Define conditions under which internal system connections will be terminated. These conditions may include changes in system configurations, security posture, or organizational requirements. When these conditions are met, the organization will promptly terminate the internal system connections to prevent unauthorized access or information disclosure. Part d: **<u>2 Twelve Solutions Responsibility</u>**: Conduct periodic reviews of the authorized internal connections to ensure their continued compliance with security and privacy requirements. These reviews may include assessments of interface characteristics, information flow, and adherence to relevant policies and regulations. Any identified issues or deviations will be addressed promptly through appropriate corrective actions. The organization will implement auditing and monitoring mechanisms to track and log internal system

	connections. This will enable the detection of unauthorized or anomalous connections, as well as provide valuable insights into the nature and frequency of internal connections. The audit logs will be regularly reviewed to identify any suspicious activities and facilitate incident response, if required.
Part b	
Part c	
Part d	

13.5. Configuration Management (CM)

CM-1 Configuration Management Policies and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles]:*

(1) A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and

(b) Reviews and updates the current:

(1) Configuration management policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Configuration management procedures [*FedRAMP Assignment: at least annually*].

CM-1	Control Summary Information
Responsible Role: Fraser, Doug	
cm-01_odp.01:	
cm-01_odp.02:	
cm-01_odp.03:	
cm-01_odp.04:	
cm-01_odp.05:	
cm-01_odp.06:	
cm-01_odp.07:	
cm-01_odp.08:	
Parameter CM-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

CM-1 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:** 2 Twelve Solutions ORE Information Security Policy directs the activities within the ORE Configuration and Change Management Plan. The plan addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements to meet the FedRAMP control implementation requirements for the configuration management control family of a moderate baseline.& The plan specifically addresses procedures or processes related to: • Baseline configuration • Configuration Change Management • Security Impact Analysis • Access Restrictions for Change • Configuration Settings • Least Functionality • System Inventory • Configuration Management Plan • Software Usage Restrictions • User-Installed Software & All ORE procedures that are captured in Thanos document management system, 2 Twelve Solutions's document repository management system, are reviewed on an annual basis by the document owner and the ORE Architecture Review Board (ARB). The ARB consists of Operations and Engineering. The ARB is responsible for notifying stakeholders when changes are made and approved by the ARB. This may require the creation of new documentation or reviewing and updating current procedures, annually or as needed; and policies every 3 years or as needed. & The Operations and Engineering team are responsible for reading the document on an annual basis. The team composition includes the following: • Engineering (Development Manager and Developers and Analysts); • Operations (Operations, Databases, and Network); and • ORE Leadership (SVP, System Owner; VP, CISO; and VP, Operations); & The 2 Twelve Solutions ORE ARB and the ISSO is responsible for reviewing and approving the policies and procedures for the ORE environment.& Once approved, the ISSO will sign the policy and procedure.

	Part b: Part c: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility:** ORE policies are reviewed and updated every three years by the ORE ARB. The Engineering team is responsible for reviewing and making updates to the ORE Configuration Management procedure annually.& The 2 Twelve Solutions ORE ARB and the ISSO is responsible for reviewing and approving the policies and procedures for the ORE environment.& Once approved, the ISSO will sign the policy and procedure
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

CM-2 Baseline Configuration (L) (M) (H)

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

CM-2	Control Summary Information
Responsible Role: Fraser, Doug	
cm-02_odp.01:	
cm-02_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-2 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions utilizes Gitlab and automation to establish and maintain the configuration baseline for the ORE information system. Gitlab is a repository for code management. Gitlab is a centralized repository to plan projects, collaborate on code, perform testing and deploy code. Gitlab is used for code development and code reviews. Gitlab includes all commits or changes to the application and provides version-control capabilities. Gitlab supplies the graphical user interface (GUI) that provides code review capabilities, controlled access, and deployment pipelines. & Automation to include terraform, docker compose, ansible and python scripts are used as software provisioning, configuration management and application deployment tools. Ansible deploys modules to nodes over SSH which are temporarily stored in the nodes and communicated through a JSON protocol. These baseline configurations changes and updates are tracked within the Gitlab and managed by the Operations team. The Operations team creates and updates the Agile system tickets for changes to network devices and machines.& Agile system tickets are also created and updated when there is a new 2 Twelve Solutions release or an update to the CIS benchmark or vendor configuration baselines. & The 2 Twelve Solutions ORE ARB& is responsible for reviewing and approving the configuration baseline updates and changes. The ARB& is responsible for signing off on the final version of any configuration baseline prior to the change being released.
Part b	
Part b1	
Part b2	
Part b3	

CM-2 (1) CONTROL ENHANCEMENT (M)

The organization reviews and updates the baseline configuration of the information system:

(a) [*FedRAMP Assignment: at least annually*];

(b) When required due to [*FedRAMP Assignment: to include when directed by the JAB*]; and

(c) As an integral part of information system component installations and upgrades.

{{CONTROL|CM-2.1}}

CM-2 (2) CONTROL ENHANCEMENT (M) (H)

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

CM-2 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
cm-02.02_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-2 (2) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: All system configurations within ORE are managed and created by Operations team through the use of automation throughout the authorization boundary. Patch management, new releases of ORE, and new configurations of the platform is handled through this process. & ORE uses InSpec, SIEM, and automation to detect any inventory changes and configuration changes. InSpec scans are run at least monthly as part of the continuous monitoring of the information system. In addition, InSpec scans are run prior to any update or release. InSpec scans are used to update and maintain the inventory of the information system. System components are checked for compliance to automation through the use of InSpec Policy Compliance scans. automation are used as baselines for the machines deployed in the environment to detect any configuration changes. & Gitlab tool is being leveraged to track all changes to automation and the Agile system ticketing system is employed to ensure they have gone through the necessary process of peer review, security impact analysis, and approval before they have been implemented in ORE. & The 2 Twelve Solutions ORE ARB& is responsible for reviewing and approving the configuration baseline updates and changes. The ARB& is responsible for signing off on the final version of any configuration baseline prior to the change being released.

CM-2 (3) CONTROL ENHANCEMENT (M)

The organization retains [*Assignment: organization-defined previous versions of baseline configurations of the information system*] to support rollback.

CM-2 (3)	Control Summary Information
Responsible Role: Fraser, Doug	
cm-02.03_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-2 (3) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE maintains every baseline configuration of ORE that has been deployed to support rollback to any point in in Gitlab. Gitlabs track all changes and maintain the configuration baseline within automation indefinitely. As changes are made to the ORE baseline configuration, the new baseline becomes the current version, and the previous baseline is no longer valid. Previous configuration baselines, in the form of scripts (playbooks) used by automation to establish and set configuration settings, are stored using Gitlab. & The 2 Twelve Solutions ORE ARB& is responsible for reviewing and approving the configuration baseline updates and changes. The ARB& is responsible for signing off on the final version of any configuration baseline prior to the change being released.

CM-2 (7) CONTROL ENHANCEMENT (M) (H)

The organization:

(a) Issues [*Assignment: organization-defined information systems, system components, or devices*] with [*Assignment: organization-defined configurations*] to individuals traveling to locations that the organization deems to be of significant risk; and

(b) Applies [*Assignment: organization-defined security safeguards*] to the devices when the individuals return.

CM-2 (7)	Control Summary Information
Responsible Role: Fraser, Doug	
cm-02.07_odp.01:	
cm-02.07_odp.02:	
cm-02.07_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-2 (7) What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: There are no physical components within the ORE authorized boundary. ORE is built on Provider and does not have access to physical assets. ORE admins utilize workstations to access the ORE environment; however, user devices are not managed by ORE. & Inherited from the [Insert policy document of related control for the provider] Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: There are no physical components within the ORE authorized boundary. ORE is built on Provider and does not have access to physical assets. ORE admins utilize workstations to access the ORE environment; however, user devices are not managed by ORE. & Inherited from the [Insert policy document of related control for the provider]
Part b	

CM-3 Configuration Change Control (M) (H)

The organization:

(a) Determines the types of changes to the information system that are configuration-controlled;

(b) Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

(c) Documents configuration change decisions associated with the information system;

(d) Implements approved configuration-controlled changes to the information system;

(e) Retains records of configuration-controlled changes to the information system for [*Assignment: organization-defined time period*];

CM-3 (e) Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with record retention policies and procedures.

(f) Audits and reviews activities associated with configuration-controlled changes to the information system; and

(g) Coordinates and provides oversight for configuration change control activities through [*FedRAMP Assignment: see additional FedRAMP requirements and guidance*] that convenes [*Selection (one or more): [Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].

CM-3 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the JAB/AO.

CM-3	Control Summary Information
Responsible Role: Fraser, Doug	
cm-03_odp.01:	
cm-03_odp.02:	
cm-03_odp.03:	
cm-03_odp.04:	
cm-03_odp.05:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-3 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: The Operations team is responsible for defining Configuration Item's (CI's) within ORE. Operations team defines CI's as any component that needs to be managed in order to maintain and execute correct operations of ORE. Information about each CI is recorded in the System Inventory Workbook and automation playbook. The ORE inventory is reviewed and updated at least monthly as part of the continuous monitoring process.& The inventory documents the CI attributes such as the unique asset name, IP address, the DNS, configuration baseline version, OS name and version, and all requirements derived from the System Inventory Workbook. & All changes to the 2 Twelve Solutions ORE are tracked in a Agile system ticket. Major changes are required to be tested, scheduled and analyzed for potential security impact. Every Configuration Item (CI) that is tracked in a Agile system ticket will contain the following information: • Unique Asset Identifier • IP Address(es) (if applicable) • Whether the CI is virtual • Whether the CI is publicly accessible • DNS name or URL (if applicable) • NetBIOS name (if applicable) • MAC Address(es) (if applicable) • Authenticated scan status • Baseline configuration name • OS Name and Version • Location information (building, room, and rack, if applicable) • Asset type • Hardware make/model • Status in latest scan • Software/Database vendor • Software/Database name/version • Patch level • Function • Serial #/Asset Tag# • VLAN/Network ID • Record of all changes to this inventory item. & **<u>Customer Responsibility:</u>&**

It is the customer responsibility to determine the types of changes to the information system that are configuration controlled.

Part b:

This control is reviewed at least annually or as needed by the ISSO and SO.

&

2 Twelve Solutions Responsibility:

The Engineering team is responsible for conducting the initial review of proposed configuration-controlled changes to ORE. The ARB will either approve or disapprove the changes through the Agile system ticketing procedure with explicit consideration for the security impact analysis during the change management process. The Engineering team and ARB reviews and approves configuration changes when a new release is being prepared, when a new base image is created, and whenever there is a proposed change to an automation playbook that could affect the security stature of ORE.

&

The Engineering Team and the ARB meets weekly to discuss and review proposed configuration changes to ORE.& ARB must both approve a change before it can be implemented. The details of the change must be fully document in the CI as described in Part a. The Agile system ticket also includes the details of the security impact analysis (SIA) that has been performed.&

&

Customer Responsibility:&

It is the customer responsibility to review proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analysis.

Part c:

This control is reviewed at least annually or as needed by the ISSO and SO.

&

2 Twelve Solutions Responsibility:

Configuration change management decisions are documented as part of the life-cycle of a Change Request and are maintained in the ORE Agile system ticketing system.& The Change Lifecycle has 6 stages:

- Submission
- Planning
- Approval
- Implementation
- Review
- Closure

&
Change Requests can be submitted by all ORE staff to the ARB where they then accept or reject the change request. The 2 Twelve Solutions ARB meets to review any proposed changes and provide oversight to the configuration management process. The ARB will review and either approve or reject a change to the ORE information system. Any notes or comments related to the approval or rejection are stored in Agile system as part of the change request. Changes are only implemented into production after all changes have been tested, scheduled, analyzed for potential security impact, and approved.
&
Upon completion of all the above steps, the change must be approved by the Architecture Control Board (ARB) prior to the implementation of any change for the Application, Database or Operating System.
&
Customer Responsibility:&
It is the customer responsibility to document configuration change decisions associated with the information system.

Part d:

This control is reviewed at least annually or as needed by the ISSO and SO.

&
2 Twelve Solutions& Responsibility:
Changes are only implemented into production after all changes have been tested, scheduled, analyzed for potential security impact, and approved. Once the change is approved, the implementation is scheduled. The implementation tasks are performed. The Operations team will implement configuration-controlled changes to ORE once they are approved by the ARB.
&
All automation playbook baselines will be updated with the latest updates approved for the release to production. Production Images will remain available to production for an extended time due to the use of Auto-scaling and custom Cloud Formation scripts.& ORE Operations Team coordinates with all the teams to ensure all agents and tools are installed on servers and hosts.
&
Customer Responsibility:&

It is the customer responsibility to implement approved configuration controlled changes to the information system. Upon completion of all the above steps, the change must be approved by the Architecture Control Board (ARB) prior to the implementation of any change for the Application, Database or Operating System.

Part e:

	This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The 2 Twelve Solutions ORE Change Management process is integrated into ORE's Agile system ticketing system. All aspects of Change Management and change requests, including records of changes, are stored in the Agile system ticketing database indefinitely, and are available at all times for historic or reporting purposes.& There is no differentiation in the retention periods for application, database or operating system. & **Customer Responsibility:&** It is the customer responsibility to retain records of configuration controlled changes to the information within the DHS defined time period for the ORE application. Part f: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The ARB audits and reviews all activities associated with configuration-controlled changes to ORE on a monthly basis through the use of Inspec& and Trivy scanner. The Agile system tickets and CIs any change or update at the application, database or operating system level are all retained indefinitely within the Agile system database.& There is no differentiation in the retention periods for application, database or operating system. & **Customer Responsibility:&** It is the customer responsibility to audits and reviews activities associated with configuration controlled changes to the information system. Part g: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The Engineering team& and the ARB coordinate and provide oversight for configuration change control activities through the change management process. The change management process is required when a new release is being prepared or whenever there is a proposed change that could affect the availability of

	ORE. These changes include but not limited to ORE version upgrades, emergency changes/fixes, adding additional services or offerings. These changes are communicated to the customer through email or phone to ensure the impact to customer is minimized. & **Customer Responsibility:&** It is the customer responsibility to coordinate and provide oversight for configuration change control activities.&
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	

CM-4 Security Impact Analysis (L) (M) (H)

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

CM-4	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-4 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: A security impact analysis (SIA) is performed for all change requests. The Engineering team performs the SIA for all changes and based on the outcome will provide an approval of the proposed change. The Engineering team will record in the Agile system ticket for each CI the results of the SIA. When the ARB meets, they will review the CI ticket in Agile system and examine the results of the SIA prior to the approval or rejection of the proposed change. & For all changes, a Security Impact Analysis checklist is used to evaluate the change impact to various aspect of the ORE. Based on the result, it may trigger the use of security impact analysis worksheet in the ORE change management plan. & If the change involves a change in any COTS or custom code, identifying vulnerabilities may include, for example, a search of the National Vulnerability Database (NVD) 24 which enumerates vulnerabilities, user experience, etc. 2 Twelve Solutions will leverage this information to address known issues and remove or mitigate them before they become a concern.& If the change involves the custom code for ORE, a more in-depth analysis of the security impact is conducted.& Once vulnerability has been identified, a risk assessment is needed to identify the likelihood of a threat exercising the vulnerability and the impact of such an event. & **<u>Customer Responsibility:</u>&** It is the customer responsibility to analyzes changes to the information system to determine potential security impacts prior to change implementation.

CM-5 Access Restrictions for Change (M) (H)

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

CM-5	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-5 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Physical access into the ORE environment is not possible as the infrastructure is hosted within Azure.& All changes to ORE are performed through automation which are run from the SSH Bastion host. Inspec runs policy compliance checks against the systems& and will flag any discrepancies. Gitlab is leveraged to maintain and track any changes that are done to the automation. Access to the source code repository is restricted to the Operations team members. & Day-to-day management of the entire 2 Twelve Solutions ORE infrastructure is accomplished through the use of configuration management tools. Only the 2 Twelve Solutions ORE Operations or Engineering personnel assigned to the task(s) approved in a change request are permitted to implement system changes. For changes requiring ARB approval, change implementation is allowed only after the change has been approved. The full life cycle of changes are documented in Agile system change tickets. To release changes into the production environment, the 2 Twelve Solutions Engineering personnel assigned to the task(s) approved in the change request must have privileged access on the applicable production servers, network devices, or databases that the change affects. & Application: Application accesses are specific to each customer. Firewall rules are leveraged to enforce access flow and provide logical separation such that customers only have access to their own environment. Application front end users must authenticate through MFA or SAML 2.0 token. Reverse Proxy enforces TLS1.2 encryption to protect the communication session. 2 Twelve Solutions administrators do not have access to client applications. Access to InSpec, SIEM, Trivy is limited to authorized personnel based on role based access on the principle of least privilege. & Database: Each customer environment has a dedicated MySQL database accessible only through the application. 2 Twelve Solutions administrators do not have access to client data. Patches and updates are accomplished through Anisble playbooks. & Operating System: Authorized 2 Twelve Solutions administrators access operating systems by authenticating through the bastion host. All users must have a valid SSH key and a one-time password from Yubikey or HSPD-12 compliant hardware token. After authenticate through the bastion host, users must have a matching public SSH key on the instance to establish connection with that host. Connections are enforced through whitelisting by Firewall rules. Creation, modification, and deletion of security groups must go through the defined CM process and requested through Agile system for ARB approval. & **Customer Responsibility:&** It is the customer responsibility to define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

CM-5 (1) CONTROL ENHANCEMENT (M) (H)

The information system enforces access restrictions and supports auditing of the enforcement actions.

{{CONTROL|CM-5.1}}

CM-5 (3) CONTROL ENHANCEMENT (M) (H)

The information system prevents the installation of [*Assignment: organization-defined software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

CM-5 (3) Additional FedRAMP Requirements and Guidance:

Guidance: If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be used.

{{CONTROL|CM-5.3}}

CM-5 (5) CONTROL ENHANCEMENT (M) (H)

The organization:

(a) Limits privileges to change information system components and system-related information within a production or operational environment; and

(b) Reviews and reevaluates privileges [*FedRAMP Assignment: at least quarterly*].

{{CONTROL|CM-5.5}}

CM-6 Configuration Settings (L) (M) (H)

The organization:

(a) Establishes and documents configuration settings for information technology products employed within the information system using [*FedRAMP Assignment: see CM-6(a) Additional FedRAMP Requirements and Guidance*] that reflect the most restrictive mode consistent with operational requirements;

CM-6(a) Additional FedRAMP Requirements and Guidance:

Requirement 1: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available. If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

Requirement 2: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) (http://scap.nist.gov/) validated or SCAP compatible (if validated checklists are not available).

Guidance: Information on the USGCB checklists can be found at: https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline.

(b) Implements the configuration settings;

(c) Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and

(d) Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

CM-6	Control Summary Information
Responsible Role: Fraser, Doug	
cm-06_odp.01:	
cm-06_odp.02:	
cm-06_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-6 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE configuration settings for all system components within the ORE boundary are all configured through automation which are verified by InSpec compliance checks.& All automation are based on Center for Internet Security guidelines (Level 1) and best practices to ensure that the ORE environment has the most restrictive mode consistent with operational requirements.& & Application: ORE applications follow the 2 Twelve Solutions ORE Lifecycle Management Plan and procedures defined in this SSP to ensure security considerations are in place in all steps of the ORE system lifecycle. There is no established baseline for the ORE application. InSpec vulnerability scanner is used at least monthly to ensure the security posture of the ORE application is below established risk level. & Database and Operating System:& 2 Twelve Solutions ORE establishes and documents configuration settings for information technology products employed within the ORE authorization boundary that reflect the most restrictive mode consistent with operational requirements and the CIS Level 1 guidelines. InSpec and Trivy scanner is used to verify and compare configuration settings with CIS Level 1. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Application: ORE applications follow the 2 Twelve Solutions ORE Lifecycle Management Plan and procedures defined in this SSP to ensure security considerations are in place in all steps of the ORE system lifecycle. There is no established baseline for the ORE application. InSpec vulnerability scanner is used at least monthly to ensure the security posture of the ORE application is below established risk level. & Database and Operating System:& 2 Twelve Solutions ORE establishes and documents configuration settings for information technology products employed within the ORE authorization boundary that reflect the most restrictive mode consistent with operational requirements and the CIS Level 1 guidelines. All changes that are done to the automation are tracked through the Gitlab to determine if unauthorized changes have been implemented and by whom. ORE privileged users are assigned roles and privileges only sufficient to complete their assigned responsibilities. Operations team is assigned access to the bastion host with privileges to launch automation scripts for the configuration and maintenance of the ORE environment.

Part c:

This control is reviewed at least annually or as needed by the ISSO and SO.

&
2 Twelve Solutions Responsibility:
Operations team identifies and documents any deviations from the established automation playbook configuration settings for all ORE components based on the requirements of ORE. All deviations from automation need to be approved by the Engineering team that would require all deviation requests to go through the same change management process.& 2 Twelve Solutions& identifies configuration baseline deviations using InSpec as the compliance scanning tool. If a deviation from baseline compliance is detected for an existing or newly commissioned system, a ticket is opened within 2 Twelve Solutions's& ticketing system to track the deviation. All changes are subject to the change control process as defined in the Configuration Management Plan.
&
Application:& & ORE applications follow the 2 Twelve Solutions ORE Lifecycle Management Plan and procedures defined in this SSP to ensure security considerations are in place in all steps of the ORE system lifecycle. There is no established baseline for the ORE application. InSpec vulnerability scanner is used at least monthly to ensure the security posture of the ORE application is below established risk level.
&
Database or Operating System:
2 Twelve Solutions ORE Engineering documents the deviations from the established CIS Level 1 configuration guidelines. The deviations are documented in Agile system.& Compliance with the CIS Level 1 baselines is confirmed with the InSpec CIS Level 1 baseline scan.& If the results of the scan show there is not 100% compliance with the CIS Level 1 baselines, a Agile system ticket is opened. If it is established the deviation is needed for operational purposes, then the ticket is updated.

Part d:

This control is reviewed at least annually or as needed by the ISSO and SO.

&
2 Twelve Solutions Responsibility:

Operations& team is the only users that have the ability to change configuration settings in ORE through automation. All changes are executed through the SSH Bastion after the change has been officially approved by the Engineering team& and the ARB through the change management process. A deviation from the baseline configuration is identified by the InSpec compliance scan. All changes that are done to the automation are tracked through the Gitlab& tool to determine if unauthorized changes have been

	implemented and by whom. All privileged functions for change management are captured in the audit logs for the application, database and operating system.&
Part b	
Part c	
Part d	

CM-6 (1) CONTROL ENHANCEMENT (M) (H)

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [*Assignment: organization-defined information system components*].

{{CONTROL|CM-6.1}}

CM-7 Least Functionality (L) (M) (H)

The organization:

(a) Configures the information system to provide only essential capabilities; and

(b) Prohibits or restricts the use of the following functions, ports, protocols, and/or services [*FedRAMP Assignment: United States Government Configuration Baseline (USGCB)*]

CM-7 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

Guidance: Information on the USGCB checklists can be found at: https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline

Partially derived from AC-17 (8).

CM-7	Control Summary Information
Responsible Role: Fraser, Doug	
cm-07_odp.01:	
cm-07_odp.02:	
cm-07_odp.03:	
cm-07_odp.04:	
cm-07_odp.05:	
cm-07_odp.06:	
cm-7_prm_2:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-7 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. **2 Twelve Solutions Responsibility**: Operations& team provides only essential capabilities of ORE infrastructure through the use of automation. The automation settings are configured based on Center for Internet Security guidelines (Level 1) and best practices to ensure that the ORE environment has the most restrictive mode consistent with operational requirements. Connections through ports and protocols are further limited through the use of Firewall rules whitelisting. The full list of approved ports and protocol can be found in section 10 of this SSP. & **Customer Responsibility:&** It is the customer responsibility to configure the information system to provide only essential capabilities.& Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE configuration settings for all system components within the ORE boundary are all configured through automation which are verified by InSpec compliance checks.& All automation are based on Center for Internet Security guidelines (Level 1) and best practices to ensure that the ORE environment has the most restrictive mode consistent with operational requirements. & Application: ORE applications follow the 2 Twelve Solutions ORE Lifecycle Management Plan and procedures defined in this SSP to ensure security considerations are in place in all steps of the ORE system lifecycle. There is no established baseline for the ORE application. InSpec vulnerability scanner is used at least monthly to ensure the security posture of the ORE application is below established risk level. & Database and Operating System:& 2 Twelve Solutions ORE establishes and documents configuration settings for information technology products employed within the ORE authorization boundary that reflect the most restrictive mode consistent with operational requirements and the CIS Level 1 guidelines. InSpec scanner is used to verify and compare configuration settings with CIS Level 1. & **Customer Responsibility:&** It is the customer responsibility to prohibit or restrict the use of functions, ports, protocols, and/or services in accordance with United States Government Configuration Baseline (USGCB).

Part b	

CM-7 (1) CONTROL ENHANCEMENT (M) (H)

The organization:

(a) Reviews the information system [*FedRAMP Assignment: at least Monthly*] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and

(b) Disables [*Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure*].

CM-7 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
cm-07.01_odp.01:	
cm-07.01_odp.02:	
cm-07.01_odp.03:	
cm-07.01_odp.04:	
cm-07.01_odp.05:	
cm-07.01_odp.06:	
Parameter CM-7(1)(b)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-7 (1) What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE configuration settings for all system components within the ORE boundary are all configured through automation which are verified by InSpec and Trivy scanner.& All automation are based on Center for Internet Security guidelines (Level 1) and best practices to ensure that the ORE environment has the most restrictive mode consistent with operational requirements. The Engineering team reviews the results of the InSpec and Trivy scans at least monthly to identify any unnecessary and/or non-secure functions, ports, protocols, and services through this process. & Application: ORE applications follow the 2 Twelve Solutions ORE Lifecycle Management Plan and procedures defined in this SSP to ensure security considerations are in place in all steps of the ORE system lifecycle. There is no established baseline for the ORE application. InSpec vulnerability scanner is used at least monthly to ensure the security posture of the ORE application is below established risk level. & Database:& Inspec scanner is utilized to scan configuration compliance on databases within the ORE environment. All scan will be completed using administrator level authentication to grant the ability to do deep scanning of the database. Inspec is configured to automatically check for updates daily. & Operating System: 2 Twelve Solutions& utilizes InSpec for configuration compliance on operating systems. InSpec authentication scans are done through the InSpec agent. InSpec agents are deployed to every instance within the environment; InSpec agent has system level access which is equivalent or better than an administrative permission. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Any unnecessary and/or non-secure functions, ports, protocols, and services discovered through the InSpec and Trivy scan by the Engineering team will be forwarded to the Operations team through the Agile system ticketing system for disablement. Scan reports are reviewed at least monthly as part of the continuous monitoring process to ensure that the ORE environment has the most restrictive mode consistent with operational requirements.
Part b	

CM-7 (2) CONTROL ENHANCEMENT (M) (H)

The information system prevents program execution in accordance with [*Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage*].

CM-7 (2) Additional FedRAMP Requirements and Guidance:

Guidance: This control shall be implemented in a technical manner on the information system to only allow programs to run that adhere to the policy (i.e., white listing). This control is not to be based off of strictly written policy on what is allowed or not allowed to run.

CM-7 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
cm-07.02_odp.01:	
cm-07.02_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-7 (2) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: <u>Application and Database</u>:& ORE applications are developed and implemented in accordance to the 2 Twelve Solutions ORE Lifecycle Management Plan. ORE Application suite includes database, installation of additional software is not possible. & <u>Operating System</u>: The 2 Twelve Solutions ORE information system and its supporting infrastructure are deployed using automation to prevent the installation of unauthorized software and executables from being run or installed. System-level change permissions are limited to members of the Operations teams, and package installations on the Linux machines supporting the 2 Twelve Solutions ORE& environment are controlled through configuration of system images and deployments using automation Playbook.

CM-7 (5) CONTROL ENHANCEMENT (M)

The organization:

(a) Identifies [*Assignment: organization-defined software programs authorized to execute on the information system*];

(b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and

(c) Reviews and updates the list of authorized software programs [*FedRAMP Assignment: at least annually or when there is a change*].

CM-7 (5)	Control Summary Information
Responsible Role: Fraser, Doug	
cm-07.05_odp.01:	
cm-07.05_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-7 (5) What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Before installing or enabling any application or service, 2 Twelve Solutions conducts a security impact analysis to determine the service's requirements, vendor reputation, and required maintenance which is then detailed and documented. When allowing a new program to be used within the environment, a change request is created which then follows 2 Twelve Solutions's change management process to receive approval for implementation from the ARB. & 2 Twelve Solutions has implemented configuration management tools used to further enforce the exclusive use of authorized software: Configuration on management tools Package installations on the Linux machines supporting the 2 Twelve Solutions ORE environment are controlled through configuration of system images and deployments using automation. 2 Twelve Solutions establishes configuration profiles that are compiled for various system components. All software found inside these profiles is authorized to run within the environment& and deployed as a means of controlling configurations for devices.& Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions employs a deny-all, permit-by-exception policy for software installation. The deny-all, permit-by-exception policy is enforced through the use of automation playbook. During each deployment of the automation playbook, configuration settings and software are readjusted to the approved baseline. In addition, all privilege action including software update and installations are captured in SIEM as an event for review. Part c: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions& reviews and updates the list of authorized software to be included within 2 Twelve Solutions ORE authorization boundary annually, or when there is a significant change requiring addition or removal of software to the approved list. Software configurations for systems are stored within the

	systems' configuration baselines and images. If any modification is required to the approved software list, a change request is created which then proceeds through the change management process to determine if approval is received.
Part b	
Part c	

CM-8 Information System Component Inventory (L) (M) (H)

The organization:

(a) Develops and documents an inventory of information system components that:

(1) Accurately reflects the current information system;
(2) Includes all components within the authorization boundary of the information system;
(3) Is at the level of granularity deemed necessary for tracking and reporting; and
(4) Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and

(b) Reviews and updates the information system component inventory [*FedRAMP Assignment: at least monthly*].

CM-8 Additional FedRAMP Requirements and Guidance:

Requirement: Must be provided at least monthly or when there is a change.

CM-8	Control Summary Information
Responsible Role: Fraser, Doug	
cm-08_odp.01:	
cm-08_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-8 What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions ORE utilizes configuration management and security tools to develop and document the complete inventory of the 2 Twelve Solutions ORE authorization boundary while providing the level of granularity deemed necessary for tracking and reporting. InSpec is used to regularly generate an output of all assets in the ORE environment. Every component within the ORE environment has a InSpec agent installed that is able to accurately reflect the hostnames, IP addresses, locations, and asset types for all components. After the initial AWS inventory is generated, ORE uses agent-based InSpec scans to verify reported system versions and automation configuration management scripts to verify the latest baseline configuration packages used for system assets. The inventory is reviewed and updated at least monthly and is also part of the SSP. & The combined functions of these tools are used to achieve compliance by: • Accurately reflecting all components within the authorization boundary of the current information system • Providing granularity required to enable tracking and reporting • Including all 2 Twelve Solutions ORE infrastructure and services to achieve effective information system component accountability Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions verifies that all components within the authorization boundary of the information system are inventoried as part of the system on a monthly basis, or when a change is made to the information system. & The component information that is generated by automation and makes use of the Azure APIs and AWS APIs as input to collect the appropriate inventory data for the Inventory Workbook that will be reviewed and updated by the Engineering at least monthly as part of the continuous monitoring process.
Part a1	
Part a2	

Part a3	
Part a4	
Part a5	
Part b	

CM-8 (1) CONTROL ENHANCEMENT (M) (H)

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

Instruction: A description of the inventory information is documented in Section 10. It is not necessary to re-document it here.

Delete this and all other instructions from your final version of this document.

CM-8 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-8 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions ORE requires all component installations, removals, and information system changes to go through the established change management process detailed in this SSP and the 2 Twelve Solutions FedRAMP ORE Configuration and Change Management Plan. As part of the security impact analysis, Engineering will identify if an inventory update is required for each change. When the change is approved, Engineering will update the inventory matrix to reflect the updated ORE component(s).

CM-8 (3) CONTROL ENHANCEMENT (M) (H)

The organization:

(a) Employs automated mechanisms [*FedRAMP Assignment: Continuously, using automated mechanisms with a maximum five-minute delay in detection*] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and

(b) Takes the following actions when unauthorized components are detected: [*Selection (one or more): disables network access by such components; isolates the components; notifies* [*Assignment: organization-defined personnel or roles*]].

CM-8 (3)	Control Summary Information
Responsible Role: Fraser, Doug	
cm-08.03_odp.01:	
cm-08.03_odp.02:	
cm-08.03_odp.03:	
cm-08.03_odp.04:	
cm-08.03_odp.05:	
cm-08.03_odp.06:	
Parameter CM-8(3)(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-8 (3) What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions utilizes its configuration policy and AWS configuration management tools to create, manage, and enforce the environment inventory.& Assets are configured using automated solutions; consequently 2 Twelve Solutions ORE team members use log collector to assist with inventory monitoring. Logs are forwarded to SIEM for near real time analysis and alerting. When components are added to the environment, SIEM will generate an alert with a maximum of five minute delay to the Operations and Engineering. & & For each component within the ORE environment, OSSEC IPS and SIEM is leveraged to detect unauthorized software. In the event system assets deviate from previous environmental states, OSSEC alerts are sent to 2 Twelve Solutions ORE administrators to the for investigation and remediation. When changes are detected by SIEM or OSSEC, a message is sent to the 2 Twelve Solutions security team.& All messages are delivered to securityincidents@2TwelveSolutions.com Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: SIEM and OSSEC are used by 2 Twelve Solutions to continuously record and monitor (with a maximum five-minute delay in detection) AWS resources (EC2 instances) to detect the presence of unauthorized hardware, software, and firmware components. SIEM and OSSEC both monitor and identify AWS resource configurations for configuration changes that create inconsistencies with established rules or profiles. & In the event system assets deviate from previous environmental states, alerts are sent to 2 Twelve Solutions ORE administrators to the for investigation and remediation. When changes are detected by SIEM or OSSEC, a message is sent to the 2 Twelve Solutions security team.& All messages are delivered to securityincidents@2TwelveSolutions.com
Part b	

CM-8 (5) CONTROL ENHANCEMENT (M) (H)

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

{{CONTROL|CM-8.5}}

CM-9 Configuration Management Plan (M) (H)

The organization develops, documents, and implements a configuration management plan for the information system that:

(a) Addresses roles, responsibilities, and configuration management processes and procedures;

(b) Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

(c) Defines the configuration items for the information system and places the configuration items under configuration management; and

(d) Protects the configuration management plan for unauthorized disclosure and modification.

CM-9	Control Summary Information
Responsible Role: Fraser, Doug	
cm-09_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-9 What is the solution and how is it implemented?

Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: 2 Twelve Solutions policies as they relate to configuration management for ORE are outlined in the ORE Configuration Management Plan. The plan addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements to meet the control implementation requirements for the configuration management control family of a moderate baseline.& The plan specifically addresses procedures or processes related to: • Configuration Management Roles and Responsibilities • Configuration Management Program Administration& • Configuration Management Tools • Configuration Management Retention, Archiving, Storage and Disposal • Configuration Identification • Configuration Baselining • Configuration Change Control • Configuration Management Monitoring& • Configuration Management Reporting & All ORE documentation related to policies and procedures are stored and protected on internal Thanos document management system. & **<u>Customer Responsibility:</u>&** It is the customer responsibility to develop a configuration management plan that addresses roles, responsibilities and configuration management processes and procedures. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: <u>Application or Database or Operating System:</u> The Operations& team is responsible for defining Configuration Item's (CI's) within ORE. Operations& team defines CI's as any component that needs to be managed in order to maintain and execute the operations of ORE. Information about each CI is recorded in Inventory Workbook, which is produced monthly as part of the continuous monitoring process.& The inventory documents the CI attributes such as the unique asset name, IP address, the DNS, configuration baseline version, OS name and version, and all

	requirements derived from the Inventory Workbook. & **Customer Responsibility:&** It is the customer responsibility to develop a configuration management plan that establishes a process for identifying configuration items throughout the system development life cycle. Part c: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The Operations& team is responsible for defining Configuration Item's (CI's) within ORE. Operations& team defines CI's as any component that needs to be managed in order to maintain and execute the operations of ORE. Information about each CI is recorded in Inventory Workbook, which is produced monthly as part of the continuous monitoring process.& The inventory documents the CI attributes such as the unique asset name, IP address, the DNS, configuration baseline version, OS name and version, and all requirements derived from the Inventory Workbook. The CI information that is generated through this process will be the backbone of the configuration management process to ensure that all CI additions, modifications, and/or deletions is parallel to the actual disposition of ORE and to ensure the security posture of the environment remains at acceptable levels. **Customer Responsibility:&** It is the customer responsibility to develop a configuration management plan that defines the configuration items for the information system and places the configuration items under configuration management.& Part d: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: All ORE documentation related to policies and procedures are stored and protected in the Thanos document management system repository. Privileged access into ORE is only available to the Engineering team with read only access to the Operations Team. Access control and the concept of least privilege is in place such that team members will only have enough permissions to carry out his or her duty. &

	Customer Responsibility:& It is the customer responsibility to protect the configuration management plan from unauthorized disclosure or modification.&
Part b	
Part c	
Part d	
Part e	

CM-10 Software Usage Restrictions (L) (M) (H)

The organization:

(a) Uses software and associated documentation in accordance with contract agreements and copyright laws;

(b) Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

(c) Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

CM-10	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-10 What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Components and/or services that require an enterprise license, contract agreements, and/or SLAs are executed in accordance with the contractual language of the agreement by 2 Twelve Solutions legal. Engineering monitor the use of these resource through the use the SIEM, Agile system ticketing system, and InSpec and Nessus Scanner. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Licenses for ORE are tracked through the management console and licenses for security tools, such as InSpec, are managed and tracked in the InSpec.& 2 Twelve Solutions also tracks the licensing and use of all software within the information system manually in an Excel spreadsheet that is managed by the Engineering team. Part c: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions does not allow the use of peer-to-peer sharing technology. Peer-to-peer is not explicitly allowed in automation and Security Group rules. Any attempt to install or executive peer-to-peer technology is captured and notified through SIEM.
Part b	
Part c	

CM-10 (1) CONTROL ENHANCEMENT (M) (H)

The organization establishes the following restrictions on the use of open source software: [*Assignment: organization-defined restrictions*].

{{CONTROL|CM-10.1}}

CM-11 User-Installed Software (M) (H)

The organization:

(a) Establishes [*Assignment: organization-defined policies*] governing the installation of software by users;

(b) Enforces software installation policies through [*Assignment: organization-defined methods*]; and

(c) Monitors policy compliance [*FedRAMP Assignment: Continuously (via CM-7 (5))*].

CM-11	Control Summary Information
Responsible Role: Fraser, Doug	
cm-11_odp.01:	
cm-11_odp.02:	
cm-11_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CM-11 What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Only privileged infrastructure users have the ability to install software in the ORE environment. The only privileged user groups within ORE are the Engineering team& (read only) and the Operations team. General users do not have the ability to install software in the ORE environment. Software installation can only be accomplished at the operating system level within the ORE environment. & Software installations obtain approval through the change management process detailed in this SSP and the 2 Twelve Solutions& ORE_Configuration and Change Management Plan. All change requires are requested, tracked, and retained in a form of Agile system ticket. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The configuration control process for ORE enforces adherence to the software installation polices, through executive oversight in the ARB, multi-party approval required by the Onboarding process and by leveraging automation. Once software is approved, it will be added to the automation as part of the baseline. automation is used to deploy the new baseline and adjust configuration settings.& Part c: This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Policy compliance monitoring for user-installed software is accomplished through SIEM. All system events, component changes, and privilege actions are captured and forward to SIEM for near real time monitoring and alerting. Pre-configured items are in place such that software installation attempts are captured and will be alerted with maximum of five minutes delay. Engineering and Operations will receive the alert to investigate the issue in detail.
Part b	

Part c	

13.6. Contingency Planning (CP)

CP-1 Contingency Planning Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

(b) Reviews and updates the current:

(1) Contingency planning policy [*FedRAMP Assignment: at least every three (3) years*].; and

(2) Contingency planning procedures [*FedRAMP Assignment: at least annually*].

CP-1	Control Summary Information
Responsible Role: Tong, Thanh	
cp-01_odp.01:	
cp-01_odp.02:	
cp-01_odp.03:	
cp-01_odp.04:	
cp-01_odp.05:	
cp-01_odp.06:	
cp-01_odp.07:	
cp-01_odp.08:	
Parameter CP-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

CP-1 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

CP-2 Contingency Plan (L) (M) (H)

The organization:

(a) Develops a contingency plan for the information system that:

(1) Identifies essential missions and business functions and associated contingency requirements;
(2) Provides recovery objectives, restoration priorities, and metrics;
(3) Addresses contingency roles, responsibilities, assigned individuals with contact information;
(4) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
(5) Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
(6) Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];

(b) Distributes copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];

(c) Coordinates contingency planning activities with incident handling activities;

(d) Reviews the contingency plan for the information system [*FedRAMP Assignment: at least* *annually*];

(e) Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

(f) Communicates contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*]; and

(g) Protects the contingency plan from unauthorized disclosure and modification.

CP-2 Additional FedRAMP Requirements and Guidance:

Requirement: For JAB authorizations the contingency lists include designated FedRAMP personnel.

CP-2	Control Summary Information
Responsible Role: Tong, Thanh	
cp-02_odp.01:	
cp-02_odp.02:	
cp-02_odp.03:	
cp-02_odp.04:	
cp-02_odp.05:	
cp-02_odp.06:	
cp-02_odp.07:	
Parameter CP-2(a)(6)):	
Parameter CP-2(b)):	
Parameter CP-2(f)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-2 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a2	
Part a3	
Part a4	
Part a5	
Part a6	
Part a7	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	

CP-2 (1) CONTROL ENHANCEMENT (M) (H)

The organization coordinates contingency plan development with organizational elements responsible for related plans.

CP-2 (1)	Control Summary Information
Responsible Role: Tong, Thanh	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-2 (1) What is the solution and how is it implemented?

CP-2 (3) CONTROL ENHANCEMENT (M) (H)

The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

CP-2 (3)	Control Summary Information
Responsible Role: Tong, Thanh	
cp-02.03_odp.01:	
cp-02.03_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-2 (3) What is the solution and how is it implemented?

CP-2 (8) CONTROL ENHANCEMENT (M) (H)

The organization identifies critical information system assets supporting essential missions and business functions.

CP-2 (8)	Control Summary Information
Responsible Role: Tong, Thanh	
cp-02.08_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-2 (8) What is the solution and how is it implemented?

CP-3 Contingency Training (L) (M) (H)

The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

(a) Within [*FedRAMP Assignment: ten (10) days*] of assuming a contingency role or responsibility;

(b) When required by information system changes; and

(c) [*FedRAMP Assignment: at least annually*] thereafter.

CP-3	Control Summary Information
Responsible Role: Tong, Thanh	
cp-03_odp.01:	
cp-03_odp.02:	
cp-03_odp.03:	
cp-03_odp.04:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-3 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a2	
Part a3	
Part b	

CP-4 Contingency Plan Testing (M)

The organization:

(a) Tests the contingency plan for the information system [*FedRAMP Assignment: at least annually*] using [*FedRAMP Assignment: functional exercises*] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

CP-4(a) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to FedRAMP prior to initiating testing. Test plans are approved and accepted by the JAB/AO prior to initiating testing.

(b) Reviews the contingency plan test results; and

(c) Initiates corrective actions, if needed.

CP-4	Control Summary Information
Responsible Role: Tong, Thanh	
cp-04_odp.01:	
cp-04_odp.02:	
cp-04_odp.03:	
Parameter CP-4(a)-2):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-4 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	

CP-4 (1) CONTROL ENHANCEMENT (M) (H)

The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

CP-4 (1)	Control Summary Information
Responsible Role: Tong, Thanh	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-4 (1) What is the solution and how is it implemented?

CP-6 Alternate Storage Site (M) (H)

The organization:

(a) Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and

(b) Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

CP-6	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-6 What is the solution and how is it implemented?	
Part a	
Part b	

CP-6 (1) CONTROL ENHANCEMENT (M) (H)

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

CP-6 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-6 (1) What is the solution and how is it implemented?

CP-6 (3) CONTROL ENHANCEMENT (M) (H)

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

CP-6 (3)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-6 (3) What is the solution and how is it implemented?

CP-7 Alternate Processing Site (M) (H)

The organization:

(a) Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined information system operations*] for essential missions/business functions within [*FedRAMP Assignment: see additional FedRAMP requirements and guidance*] when the primary processing capabilities are unavailable;

CP-7a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

(b) Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and

(c) Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

CP-7	Control Summary Information
Responsible Role: Fraser, Doug	
cp-07_odp.01:	
cp-07_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-7 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	

CP-7 (1) CONTROL ENHANCEMENT (M) (H)

The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

CP-7 (1) Additional FedRAMP Requirements and Guidance

Guidance: The service provider may determine what is considered a sufficient degree of separation between the primary and alternate processing sites, based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites will be less relevant.

CP-7 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-7 (1) What is the solution and how is it implemented?

CP-7 (2) CONTROL ENHANCEMENT (M) (H)

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

CP-7 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-7 (2) What is the solution and how is it implemented?

CP-7 (3) CONTROL ENHANCEMENT (M) (H)

The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

CP-7 (3)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-7 (3) What is the solution and how is it implemented?

CP-8 Telecommunications Services (M) (H)

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [*Assignment: organization-defined information system operations*] for essential missions and business functions within [*FedRAMP Assignment: See CP-8 additional FedRAMP requirements and guidance*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

CP-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

CP-8	Control Summary Information
Responsible Role: Fraser, Doug	
cp-08_odp.01:	
cp-08_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-8 What is the solution and how is it implemented?

CP-8 (1) CONTROL ENHANCEMENT (M) (H)

The organization:

(a) Develops primary and alternate telecommunications service agreements that contain priority- of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and

(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

CP-8 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-8 (1) What is the solution and how is it implemented?	
Part a	
Part b	

CP-8 (2) CONTROL ENHANCEMENT (M) (H)

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

CP-8 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-8 (2) What is the solution and how is it implemented?

CP-9 Information System Backup (L) (M) (H)

The organization:

CP-9 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine what elements of the cloud environment require the Information System Backup control. The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check.

(a) Conducts backups of user-level information contained in the information system [*FedRAMP Assignment: daily incremental; weekly full*]

CP-9 (a) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online).

(b) Conducts backups of system-level information contained in the information system [*FedRAMP Assignment: daily incremental; weekly full*];

CP-9 (b) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online).

(c) Conducts backups of information system documentation including security-related documentation [*FedRAMP Assignment: daily incremental; weekly full*]; and

CP-9 (c) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online).

(d) Protects the confidentiality, integrity, and availability of backup information at storage locations.

CP-9	Control Summary Information
Responsible Role: Fraser, Doug	
cp-09_odp.01:	
cp-09_odp.02:	
cp-09_odp.03:	
cp-09_odp.04:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-9 What is the solution and how is it implemented?

Part a	This control is reviewed annually by the ISSO and SO. Part a: & **<u>2 Twelve Solutions Responsibility</u>** 2 Twelve Solutions performs full nightly backups of user-level information through snapshots. 2 Twelve Solutions ORE ensures at least three backup snapshots of user-level information are maintained for long-term storage. All snapshots in the S3 buckets are available online. Backups stored on the S3 bucket are automatically stored across multiple devices spanning a minimum of three Availability Zones, each separated by miles across an AWS Region. Part b: **<u>2 Twelve Solutions Responsibility</u>** 2 Twelve Solutions performs full nightly backups of user-level information through snapshots. 2 Twelve Solutions ORE ensures at least three backup snapshots of user-level information are maintained for long-term storage. All snapshots in the S3 buckets are available online. Backups stored on the S3 bucket are automatically stored across multiple devices spanning a minimum of three Availability Zones, each separated by miles across an AWS Region. Part c: **<u>2 Twelve Solutions Responsibility</u>** All documentation including security-related information is maintained and backed up on the internal Thanos document management system. Version controls for all documents are enforced and all versions are archived and never deleted. The Thanos document management system has access control in place to only allow authorized users to access each document. Part d: **<u>2 Twelve Solutions Responsibility</u>** 2 Twelve Solutions ORE utilizes AWS S3 bucket for long-term storage. All snapshots in the S3 buckets are available online. Backups stored on the S3 bucket are automatically stored across multiple devices spanning a minimum of three Availability Zones, each separated by miles across an AWS Region. & Encryptions for backups are automatically enabled to protect the confidentiality, integrity, and availability

	of the data at rest. By& default, AWS KMS keys with AES-256 are used for each S3 bucket. Multiple layers of security protect the S3 buckets; the S3 buckets are only accessible by users that have been previously authorized to access the buckets. The ORE environment operates on a strict whitelist, only the IPs that has been put into the security group rule has access to the system.
Part b	
Part c	
Part d	

CP-9 (1) CONTROL ENHANCEMENT (M)

The organization tests backup information [*FedRAMP Assignment: at least annually*] to verify media reliability and information integrity.

CP-9 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
cp-09.01_odp.01:	
cp-09.01_odp.02:	
Parameter CP-9 (1)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-9 (1) What is the solution and how is it implemented?
This control is reviewed annually by the ISSO and SO. & **2 Twelve Solutions Responsibility:** 2 Twelve Solutions tests the reliability and integrity of backup information at least annually as part of the annual contingency plan exercise. ORE backup test ensures normal functions can be resumed within the established recovery time objective.

CP-9 (3) CONTROL ENHANCEMENT (M) (H)

The organization stores backup copies of [*Assignment: organization-defined critical information system software and other security-related information*] in a separate facility or in a fire-rated container that is not collocated with the operational system.

{{CONTROL|CP-9.3}}

CP-10 Information System Recovery and Reconstitution (L) (M) (H)

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

CP-10	Control Summary Information
Responsible Role: Fraser, Doug	
cp-10_odp.01:	
cp-10_odp.02:	
cp-10_prm_1:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-10 What is the solution and how is it implemented?
This control is reviewed annually by the ISSO and SO. & **2 Twelve Solutions Responsibility** 2 Twelve Solutions' ORE environment spans multiple availability zones. Load Balancers distribute traffic to instances such as that if instances in one AZ become unhealthy or experienced a failure in services; traffic would automatically be routed to the other AZs in the same region. & In the event of a disruption, compromise, or failure, the Operations team will receive an alert. The Operations team will analyze the event and determine if ISCP activation is required. The Operations& team will resolve the issues for the client(s) that were affected. ORE has nightly full backups, so 2 Twelve Solutions is able to bring the system back up to a good state before the disaster occurred. 2 Twelve Solutions' recovery time objective is to have the system back up and operational within 2 hours of activation of the Contingency Plan.

CP-10 (2) CONTROL ENHANCEMENT (M) (H)

The information system implements transaction recovery for systems that are transaction-based.

CP-10 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

CP-10 (2) What is the solution and how is it implemented?
This control is reviewed annually by the ISSO and SO. & **2 Twelve Solutions Responsibility** Database backups are done through snapshots on a daily basis and are stored encrypted. All ORE environment information is replicated across the availability zones to prevent loss of data in the event of an availability zone failure.

13.7. Identification and Authentication (IA)

IA-1 Identification and Authentication Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and

(b) Reviews and updates the current:

(1) Identification and authentication policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Identification and authentication procedures [*FedRAMP Assignment: at least annually*].

IA-1	Control Summary Information
Responsible Role: Fraser, Doug	
ia-01_odp.01:	
ia-01_odp.02:	
ia-01_odp.03:	
ia-01_odp.04:	
ia-01_odp.05:	
ia-01_odp.06:	
ia-01_odp.07:	
ia-01_odp.08:	
Parameter IA-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

IA-1 What is the solution and how is it implemented?

Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Part a: & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions ORE Information Security Policy directs the activities within the ORE Access Management Plan. The plan addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements to meet the control implementation requirements for the IA family of a moderate baseline. The plan specifically addresses procedures or processes related to: • Information Access Restriction • The Request Fulfillment Process for Provisioning Access • The Periodic Review of Access • The Revocation of Access • The Separation of Duties • Access Control to Program Source Code • Authenticator Device Management • Encryption & All ORE procedures that are captured in Thanos document management system, 2 Twelve Solutions's document repository management system, are reviewed on an annual basis by the Engineering and ARB. The ARB consists of the Engineering and Operations. The ARB is responsible for notifying stakeholders when changes are made and approved by the ARB. This may require the creation of new documentation or reviewing and updating current procedures, annually or as needed; and policies every 3 years or as needed. Part b: The Operations and Engineering team are responsible for reading the document on an annual basis. The team composition includes the following: • Engineering; • Operations; and

	- ORE Leadership Part c: **2 Twelve Solutions Responsibility**: ORE policies are reviewed and updated every three years by the Operations team. The Engineering team updates the procedures annually. The ARB approves all changes.
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

IA-2 User Identification and Authentication (L) (M) (H)

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

IA-2	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-2 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions uniquely identifies and authenticates organizational users.& The ORE& application accepts and electronically verifies PIV cards and CAC through interaction with upstream identity management solutions. Accounts maintained on upstream Identity Management systems will be used for application access. ORE will accept SAML and OIDC tokens from Identity Access Management Systems. These users would connect to ORE using HTTPS with TLS v1.3. Typically this would include a user ID, password or PIN and a Personal Identity Verification (PIV) card or Common Access Card (CAC) to complete authentication to the ORE. Once users have been successfully authenticated, a specific role will be assigned.

IA-2 (1) CONTROL ENHANCEMENT (L) (M) (H)

The information system implements multifactor authentication for network access to privileged accounts.

IA-2 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-2 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions ORE requires MFA for network access to privileged accounts. Additionally, the ORE& application accepts and electronically verifies PIV cards and CAC through interaction with upstream identity management solutions. Accounts maintained on upstream Identity Management systems will be used for application access. ORE will accept SAML and OIDC tokens from Identity Access Management Systems. These users would connect to ORE using HTTPS with TLS v1.3. Typically this would include a user ID, password or PIN and a Personal Identity Verification (PIV) card or Common Access Card (CAC) to complete authentication to the ORE. Firewall rules are used to define access to the ORE Application.

IA-2 (2) CONTROL ENHANCEMENT (M) (H)

The information system implements multifactor authentication for network access to non-privileged accounts.

IA-2 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-2 (2) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Applications can only be accessed through the front portal through MFA or SSO through SAML or OIDC. All access to the applications and APIs is through reverse proxies that enforce HTTPS via TLS v1.3. Additionally, the ORE& application accepts and electronically verifies PIV cards and CAC through interaction with upstream identity management solutions. Accounts maintained on upstream Identity Management systems will be used for application access. ORE will accept SAML and OIDC tokens from Identity Access Management Systems. These users would connect to ORE using HTTPS with TLS v1.3. Typically this would include a user ID, password or PIN and a Personal Identity Verification (PIV) card or Common Access Card (CAC) to complete authentication to the ORE.Firewall rules are used to define access to the ORE Application. & Authorized 2 Twelve Solutions administrators access operating systems by authenticating through the bastion host. All users must have a valid SSH key. After authentication through the bastion host, users must have a matching public SSH key on the operating system to establish a connection with that host. Connections are enforced through whitelisting by Firewall rules. &

IA-2 (3) CONTROL ENHANCEMENT (M) (H)

The information system implements multifactor authentication for local access to privileged accounts.

{{CONTROL|IA-2.3}}

IA-2 (5) CONTROL ENHANCEMENT (M) (H)

The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

{{CONTROL|IA-2.5}}

IA-2 (8) CONTROL ENHANCEMENT (M) (H)

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

IA-2 (8)	Control Summary Information
Responsible Role: Fraser, Doug	
ia-02.08_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-2 (8) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Applications can only be accessed through the front portal through MFA or SSO through SAML or OIDC. All access to the applications and APIs is through reverse proxies that enforce HTTPS via TLS v1.3. Firewall rules are used to define access to the ORE Application. & Authorized 2 Twelve Solutions administrators access operating systems by authenticating through the bastion host. All users must have a valid SSH key. After authentication through the bastion host, users must have a matching public SSH key on the operating system to establish a connection with that host. Connections are enforced through whitelisting by Firewall rules. &

IA-2 (11) CONTROL ENHANCEMENT (M) (H)

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [*FedRAMP Assignment: FIPS 140-2, NIAP* Certification, or NSA approval*].

*National Information Assurance Partnership (NIAP)

Additional FedRAMP Requirements and Guidance:

Guidance: PIV = separate device. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials. FIPS 140-2 means validated by the Cryptographic Module Validation Program (CMVP).

{{CONTROL|IA-2.11}}

IA-2 (12) CONTROL ENHANCEMENT (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

IA-2 (12) Additional FedRAMP Requirements and Guidance:

Guidance: Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12.

IA-2 (12)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-2 (12) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE& application accepts and electronically verifies PIV cards and CAC through interaction with upstream identity management solutions. Accounts maintained on upstream Identity Management systems will be used for application access. ORE will accept SAML and OIDC tokens from Identity Access Management Systems. These users would connect to ORE using HTTPS with TLS v1.3. Typically this would include a user ID, password or PIN and a Personal Identity Verification (PIV) card or Common Access Card (CAC) to complete authentication to the ORE.

IA-3 Device Identification and Authentication (M) (H)

The information system uniquely identifies and authenticates [*Assignment: organization-defined specific and/or types of devices*] before establishing a [*Selection (one or more): local; remote; network*] connection.

IA-3	**Control Summary Information**
Responsible Role: Fraser, Doug	
ia-03_odp.01:	
ia-03_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-3 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions uniquely identifies all devices based on their assigned IP address and hostname. The assigned private IP address is used to identify network devices and an SSH key verification is used to authenticate the servers and network devices before a connection is established.

IA-4 Identifier Management (L) (M)

The organization manages information system identifiers for users and devices by:

(a) Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier;

(b) Selecting an identifier that identifies an individual, group, role, or device;

(c) Assigning the identifier to the intended individual, group, role, or device;

(d) Preventing reuse of identifiers for [*FedRAMP Assignment: at least two (2) years*]; and

(e) Disabling the identifier after [*FedRAMP Assignment: ninety days for user identifiers (see additional requirements and guidance)*]

IA-4e Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines the time period of inactivity for device identifiers.

Guidance: For DoD clouds, see DoD cloud website for specific DoD requirements that go above and beyond FedRAMP http://iase.disa.mil/cloud_security/Pages/index.aspx.

IA-4	Control Summary Information
Responsible Role: Fraser, Doug	
ia-04_odp.01:	
ia-04_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-4 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Part a: & **2 Twelve Solutions Responsibility**: The organization requires authorization in the form of an access authorization ticket, approved prior to the assignment of an identifier. The engineering or account manager will provide the final approval in Agile system for Operations to provision the new user and relevant privileges.& Individuals receive unique identifiers in the form of a User ID (UID). ORE utilizes instance hostname and IP addresses& as device identifiers. Change requests will go through the ARB for new server instances and requirements. Part b: **2 Twelve Solutions Responsibility**: 2 Twelve Solutions uses a naming convention for user accounts that follows [first name].[last name]. In the case of multiple personnel with the same name, numerical values are added at the end of the username. ORE utilizes instance hostnames and IP addresses& as device identifiers. The ORE inventory contains the IP address and hostname associated with each device within the authorization boundary. Part c: **2 Twelve Solutions Responsibility**: Account IDs, are assigned as part of the initial onboarding process. This process is tracked using Agile system tickets. In addition, Device IDs are assigned as part of the launching of the system. This process is also tracked using Agile system tickets. Part d: **2 Twelve Solutions Responsibility**: 2 Twelve Solutions does not reuse any account names or identifiers.
Part b	
Part c	

Part d	

IA-4 (4) CONTROL ENHANCEMENT (M) (H)

The organization manages individual identifiers by uniquely identifying each individual as [*FedRAMP Assignment: contractors; foreign nationals*].

IA-4 (4)	**Control Summary Information**
Responsible Role: Fraser, Doug	
ia-04.04_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-4 (4) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: In the event that a user is a contractor or foreign national, the 2 Twelve Solutions account manager will designate this role condition with either a -CTR or -FN, respectively. At this time, 2 Twelve Solutions ORE does not authorize access to foreign national personnel. For contractors, the same authorization process will be followed and documented through Agile system ticket.

IA-5 Authenticator Management (L) (M)

The organization manages information system authenticators by:

(a) Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

(b) Establishing initial authenticator content for authenticators defined by the organization;

(c) Ensuring that authenticators have sufficient strength of mechanism for their intended use;

(d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

(e) Changing default content of authenticators prior to information system installation;

(f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

(g) Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*].

(h) Protecting authenticator content from unauthorized disclosure and modification;

(i) Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

(j) Changing authenticators for group/role accounts when membership to those accounts changes.

IA-5 Additional FedRAMP Requirements and Guidance:

Requirement: Authenticators must be compliant with NIST SP 800-63-3 Digital Identity Guidelines IAL, AAL, FAL level 2. Link https://pages.nist.gov/800-63-3.

IA-5	Control Summary Information
Responsible Role: Fraser, Doug	
ia-05_odp.01:	
ia-05_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-5 What is the solution and how is it implemented?

Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Part a: & **<u>2 Twelve Solutions Responsibility</u>**: 2 Twelve Solutions& personnel who require administrator access to the ORE environment are verified as part of the onboarding process. The onboarding process includes a background check to include the verification of the individual's identity and address. User accounts and initial temporary passwords will be set up as follows: & • The Operations team creates user accounts and distributes initial temporary passwords through email, or by separate channels such as slack or phone. • Initial temporary passwords cannot be blank and must be set to force change at first login. • Each user must have a unique ID and password, and may not access environments without individual identification and multi-factor authentication. Part b: & **<u>2 Twelve Solutions Responsibility</u>**: 2 Twelve Solutions& personnel who require administrator access to the ORE environment are verified as part of the onboarding process. The onboarding process includes a background check to include the verification of the individual's identity and address. User accounts and initial temporary passwords will be set up as follows: & • The Operations team creates user accounts and distributes initial temporary passwords through email, or by separate channels such as slack or phone. • Initial temporary passwords cannot be blank and must be set to force change at first login. • Each user must have a unique ID and password, and may not access environments without individual identification and multi-factor authentication. Part c: **<u>2 Twelve Solutions Responsibility</u>**: 2 Twelve Solutions Policy and Procedures Identification and Authentication, governs 2 Twelve Solutions ORE user accounts and authenticators. Issued passwords meet 2 Twelve Solutions policy requirements respectively for password complexity.

Strong passwords and passphrases must meet the following requirements:&

- Contain at least twelve alphanumeric characters
- Contain both upper and lower case letters.&
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/)

Part d:

<u>2 Twelve Solutions Responsibility</u>:

Lost, compromised, or damaged authenticators are revoked from being used. Users are required to report to Engineering when passwords are lost, compromised, or damaged. The 2 Twelve Solutions ORE Access and Digital Identity Plan establish the procedure for administrating authenticators.
&

Part e:

<u>2 Twelve Solutions Responsibility</u>:

All user passwords for access to the 2 Twelve Solutions ORE environment are required to be changed upon initial user logon.& All default authenticators are required to be changed for all new components that are added to the 2 Twelve Solutions ORE environment.&

Part f:

<u>2 Twelve Solutions Responsibility</u>:

ORE enforce refreshing authenticators through password expiration setting. For all password settings, password expiration is set for 60 or 90 days, defined as the maximum lifetime restriction.

Part g:

<u>2 Twelve Solutions Responsibility</u>:

2 Twelve Solutions administrators are required to protect authenticator content from unauthorized disclosure and modification. The protection of authenticator content is required under the 2 Twelve Solutions ORE Rules of Behavior and the Access and Identify Management Plan. Users who do not comply with the 2 Twelve Solutions ORE Rules of Behavior may incur disciplinary action, including but not limited to employment termination and/or criminal prosecution.

	Part h: **2 Twelve Solutions Responsibility**: Operations maintains password management system features and functionality to include: • Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors • Enforce password complexity • Force users to change their passwords at first log-on • Enforce regular password changes with a maximum password lifetime of 60 or 90 days • Obscure passwords on the screen when being entered • Authenticators are encrypted in storage and transmission Part I: **2 Twelve Solutions Responsibility**: ORE does not utilize group accounts. But if group accounts are ever used regular password changes are enforced with a maximum password lifetime of 60 or 90 days &
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	

IA-5 (1) CONTROL ENHANCEMENT (L) (M)

The information system, for password-based authentication:

(a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*];

(b) Enforces at least the following number of changed characters when new passwords are created: [*FedRAMP Assignment: at least one (1)*];

(c) Stores and transmits only cryptographically-protected passwords;

(d) Enforces password minimum and maximum lifetime restrictions of [*Assignment: organization- defined numbers for lifetime minimum, lifetime maximum*];

(e) Prohibits password reuse for [*FedRAMP Assignment: twenty-four (24)*] generations; and

(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

IA-5 (1) a and d Additional FedRAMP Requirements and Guidance:

Guidance: If password policies are compliant with NIST SP 800-63B Memorized Secret (Section 5.1.1) Guidance, the control may be considered compliant.

IA-5 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
ia-05.01_odp.01:	
ia-05.01_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-5 (1) What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE ensures that technical controls are in place to ensure appropriate password complexity. PKI authentication is available using PIV and CAC credentials to access the ORE Application. In the event, a specific access surface does require username/password it will be inline with the requirements as seen below. & Strong passwords and passphrases must meet the following requirements:& • Contain at least twelve alphanumeric characters • Contain both upper and lower case letters.& • Contain at least one number (for example, 0-9). • Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/) & When issued, default credentials are required to be changed immediately upon issuance and changed to a complex password as indicated above. All password transmissions are submitted via TLS 1.3 encrypted session.
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	

IA-5 (2) CONTROL ENHANCEMENT (M) (H)

The information system, for PKI-based authentication:

(a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;

(b) Enforces authorized access to the corresponding private key;

(c) Maps the authenticated identity to the account of the individual or group; and

(d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

IA-5 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-5 (2) What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Part a: **<u>2 Twelve Solutions Responsibility</u>**: Certificate-based PKI authentication is available to be used to authenticate to the ORE.& The ORE integrates with upstream identity management systems which allows the leveraging of PIV and CAC card credentials for access. This service additionally enables SSO functionality. The upstream identity management system validates the PIV and CAC certificate data, including checking the validation of certificate status, validation of keys, user data, and revocation data. By default, the Reverse Proxy only accepts TLS 1.3 and Let's Encrypt is leveraged as the root certificate for HTTPS connection. Part b: **<u>2 Twelve Solutions Responsibility</u>**: Certificate-based PKI authentication is available to be used to authenticate to the ORE.& The ORE integrates with upstream identity management systems which allows the leveraging of PIV and CAC card credentials for access. This service additionally enables SSO functionality. The upstream identity management system validates the PIV and CAC certificate data, including checking the validation of certificate status, validation of keys, user data, and revocation data. By default, the Reverse Proxy only accepts TLS 1.3 and Let's Encrypt is leveraged as the root certificate for HTTPS connection. &
Part a1	
Part a2	
Part b	
Part b1	
Part b2	

IA-5 (3) CONTROL ENHANCEMENT (M) (H)

The organization requires that the registration process to receive [*FedRAMP Assignment: All hardware/biometric (multifactor authenticators*] be conducted [*FedRAMP Selection: in person*] before

[*Assignment: organization-defined registration authority*] with authorization by [*Assignment: organization-defined personnel or roles*].

{{CONTROL|IA-5.3}}

IA-5 (4) CONTROL ENHANCEMENT (M)

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [*Assignment: organization-defined requirements*].

IA-5 (4) Additional FedRAMP Requirements and Guidance:

Guidance: If automated mechanisms which enforce password authenticator strength at creation are not used, automated mechanisms must be used to audit strength of created password authenticators.

{{CONTROL|IA-5.4}}

IA-5 (6) CONTROL ENHANCEMENT (M) (H)

The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

IA-5 (6)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-5 (6) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE protects authenticators commensurate with the Moderate categorization of the data in the system per the ORE FIPS-199 categorization. Authenticators are encrypted in transmission and storage. The ORE Rules of Behavior specify actions for individuals to take to protect passwords. Users are trained in security best practices during annual security training.& Users who do not comply with the 2 Twelve Solutions ORE Rules of Behavior may incur disciplinary action, including but not limited to employment termination and/or criminal prosecution. & ORE tools obscure feedback of authentication during the authentication process and does not display passwords in plain text. For access to the ORE application, certificates can be used over HTTPS in the web browser. By default, the Reverse Proxy only accepts TLS 1.3 and Let's Encrypt is leveraged as the root certificate for HTTPS connections. &

IA-5 (7) CONTROL ENHANCEMENT (M) (H)

The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

{{CONTROL|IA-5.7}}

IA-5 (11) CONTROL ENHANCEMENT (L) (M) (H)

The information system, for hardware token-based authentication, employs mechanisms that satisfy [*Assignment: organization-defined token quality requirements*].

{{CONTROL|IA-5.11}}

IA-6 Authenticator Feedback (L) (M) (H)

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

IA-6	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-6 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions obscures authenticator feedback that protects password inputs when the authentication process occurs. Authenticator feedback for the ORE is either hidden or obscured with the use of asterisks (*). This prevents exploitation and use by unauthorized individuals. &

IA-7 Cryptographic Module Authentication (L) (M) (H)

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

IA-7	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-7 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE implements FIPS-validated cryptographic modules, which provide mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. All access to the applications and APIs is through reverse proxies that enforce HTTPS via TLS v1.3. The ORE environment accepts FICAM credentials in the form of a SAML or OIDC token; however, this control requirement is met by the upstream implementation. The ORE environment integrates with upstream identity management systems which allows the leveraging of PIV and CAC card credentials for access. This enforces multi-factor authentication. & &

IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H)

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

IA-8	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-8 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: There are no non-organizational users with access to the ORE. 2 Twelve Solutions ORE supports federated authentication for user SSO using SAML 2.0 assertions or OIDC claims from upstream identity management systems.

IA-8 (1) CONTROL ENHANCEMENT (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

IA-8 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-8 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: Verification of PIV and CAC credentials will be carried out by an upstream identity management system. After successful authentication, SAML assertions or OIDC claims will be transmitted from the identity management systems to ORE. &

IA-8 (2) CONTROL ENHANCEMENT (L) (M) (H)

The information system accepts only FICAM-approved third-party credentials.

IA-8 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-8 (2) What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: All verification of third party credentials will be carried out by upstream identity management systems. It is a customer responsibility to configure their identity management systems to accept only NIST-compliant external authenticators. The ORE environment accepts FICAM credentials in the form of a SAML or OIDC token; however this control requirement is met by the upstream implementation. &
Part b	

IA-8 (3) CONTROL ENHANCEMENT (L) (M) (H)

The organization employs only FICAM-approved information system components in [*Assignment: organization-defined information systems*] to accept third-party credentials.

{{CONTROL|IA-8.3}}

IA-8 (4) CONTROL ENHANCEMENT (L) (M) (H)

The information system conforms to FICAM-issued profiles.

IA-8 (4)	Control Summary Information
Responsible Role: Fraser, Doug	
ia-08.04_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IA-8 (4) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE accepts SAML and OIDC tokens from identity management systems and can work with identity management systems that implement CAC or PIV identification. &

13.8. Incident Response (IR)

IR-1 Incident Response Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

(b) Reviews and updates the current:

(1) Incident response policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Incident response procedures [*FedRAMP Assignment: at least annually*].

IR-1	Control Summary Information
Responsible Role: Tong, Thanh	
ir-01_odp.01:	
ir-01_odp.02:	
ir-01_odp.03:	
ir-01_odp.04:	
ir-01_odp.05:	
ir-01_odp.06:	
ir-01_odp.07:	
ir-01_odp.08:	
Parameter IR-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

IR-1 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

IR-2 Incident Response Training (L) (M)

The organization provides incident response training to information system users consistent with assigned roles and responsibilities in accordance with NIST SP 800-53 Rev 4:

(a) Within [*Assignment: organization-defined time period*] of assuming an incident response role or responsibility;

(b) When required by information system changes; and

(c) [*FedRAMP Assignment: at least annually*] thereafter.

IR-2	Control Summary Information
Responsible Role: Tong, Thanh	
ir-02_odp.01:	
ir-02_odp.02:	
ir-02_odp.03:	
ir-02_odp.04:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IR-2 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a2	
Part a3	
Part b	

IR-3 Incident Response Testing (M)

The organization tests the incident response capability for the information system [*FedRAMP Assignment: at least annually*] using [*FedRAMP Assignment: see additional FedRAMP Requirements and Guidance*] to determine the incident response effectiveness and documents the results.

IR-3 Additional FedRAMP Requirements and Guidance:

Requirements: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). For JAB authorization, the service provider provides test plans to the JAB/AO annually. Test plans are approved and accepted by the JAB/AO prior to the test commencing.

IR-3	Control Summary Information
Responsible Role: Tong, Thanh	
ir-03_odp.01:	
ir-03_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IR-3 What is the solution and how is it implemented?

IR-3 (2) CONTROL ENHANCEMENT (M) (H)

The organization coordinates incident response testing with organizational elements responsible for related plans.

IR-3 (2)	Control Summary Information
Responsible Role: Tong, Thanh	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IR-3 (2) What is the solution and how is it implemented?

IR-4 Incident Handling (L) (M) (H)

The organization:

(a) Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

(b) Coordinates incident handling activities with contingency planning activities; and

(c) Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

IR-4 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

IR-4	Control Summary Information
Responsible Role: Tong, Thanh	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IR-4 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	

IR-4 (1) CONTROL ENHANCEMENT (M) (H)

The organization employs automated mechanisms to support the incident handling process.

IR-4 (1)	Control Summary Information
Responsible Role: Tong, Thanh	
ir-04.01_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IR-4 (1) What is the solution and how is it implemented?

IR-5 Incident Monitoring (L) (M) (H)

The organization tracks and documents information system security incidents.

IR-5	Control Summary Information
Responsible Role: Tong, Thanh	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IR-5 What is the solution and how is it implemented?

IR-6 Incident Reporting (L) (M) (H)

The organization:

(a) Requires personnel to report suspected security incidents to the organizational incident response capability within [*FedRAMP Assignment: US-CERT incident reporting timelines as specified in NIST SP800-61 (as amended)*]; and

(b) Reports security incident information to [*Assignment: organization-defined authorities*].

IR-6 Additional FedRAMP Requirements and Guidance

Requirement: Report security incident information according to FedRAMP Incident Communications Procedure.

IR-6	Control Summary Information
Responsible Role: Tong, Thanh	
ir-06_odp.01:	
ir-06_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IR-6 What is the solution and how is it implemented?	
Part a	
Part b	

IR-6 (1) CONTROL ENHANCEMENT (M) (H)

The organization employs automated mechanisms to assist in the reporting of security incidents.

IR-6 (1)	Control Summary Information
Responsible Role: Tong, Thanh	
ir-06.01_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IR-6 (1) What is the solution and how is it implemented?	
Part b	

IR-7 Incident Response Assistance (L) (M) (H)

The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

IR-7	Control Summary Information
Responsible Role: Tong, Thanh	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IR-7 What is the solution and how is it implemented?

IR-7 (1) CONTROL ENHANCEMENT (M) (H)

The organization employs automated mechanisms to increase the availability of incident response related information and support.

IR-7 (1)	Control Summary Information
Responsible Role: Tong, Thanh	
ir-07.01_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IR-7 (1) What is the solution and how is it implemented?

IR-7 (2) CONTROL ENHANCEMENT (M) (H)

The organization:

(a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and

(b) Identifies organizational incident response team members to the external providers.

{{CONTROL|IR-7.2}}

IR-8 Incident Response Plan (L) (M) (H)

The organization:

(a) Develops an incident response plan that:

(1) Provides the organization with a roadmap for implementing its incident response capability;
(2) Describes the structure and organization of the incident response capability;
(3) Provides a high-level approach for how the incident response capability fits into the overall organization;
(4) Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
(5) Defines reportable incidents;
(6) Provides metrics for measuring the incident response capability within the organization;
(7) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
(8) Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];

(b) Distributes copies of the incident response plan to [*FedRAMP Assignment: see additional FedRAMP Requirements and Guidance*].

IR-8(b) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

(c) Reviews the incident response plan [*FedRAMP Assignment: at least annually*];

(d) Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

(e) Communicates incident response plan changes to [*FedRAMP Assignment: see additional FedRAMP Requirements and Guidance*]; and

IR-8(e) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

(f) Protects the incident response plan from unauthorized disclosure and modification.

IR-8	Control Summary Information
Responsible Role: Tong, Thanh	
ir-08_odp.01:	
ir-08_odp.02:	
ir-08_odp.03:	
ir-08_odp.04:	
ir-08_odp.05:	
ir-08_odp.06:	
ir-08_odp.07:	
ir-8_prm_5:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

IR-8 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a2	
Part a3	
Part a4	
Part a5	
Part a6	
Part a7	
Part a8	
Part a9	
Part a10	
Part b	
Part c	
Part d	
Part e	

IR-9 Information Spillage Response (M) (H)

The organization responds to information spills by:

(a) Identifying the specific information involved in the information system contamination;

(b) Alerting [*Assignment: organization-defined personnel or roles*] of the information spill using a method of communication not associated with the spill;

(c) Isolating the contaminated information system or system component;

(d) Eradicating the information from the contaminated information system or component;

(e) Identifying other information systems or system components that may have been subsequently contaminated; and

(f) Performing other [*Assignment: organization-defined actions*].

{{CONTROL|IR-9}}

IR-9 (1) CONTROL ENHANCEMENT (M) (H)

The organization assigns [*Assignment: organization-defined personnel or roles*] with responsibility for responding to information spills.

{{CONTROL|IR-9.1}}

IR-9 (2) CONTROL ENHANCEMENT (M)

The organization provides information spillage response training [*Assignment: organization- defined frequency*].

{{CONTROL|IR-9.2}}

IR-9 (3) CONTROL ENHANCEMENT (M) (H)

The organization implements [*Assignment: organization-defined procedures*] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

{{CONTROL|IR-9.3}}

IR-9 (4) CONTROL ENHANCEMENT (M) (H)

The organization employs [*Assignment: organization-defined security safeguards*] for personnel exposed to information not within assigned access authorizations.

{{CONTROL|IR-9.4}}

13.9. Maintenance (MA)

MA-1 System Maintenance Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

(b) Reviews and updates the current:

(1) System maintenance policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) System maintenance procedures [*FedRAMP Assignment: at least annually*].

MA-1	Control Summary Information
Responsible Role: Fraser, Doug	
ma-01_odp.01:	
ma-01_odp.02:	
ma-01_odp.03:	
ma-01_odp.04:	
ma-01_odp.05:	
ma-01_odp.06:	
ma-01_odp.07:	
ma-01_odp.08:	
Parameter MA-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

MA-1 What is the solution and how is it implemented?	
Part a	This control is reviewed annually by the ISSO and SO. Part a: & **2 Twelve Solutions Responsibility:** 2 Twelve Solutions ORE Information Security Policy directs the activities within the Maintenance Control Family. The policy addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements for this family of controls. ORE Maintenance Policies and Procedures are derived from the requirements set forth initially by NIST 800-53 control tailored to the ORE. Maintenance policies and procedures apply to all systems and devices within the 2 Twelve Solutions ORE boundary including system users, groups, services, protocols, and functions. All ORE procedures that are captured in Thanos document management system, 2 Twelve Solutions' document repository management system, are reviewed on an annual basis by the document owner and the ORE& Architecture Review Board (ARB). The ARB consists of the& Operations, Engineering, and ORE Leadership teams. The ARB is responsible for notifying stakeholders when changes are made and approved by the ARB. This may require the creation of new documentation or reviewing and updating current procedures, annually or as needed; and policies every 3 years or as needed. & The Operations and Engineering team are responsible for reviewing the document on an annual basis. The team composition includes the following: • Engineering; • Operations; and • ORE Leadership; Part b: **2 Twelve Solutions Responsibility:** ORE policies are reviewed and updated at least every three years by the& Engineering team to ensure the accurate depiction of the content within the ORE environment. The Engineering team updates the procedure at least annually or when required due to major changes in the environment. The ARB is responsible for reviewing and approving all changes made to the ORE system.
Part a1	
Part a1a	

Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

MA-2 Controlled Maintenance (L) (M) (H)

The organization:

(a) Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

(b) Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

(c) Requires that [*Assignment: organization-defined personnel or roles*] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

(d) Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

(e) Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

(f) Includes *[Assignment: organization-defined maintenance-related information*] in organizational maintenance records.

MA-2	Control Summary Information
Responsible Role: Fraser, Doug	
ma-02_odp.01:	
ma-02_odp.02:	
ma-02_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MA-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	

MA-3 Maintenance Tools (M) (H)

The organization approves, controls, and monitors information system maintenance tools.

MA-3	Control Summary Information
Responsible Role: Fraser, Doug	
ma-03_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MA-3 What is the solution and how is it implemented?	
Part a	
Part b	

MA-3 (1) CONTROL ENHANCEMENT (M) (H)

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

MA-3 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MA-3 (1) What is the solution and how is it implemented?

MA-3 (2) CONTROL ENHANCEMENT (M) (H)

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

MA-3 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MA-3 (2) What is the solution and how is it implemented?

MA-3 (3) CONTROL ENHANCEMENT (M) (H)

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

(a) Verifying that there is no organizational information contained on the equipment;

(b) Sanitizing or destroying the equipment;

(c) Retaining the equipment within the facility; or

(d) Obtaining an exemption from [*FedRAMP Assignment: the information owner explicitly authorizes removal of the equipment from the facility*].

MA-3 (3)	Control Summary Information
Responsible Role: Fraser, Doug	
ma-03.03_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MA-3 (3) What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	

MA-4 Remote Maintenance (L) (M) (H)

The organization:

(a) Approves and monitors nonlocal maintenance and diagnostic activities;

(b) Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

(c) Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

(d) Maintains records for nonlocal maintenance and diagnostic activities; and

(e) Terminates session and network connections when nonlocal maintenance is completed.

MA-4	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MA-4 What is the solution and how is it implemented?

Part a	This control is reviewed annually by the ISSO and SO. Part a: & **2 Twelve Solutions Responsibility:** 2 Twelve Solutions ORE Architecture Review Board (ARB) is responsible for approving nonlocal maintenance and diagnostics activities. Standard scheduled maintenance of patching and updates are preapproved by the ARB. Remote maintenance activities are accomplished through automation and stored in Gitlab. All automation changes are tracked within Gitlab to ensure all change history, problems, contracts, and other asset related information is tracked well. Operations also have the option to roll back changes through the history of automation updates. Before deployment into the production instances, nonlocal maintenance activities are required to be tested, scheduled, and analyzed for potential security impacts. The Operations team is responsible for monitoring nonlocal maintenance and diagnostic activities. Part b: **2 Twelve Solutions Responsibility:** 2 Twelve Solutions ORE leverages the use of automation as its centralized tool for deploying patches and updates to the ORE environment. The use of automation is documented, tracked, and maintained within Gitlab. Updates of automation codes are reviewed and must be approved by multiple personnel. Part c: **2 Twelve Solutions Responsibility:** Authorized 2 Twelve Solutions administrators conducting maintenance activities must authenticate through the bastion host. 2 Twelve Solutions& Operations and Engineering teams are considered privileged users in ORE and access the operating system through a bastion host. The bastion host itself has a whitelist of IP ranges that allows connection to be established. All users must have a valid SSH key. After authentication through the bastion host, users must have a matching public SSH key on the operating system to establish a connection with that host. Connections are enforced through whitelisting by Firewall rules. Creation, modification, and deletion of security groups must go through the defined CM process and requested through Agile system for ARB approval. Part d:

	<u>2 Twelve Solutions Responsibility:</u> As indicated in the Change Management Policies and Procedures, changes made to the 2 Twelve Solutions ORE environment are approved before implementation can occur. This sequence is captured as part of the standard 2 Twelve Solutions& configuration management process and is tracked in 2 Twelve Solutions' Agile system ticketing system. Part e: **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions admins are to disconnect at the end of the maintenance window and at the end of the day. In addition, authorized remote access to 2 Twelve Solutions& infrastructure is only accessible after successful authentication through the bastion host. For inactive connections, session termination is automatically configured to drop& after 15 minutes of inactivity. To resume work after the session expires, a remote user must log in again to restart the session and to re-establish communication through the bastion host.
Part b	
Part c	
Part d	
Part e	

MA-4 (2) CONTROL ENHANCEMENT (M) (H)

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

{{CONTROL|MA-4.2}}

MA-5 Maintenance Personnel (L) (M) (H)

The organization:

(a) Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

(b) Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and

(c) Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

MA-5	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MA-5 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	

MA-5 (1) CONTROL ENHANCEMENT (L) (M)

The organization:

(a) Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

(1) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;

(2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

(b) Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

MA-5 (1) Additional FedRAMP Requirements and Guidance:

Requirement: Only MA-5 (1) (a) (1) is required by FedRAMP

{{CONTROL|MA-5.1}}

MA-6 Timely Maintenance (M) (H)

The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined information system components*] within [*Assignment: organization-defined time period*] of failure.

MA-6	Control Summary Information
Responsible Role: Fraser, Doug	
ma-06_odp.01:	
ma-06_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MA-6 What is the solution and how is it implemented?

13.10. Media Protection (MP)

MP-1 Media Protection Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and

(b) Reviews and updates the current:

(1) Media protection policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Media protection procedures [*FedRAMP Assignment: at least annually*].

MP-1	Control Summary Information
Responsible Role: Fraser, Doug	
mp-01_odp.01:	
mp-01_odp.02:	
mp-01_odp.03:	
mp-01_odp.04:	
mp-01_odp.05:	
mp-01_odp.06:	
mp-01_odp.07:	
mp-01_odp.08:	
Parameter MP-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

MP-1 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

MP-2 Media Access (L) (M)

The organization restricts access to [*Assignment: organization-defined types of digital and/or non-digital media*] to [*Assignment: organization-defined personnel or roles*].

MP-2	Control Summary Information
Responsible Role: Fraser, Doug	
mp-02_odp.01:	
mp-02_odp.02:	
mp-02_odp.03:	
mp-02_odp.04:	
Parameter MP-2-1):	
Parameter MP-2-2):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MP-2 What is the solution and how is it implemented?

MP-3 Media Labeling (M) (H)

The organization:

(a) Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

(b) Exempts [*FedRAMP Assignment: no removable media types*] from marking as long as the media remain within [*Assignment: organization-defined controlled areas*].

MP-3(b) Additional FedRAMP Requirements and Guidance:

Guidance: Second parameter in MP-3(b)-2 is not applicable.

MP-3	Control Summary Information
Responsible Role: Fraser, Doug	
mp-03_odp.01:	
mp-03_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MP-3 What is the solution and how is it implemented?	
Part a	
Part b	

MP-4 Media Storage (M) (H)

The organization:

(a) Physically controls and securely stores [*FedRAMP Assignment: [all types of digital and non-digital media with sensitive information*]] within [*FedRAMP Assignment: see additional FedRAMP requirements and guidance*]; and

MP-4a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines controlled areas within facilities where the information and information system reside.

(b) Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

This document details the System Security Plan (SSP) for the Orchestrated Repository for the Enterprise (ORE) security controls. This System Security Plan was written in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Revision 1, Guide for Developing Security Plans for Information Technology Systems.&nbsp; Completion of this SSP, which describes how U.S. federal information will be safeguarded, is a requirement of the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, the Computer Security Act of 1987., 02/18/2023 18:00:00

MP-4	Control Summary Information
Responsible Role: Fraser, Doug	
mp-04_odp.01:	
mp-04_odp.02:	
mp-04_odp.03:	
mp-04_odp.04:	
mp-04_odp.05:	
mp-04_odp.06:	
Parameter MP-4(a)-1):	
Parameter MP-4(a)-2):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MP-4 What is the solution and how is it implemented?	
Part a	
Part b	

MP-5 Media Transport (M) (H)

The organization:

(a) Protects and controls [*FedRAMP Assignment: all media with sensitive information*] during transport outside of controlled areas using [*FedRAMP Assignment: for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secured in locked container*];

MP-5a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB/AO.

(b) Maintains accountability for information system media during transport outside of controlled areas;

(c) Documents activities associated with the transport of information system media; and

(d) Restricts the activities associated with transport of information system media to authorized personnel.

MP-5	Control Summary Information
Responsible Role: Fraser, Doug	
mp-05_odp.01:	
mp-05_odp.02:	
mp-05_odp.03:	
Parameter MP-5(a)-2):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MP-5 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	

MP-5 (4) CONTROL ENHANCEMENT (M) (H)

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

{{CONTROL|MP-5.4}}

MP-6 Media Sanitization and Disposal (L) (M)

The organization:

(a) Sanitizes [*Assignment: organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and

(b) Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

MP-6	Control Summary Information
Responsible Role: Fraser, Doug	
mp-06_odp.01:	
mp-06_odp.02:	
mp-06_odp.03:	
mp-06_odp.04:	
mp-06_odp.05:	
mp-06_odp.06:	
Parameter MP-6(a)-1):	
Parameter MP-6(a)-2):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MP-6 What is the solution and how is it implemented?	
Part a	
Part b	

MP-6 (2) CONTROL ENHANCEMENT (M)

The organization tests sanitization equipment and procedures [*FedRAMP Assignment: at least annually*] to verify that the intended sanitization is being achieved.

MP-6 (2) Additional FedRAMP Requirements and Guidance:

Guidance: Equipment and procedures may be tested or evaluated for effectiveness.

{{CONTROL|MP-6.2}}

MP-7 Media Use (L) (M) (H)

The organization [*Selection: restricts; prohibits*] the use of [*Assignment: organization-defined types of information system media*] on [*Assignment: organization-defined information systems or system components*] using [*Assignment: organization-defined security safeguards*].

MP-7	Control Summary Information
Responsible Role: Fraser, Doug	
mp-07_odp.01:	
mp-07_odp.02:	
mp-07_odp.03:	
mp-07_odp.04:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

MP-7 What is the solution and how is it implemented?	
Part a	
Part b	

MP-7 (1) CONTROL ENHANCEMENT (M) (H)

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

{{CONTROL|MP-7.1}}

13.11. Physical and Environmental Protection (PE)

PE-1 Physical and Environmental Protection Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and

(b) Reviews and updates the current:

(1) Physical and environmental protection policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Physical and environmental protection procedures [*FedRAMP Assignment: at least annually*].

PE-1	Control Summary Information
Responsible Role: Tong, Thanh	
pe-01_odp.01:	
pe-01_odp.02:	
pe-01_odp.03:	
pe-01_odp.04:	
pe-01_odp.05:	
pe-01_odp.06:	
pe-01_odp.07:	
pe-01_odp.08:	
Parameter PE-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

PE-1 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

PE-2 Physical Access Authorizations (L) (M)

The organization:

(a) Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

(b) Issues authorization credentials for facility access;

(c) Reviews the access list detailing authorized facility access by individuals [*FedRAMP Assignment: at least annually*]; and

(d) Removes individuals from the facility access list when access is no longer required.

PE-2	Control Summary Information
Responsible Role: Tong, Thanh	
pe-02_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	

PE-3 Physical Access Control (L) (M) (H)

The organization:

(a) Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] by:

(1) Verifying individual access authorizations before granting access to the facility; and

(2) Controlling ingress/egress to the facility using [*FedRAMP Assignment: CSP defined physical access control systems/devices AND guards*];

(b) Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*];

(c) Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible;

(d) Escorts visitors and monitors visitor activity [*FedRAMP Assignment: in all circumstances within restricted access area where the information system resides*];

(e) Secures keys, combinations, and other physical access devices;

(f) Inventories [*Assignment: organization-defined physical access devices*] every [*FedRAMP Assignment: at least annually*]; and

(g) Changes combinations and keys [*FedRAMP Assignment: at least annually*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

PE-3	Control Summary Information
Responsible Role: Tong, Thanh	
pe-03_odp.01:	
pe-03_odp.02:	
pe-03_odp.03:	
pe-03_odp.04:	
pe-03_odp.05:	
pe-03_odp.06:	
pe-03_odp.07:	
pe-03_odp.08:	
pe-03_odp.09:	
pe-03_odp.10:	
Parameter PE-3(h)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-3 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a2	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	

PE-4 Access Control for Transmission Medium (M) (H)

The organization controls physical access to [*Assignment: organization-defined information system distribution and transmission lines*] within organizational facilities using [*Assignment: organization-defined security safeguards*].

PE-4	Control Summary Information
Responsible Role: Tong, Thanh	
pe-04_odp.01:	
pe-04_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-4 What is the solution and how is it implemented?

PE-5 Access Control for Output Devices (M) (H)

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

PE-5	Control Summary Information
Responsible Role: Tong, Thanh	
pe-05_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-5 What is the solution and how is it implemented?

PE-6 Monitoring Physical Access (L) (M) (H)

The organization:

(a) Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;

(b) Reviews physical access logs [*FedRAMP Assignment: at least monthly*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]; and

(c) Coordinates results of reviews and investigations with the organization's incident response capability.

PE-6	Control Summary Information
Responsible Role: Tong, Thanh	
pe-06_odp.01:	
pe-06_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-6 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	

PE-6 (1) CONTROL ENHANCEMENT (M) (H)

The organization monitors physical intrusion alarms and surveillance equipment.

PE-6 (1)	Control Summary Information
Responsible Role: Tong, Thanh	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-6 (1) What is the solution and how is it implemented?

PE-8 Visitor Access Records (L) (M) (H)

The organization:

(a) Maintains visitor access records to the facility where the information system resides for [*FedRAMP Assignment: for a minimum of one (1) year*]; and

(b) Reviews visitor access records [*FedRAMP Assignment: at least monthly*]

PE-8	Control Summary Information
Responsible Role: Tong, Thanh	
pe-08_odp.01:	
pe-08_odp.02:	
pe-08_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-8 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	

PE-9 Power Equipment and Cabling (M) (H)

The organization protects power equipment and power cabling for the information system from damage and destruction.

PE-9	Control Summary Information
Responsible Role: Tong, Thanh	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-9 What is the solution and how is it implemented?

PE-10 Emergency Shutoff (M) (H)

The organization:

(a) Provides the capability of shutting off power to the information system or individual system components in emergency situations;

(b) Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and

(c) Protects emergency power shutoff capability from unauthorized activation.

PE-10	Control Summary Information
Responsible Role: Tong, Thanh	
pe-10_odp.01:	
pe-10_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-10 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	

PE-11 Emergency Power (M) (H)

The organization provides a short-term uninterruptible power supply to facilitate [*Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power*] in the event of a primary power source loss.

PE-11	Control Summary Information
Responsible Role: Tong, Thanh	
pe-11_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-11 What is the solution and how is it implemented?

PE-12 Emergency Lighting (L) (M) (H)

The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

PE-12	Control Summary Information
Responsible Role: Tong, Thanh	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-12 What is the solution and how is it implemented?

PE-13 Fire Protection (L) (M) (H)

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

PE-13	Control Summary Information
Responsible Role: Tong, Thanh	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-13 What is the solution and how is it implemented?

PE-13 (2) CONTROL ENHANCEMENT (M) (H)

The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation [*Assignment: organization-defined personnel or roles*] and [*Assignment: organization-defined emergency responders*].

PE-13 (2)	Control Summary Information
Responsible Role: Tong, Thanh	
pe-13.02_odp.01:	
pe-13.02_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-13 (2) What is the solution and how is it implemented?	
Part a	
Part b	

PE-13 (3) CONTROL ENHANCEMENT (M) (H)

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

{{CONTROL|PE-13.3}}

PE-14 Temperature and Humidity Controls (L) (M) (H)

The organization:

(a) Maintains temperature and humidity levels within the facility where the information system resides at [*FedRAMP Assignment: consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled "Thermal Guidelines for Data Processing Environments*]; and

PE-14 (a) Additional FedRAMP Requirements and Guidance:
Requirement: *The service provider measures temperature at server inlets and humidity levels by dew point*.

(b) Monitors temperature and humidity levels [*FedRAMP Assignment: continuously*].

PE-14	Control Summary Information
Responsible Role: Tong, Thanh	
pe-14_odp.01:	
pe-14_odp.02:	
pe-14_odp.03:	
pe-14_odp.04:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-14 What is the solution and how is it implemented?	
Part a	
Part b	

PE-14 (2) CONTROL ENHANCEMENT (M) (H)

The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

{{CONTROL|PE-14.2}}

PE-15 Water Damage Protection (L) (M) (H)

The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

PE-15	Control Summary Information
Responsible Role: Tong, Thanh	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-15 What is the solution and how is it implemented?

PE-16 Delivery and Removal (L) (M) (H)

The organization authorizes, monitors, and controls [*FedRAMP Assignment: all information system components*] entering and exiting the facility and maintains records of those items.

PE-16	Control Summary Information
Responsible Role: Tong, Thanh	
pe-16_odp.01:	
pe-16_odp.02:	
Parameter PE-16):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-16 What is the solution and how is it implemented?	
Part a	
Part b	

PE-17 Alternate Work Site (M) (H)

The organization:

(a) Employs [*Assignment: organization-defined security controls*] at alternate work sites*;*

(b) Assesses as feasible, the effectiveness of security controls at alternate work sites; and

(c) Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

PE-17	Control Summary Information
Responsible Role: Fraser, Doug	
pe-17_odp.01:	
pe-17_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PE-17 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	

13.12. Planning (PL)

PL-1 Security Planning Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and

(b) Reviews and updates the current:

(1) Security planning policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Security planning procedures [*FedRAMP Assignment: at least annually*].

PL-1	Control Summary Information
Responsible Role: Fraser, Doug	
pl-01_odp.01:	
pl-01_odp.02:	
pl-01_odp.03:	
pl-01_odp.04:	
pl-01_odp.05:	
pl-01_odp.06:	
pl-01_odp.07:	
pl-01_odp.08:	
Parameter PL-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

PL-1 What is the solution and how is it implemented?	
Part a	This control is reviewed annually by the ISSO and SO. Part a: & **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions Security Planning Policies and Procedures have been developed to establish security planning within the ORE environment. 2 Twelve Solutions's security policies and procedures are derived by the requirements set forth initially by NIST 800-53 control tailored to the ORE defined parameters. The plan addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements to meet the control implementation requirements for the security planning control family of a moderate baseline. The plan specifically addresses policies and procedures related to: • The System Security Plan • Rules of Behavior • Information Security Architecture 2 Twelve Solutions security planning policies and procedures applies to all systems and devices within the Orchestrated Repository for the Enterprise (ORE) information system boundary including system users, groups, services, protocols and functions. All ORE procedures that are captured in Thanos document management system, 2 Twelve Solutions's document repository management system, are reviewed on an annual basis by the document owner and the ORE& Architecture Review Board (ARB). The ARB consists of the Engineering, ORE Leadership and Operations team. This may require the creation of new documentation or reviewing and updating current procedures, annually or as needed; and policies every 3 years or as Needed. The Operations and Engineering team are responsible for reading the document on an annual basis. The team composition includes the following: • Engineering; • Operations; and • ORE Leadership; Part b: **<u>2 Twelve Solutions Responsibility:</u>** ORE Security Planning policies are reviewed and updated at least every three years by the Engineering team. The Engineering team updates the procedure at least annually& or when there is a significant change to the system. The ORE Leadership team reviews and approves all changes.
Part a1	

Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

PL-2 System Security Plan (L) (M) (H)

The organization:

(a) Develops a security plan for the information system that:

(1) Is consistent with the organization’s enterprise architecture;
(2) Explicitly defines the authorization boundary for the system;
(3) Describes the operational context of the information system in terms of missions and business processes;
(4) Provides the security categorization of the information system including supporting rationale;
(5) Describes the operational environment for the information system and relationships with or connections to other information;
(6) Provides an overview of the security requirements for the system;
(7) Identifies any relevant overlays, if applicable;
(8) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
(9) Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

(b) Distributes copies of the security plan and communicates subsequent changes to the plan to [*Assignment: organization-defined personnel or roles*];

(c) Reviews the security plan for the information system [*FedRAMP Assignment: at least annually*];

(d) Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

(e) Protects the security plan from unauthorized disclosure and modification.

PL-2	Control Summary Information
Responsible Role: Fraser, Doug	
pl-02_odp.01:	
pl-02_odp.02:	
pl-02_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PL-2 What is the solution and how is it implemented?

Part a	This control is reviewed annually by the ISSO and SO. Part a: & **<u>2 Twelve Solutions Responsibility:</u>** ORE System Security Plan (SSP) has been developed and is maintained in accordance with NIST SP 800-53 Rev 5 to ensure moderate controls are implemented and documented to protect the confidentiality, integrity and availability of the ORE system and its data. 2 Twelve Solutions has developed the SSP in accordance with NIST 800-18 rev1 Guide for developing Federal Information System Security Plans. 2 Twelve Solutions ORE SSP encompasses the applicable management, operational, and technical security controls which commensurate with FIPS 199 security categorization. 2 Twelve Solutions ORE SSP aligns with enterprise architecture of the application. It defines the authorization boundary of the system in a diagram shown in Fig 9-1 of the SSP. 2 Twelve Solutions has created an operational system for information system where customers can store, track data, create reports, and use workflows to validate data. Customers within the ORE platform can build a data governance management system that includes but is not limited to: user management, privilege management, workflows, and data stewardship. ORE has been designed with controls in place to meet the requirements mandated by NIST SP 800-53 Rev5 controls.& Proper updates to 2 Twelve Solutions SSP fall under a strict command structure to ensure that governance remains accurate and so does the disposition of ORE. ORE SSP is reviewed by the authorizing official prior to plan implementation. & **<u>Customers Responsibility:</u>** Customers are responsible for developing a security plan for the information system that: • Is consistent with the organization's architecture: • Explicitly defines the authorization boundary for the system; • Describes the operational context of the information system in terms of mission and business processes; • Provides the security categorization of the information system including supporting rationale; • Describe the operational environment for the information system and its relationship with or connections to other information; • Provides an overview of the security requirements for the system; • Identifies any relevant overlays, if applicable; • Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and Is reviewed and approved by the authorizing official or designated representative prior to plan implementation. Part b:

	<u>2 Twelve Solutions Responsibility:</u> Copies of ORE SSP are distributed by the Engineering team to personnel who are responsible for the operations, maintenance, and security of the ORE system. Roles of personnel include: • Operations • ORE Leadership (SVP, System Owner, VP, CISO, and VP) • Legal/CPO & **<u>Customer Responsibility</u>** Customers are responsible to distribute copies of the security plan and communicate subsequent changes to the plan The Authorizing Official is responsible for reviewing and approving the SSP within the ORE environment. Part c: **<u>2 Twelve Solutions Responsibility:</u>** ORE SSP for the information system is reviewed at least annually or whenever there is a significant change to the system. Part d: **<u>2 Twelve Solutions Responsibility:</u>** Updates to 2 Twelve Solutions SSP address service changes, (e.g. New software rollouts) follow Change Management Procedure to ensure continued availability and integrity. 2 Twelve Solutions SSP updates are documented in the revision history of the document and applicable personnel are notified through email whenever the SSP has been revised. The SSP is reviewed and updated at least annually to address significant problems and risks reported as part of the security controls assessments or whenever major changes take place in the system. & **<u>Customers Responsibility:</u>** Customers are responsible to update the plan to address changes to the information system/environment of operation or problems identified during implementation or security control assessments. Part e: **<u>2 Twelve Solutions Responsibility:</u>** The ORE SSP is posted on the 2 Twelve Solutions Thanos document management system repository and is

	only accessible to authorized personnel within. Default access to the repository is read-only to prevent unauthorized disclosure and modification. Updates made to the SSP are recorded in the document revision history within the SSP that includes date, description, version, and author to keep track of changes made to the system. & **Customers Responsibility:** Customers are responsible to protect the security plan from unauthorized disclosure and modification.
Part a1	
Part a2	
Part a3	
Part a4	
Part a5	
Part a6	
Part a7	
Part a8	
Part a9	
Part a10	
Part a11	
Part a12	
Part a13	
Part a14	
Part a15	
Part b	
Part c	
Part d	
Part e	

PL-2 (3) CONTROL ENHANCEMENT (M) (H)

The organization plans and coordinates security-related activities affecting the information system with [*Assignment: organization-defined individuals or groups*] before conducting such activities in order to reduce the impact on other organizational entities.

{{CONTROL|PL-2.3}}

PL-4 Rules of Behavior (L) (M)

The organization:

(a) Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;

(b) Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;

(c) Reviews and updates the rules of behavior [*FedRAMP Assignment: at least every three (3) years*]; and

(d) Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

PL-4	Control Summary Information
Responsible Role: Fraser, Doug	
pl-04_odp.01:	
pl-04_odp.02:	
pl-04_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PL-4 What is the solution and how is it implemented?

Part a	This control is reviewed annually by the ISSO and SO. Part a: & **2 Twelve Solutions Responsibility:** 2 Twelve Solutions has established Rules of Behavior for personnel who have access to the ORE environment. ORE Rules of Behavior dictate the acceptable behavior of both internal and external users while utilizing the ORE environment. It describes security controls associated with personnel responsibilities and certain behavior for following security policies, standards, and procedures.& & **Customers Responsibility:** Customers are responsible to establish and making readily available to individuals requiring access to the ORE application rules that describe their responsibilities and expected behavior with regard to information and information system usage. Part b: **2 Twelve Solutions Responsibility:** 2 Twelve Solutions does not authorize personnel access to information and information systems until the Rules of Behavior have been read and signed by the user. Rules of Behavior signed by personnel may be on paper or electronically. Signed Rules of Behavior are retained for record purposes by the Engineering team. & **Customers Responsibility:** Customers are responsible to receive a signed acknowledgment from individuals, indicating that they have read, understand, and agreed to abide by the rules of behavior, before authorizing access to information and the ORE application. Part c: **2 Twelve Solutions Responsibility:** & All ORE procedures that are captured in Thanos document management system, 2 Twelve Solutions' document repository management system, are reviewed annually or after any updates by the document owner and the ORE& Architecture Review Board (ARB). The ARB consists of the Engineering and Operations teams. & & **Customers Responsibility:**

	Customers are responsible to review and update the rules of behavior at least every three (3) years. Part d: **2 Twelve Solutions Responsibility:** Personnel within the ORE environment who have already signed a previous version of the Rules of Behavior, are required to read and re-sign following updates and changes. ORE personnel receive an email notification requesting to read and re-sign, acknowledging they have read and understood the requirements. A physical signature or electronic signature is used to capture user acknowledgment. & **Customers Responsibility:** Customers are responsible to require individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised or updated.
Part b	
Part c	
Part d	
Part b	

PL-4 (1) CONTROL ENHANCEMENT (M) (H)

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

PL-4 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PL-4 (1) What is the solution and how is it implemented?	
Part a	This control is reviewed annually by the ISSO and SO. & **2 Twelve Solutions Responsibility:** Rules of Behavior within 2 Twelve Solutions ORE environment includes explicit restrictions on the use of social media/media networking sites and posting of 2 Twelve Solutions information on public websites. The Rules of Behavior provides guidance on how: • Personnel should participate on social media sites using their own personal social media accounts and be transparent if discussing official 2 Twelve Solutions business. • Personnel should not post any business-related confidential or internal-use-only information obtained as part of your duties within the ORE environment. • Posting of maliciously false, abusive, threatening, or defamatory content is a violation of 2 Twelve Solutions' policies against discrimination, harassment, or hostility on account of age and race. & **Customers Responsibility:** Customers are responsible to include rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.
Part b	
Part c	

PL-8 Information Security Architecture (M) (H)

The organization:

(a) Develops an information security architecture for the information system that:

(1) Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
(2) Describes how the information security architecture is integrated into and supports the enterprise architecture; and
(3) Describes any information security assumptions about, and dependencies on, external services;

(b) Reviews and updates the information security architecture [*FedRAMP Assignment: at least annually or when a significant change occurs*] to reflect updates in the enterprise architecture; and

PL-8 (b) Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F, on Page F-8.

(c) Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

PL-8	Control Summary Information
Responsible Role: Fraser, Doug	
pl-08_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PL-8 What is the solution and how is it implemented?

Part a	This control is reviewed annually by the ISSO and SO. Part a: & **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions ORE SSP describes the overall philosophy, requirements, and approach with regard to protecting the confidentiality, integrity, and availability of ORE information at the Moderate level, as determined by the FIPS 199 categorization. & & **<u>Customers Responsibility:</u>** Customers are responsible to develop an information security architecture for the information system that: • Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; • Describes how the information security architecture is integrated into and supports the organization and; Describes any information security assumptions about and dependencies on, external services. Part b: **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions ORE Leadership Team is responsible for all reviews and updates to ensure updates are documented as part of the continuous monitoring program. ORE SSP through its control implementation captures the security posture and solution in place for ORE. 2 Twelve Solutions SSP serves as the Information Security Architecture which is updated continuously to accurately reflect the environment. & **<u>Customers Responsibility:</u>** Customers are responsible to review and update the information security architecture at least annually or when a significant change occurs to reflect updates in the enterprise architecture. Part c: **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions ensures that System Security Plan (SSP) changes are reflected in the security plan and organizational procurements/acquisitions. 2 Twelve Solutions follows NIST 800-37 Rev. 1 “Guide for Applying the Risk Management Framework to Federal Information Systems” which includes conducting

	annual risk assessments for its information systems and infrastructure. Any changes are then updated into the SSP, Plan of Actions and Milestones (POA&Ms), and Security Assessment Reports (SAR). & **Customers Responsibility:** Customers are responsible to ensure that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/ acquisitions.
Part a1	
Part a2	
Part a3	
Part a4	
Part b	
Part c	

13.13. Personnel Security (PS)

PS-1 Personnel Security Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and

(b) Reviews and updates the current:

(1) Personnel security policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Personnel security procedures [*FedRAMP Assignment: at least annually*].

PS-1	Control Summary Information
Responsible Role: Tong, Thanh	
ps-01_odp.01:	
ps-01_odp.02:	
ps-01_odp.03:	
ps-01_odp.04:	
ps-01_odp.05:	
ps-01_odp.06:	
ps-01_odp.07:	
ps-01_odp.08:	
Parameter PS-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

PS-1 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

PS-2 Position Categorization (L) (M)

The organization:

(a) Assigns a risk designation to all positions;

(b) Establishes screening criteria for individuals filling those positions; and

(c) Reviews and revises position risk designations [*FedRAMP Assignment: at least every three (3) years*].

PS-2	Control Summary Information
Responsible Role: Tong, Thanh	
ps-02_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PS-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	

PS-3 Personnel Screening (L) (M) (H)

The organization:

(a) Screens individuals prior to authorizing access to the information system; and

(b) Rescreens individuals according to [*FedRAMP Assignment: For national security clearances; a reinvestigation is required during the fifth (5th) year for top secret security clearance, the tenth (10th) year for secret security clearance, and fifteenth (15th) year for confidential* *security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the fifth (5th) year. There is no reinvestigation for other moderate risk positions or any low risk positions*].

PS-3	Control Summary Information
Responsible Role: Tong, Thanh	
ps-03_odp.01:	
ps-03_odp.02:	
Parameter PS-3(b)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PS-3 What is the solution and how is it implemented?	
Part a	
Part b	

PS-3 (3) CONTROL ENHANCEMENT (M) (H)

The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

(a) Have valid access authorizations that are demonstrated by assigned official government duties; and

(b) Satisfy [*FedRAMP Assignment: personnel screening criteria – as required by specific information*].

{{CONTROL|PS-3.3}}

PS-4 Personnel Termination (L) (M)

The organization, upon termination of individual employment:

(a) Disables information system access within [*FedRAMP Assignment: same day*];

(b) Terminates/revokes any authenticators/credentials associated with the individual;

(c) Conducts exit interviews that include a discussion of [*Assignment: organization-defined information security topics*];

(d) Retrieves all security-related organizational information system-related property;

(e) Retains access to organizational information and information systems formerly controlled by terminated individual; and

(f) Notifies [*Assignment: organization-defined personnel or roles]* within [*Assignment: organization-defined time period*].

PS-4	Control Summary Information
Responsible Role: Tong, Thanh	
ps-04_odp.01:	
ps-04_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PS-4 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	

PS-5 Personnel Transfer (L) (M)

The organization:

(a) Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

(b) Initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*];

(c) Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

(d) Notifies [*Assignment: organization-defined personnel or roles*] within [*FedRAMP Assignment: within five days of the formal transfer action (DoD 24 hours)*].

PS-5	Control Summary Information
Responsible Role: Tong, Thanh	
ps-05_odp.01:	
ps-05_odp.02:	
ps-05_odp.03:	
ps-05_odp.04:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PS-5 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	

PS-6 Access Agreements (L) (M)

The organization:

(a) Develops and documents access agreements for organizational information systems;

(b) Reviews and updates the access agreements [*FedRAMP Assignment: at least annually*]; and

(c) Ensures that individuals requiring access to organizational information and information systems:

(1) Sign appropriate access agreements prior to being granted access; and
(2) Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [*FedRAMP Assignment: at least annually*].

PS-6	Control Summary Information
Responsible Role: Tong, Thanh	
ps-06_odp.01:	
ps-06_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PS-6 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part c1	
Part c2	

PS-7 Third-Party Personnel Security (L) (M)

The organization:

(a) Establishes personnel security requirements including security roles and responsibilities for third-party providers;

(b) Requires third-party providers to comply with personnel security policies and procedures established by the organization;

(c) Documents personnel security requirements;

(d) Requires third-party providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [*FedRAMP Assignment: same day*]; and

(e) Monitors provider compliance.

PS-7	Control Summary Information
Responsible Role: Tong, Thanh	
ps-07_odp.01:	
ps-07_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PS-7 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	

PS-8 Personnel Sanctions (L) (M)

The organization:

(a) Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and

(b) Notifies [A*ssignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

PS-8	Control Summary Information
Responsible Role: Tong, Thanh	
ps-08_odp.01:	
ps-08_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

PS-8 What is the solution and how is it implemented?	
Part a	
Part b	

13.14. Risk Assessment (RA)

RA-1 Risk Assessment Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

(b) Reviews and updates the current:

(1) Risk assessment policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) Risk assessment procedures [*FedRAMP Assignment: at least annually*].

RA-1	Control Summary Information
Responsible Role: Tong, Thanh	
ra-01_odp.01:	
ra-01_odp.02:	
ra-01_odp.03:	
ra-01_odp.04:	
ra-01_odp.05:	
ra-01_odp.06:	
ra-01_odp.07:	
ra-01_odp.08:	
Parameter RA-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

RA-1 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

RA-2 Security Categorization (L) (M) (H)

The organization:

(a) Categorizes information and the information system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance;

(b) Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

(c) Ensures the security categorization decision is reviewed and approved by the AO or authorizing official designated representative.

RA-2	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

RA-2 What is the solution and how is it implemented?	
Part a	This control is reviewed annually by the ISSO and SO. Part a: & **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions information system is categorized as a Moderate system. 2 Twelve Solutions categorizes information and the information system to protect the confidentiality, integrity, and availability of the information. Categorization of information and information system is outlined within 2 Twelve Solutions SSP and it is based on guidance provided in FIPS 199, and NIST SP 800-60 Rev1. The FIPS 199 worksheet is reviewed at least annually. Part b: **<u>2 Twelve Solutions Responsibility:</u>** The FIPS 199 Security Categorization for the ORE has been conducted and categorized the system as “Moderate”, using the methodology described in NIST 800-60 Rev1 to determine the appropriate confidentiality, integrity, and availability impact levels outlined in section 2 of this SSP. The FIPS 199 worksheet is reviewed at least annually. Part c: **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions ensures the ‘Moderate’ security categorization result decision is approved by the Authorizing Official designated representative annually or when significant changes are made to the ORE system. The FIPS 199 worksheet is reviewed at least annually.
Part b	
Part c	

RA-3 Risk Assessment (L) (M)

The organization:

(a) Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

(b) Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*FedRAMP Assignment: security assessment report*]];

(c) Reviews risk assessment results [*FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs*];

(d) Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and

(e) Updates the risk assessment [*FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

RA-3 Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.

RA-3 (d) Requirement: Include all Authorizing Officials; for JAB authorizations to include FedRAMP.

RA-3	Control Summary Information
Responsible Role: Tong, Thanh	
ra-03_odp.01:	
ra-03_odp.02:	
ra-03_odp.03:	
ra-03_odp.04:	
ra-03_odp.05:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

RA-3 What is the solution and how is it implemented?	
Part a	
Part a1	
Part a2	
Part a3	
Part b	
Part c	
Part d	
Part e	
Part f	

RA-5 Vulnerability Scanning (L) (M) (H)

The organization:

(a) Scans for vulnerabilities in the information system and hosted applications [*FedRAMP Assignment: monthly operating system/infrastructure; monthly web applications and databases*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

RA-5 (a) Additional FedRAMP Requirements and Guidance:

Requirement: An accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.

(b) Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:

(1) Enumerating platforms, software flaws, and improper configurations;
(2) Formatting and making transparent, checklists and test procedures; and
(3) Measuring vulnerability impact;

(c) Analyzes vulnerability scan reports and results from security control assessments

(d) Remediates legitimate vulnerabilities; [*FedRAMP Assignment: high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate risk vulnerabilities* *mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery*], in accordance with an organizational assessment of risk; and

(e) Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

RA-5 (e) Additional FedRAMP Requirements and Guidance:

Requirement: To include all Authorizing Officials; for JAB authorizations to include FedRAMP.

RA-5 Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Vulnerability Scanning Requirements https://www.FedRAMP.gov/documents/

RA-5	Control Summary Information
Responsible Role: Fraser, Doug	
ra-05_odp.01:	
ra-05_odp.02:	
ra-05_odp.03:	
ra-05_odp.04:	
Parameter RA-5(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

RA-5 What is the solution and how is it implemented?

Part a	This control is reviewed annually by the ISSO and SO. Part a:& **<u>2 Twelve Solutions Responsibility:</u>** 2 Twelve Solutions performs vulnerability scanning of the ORE Information System using Semgrep and Trivy. 2 Twelve Solutions follows guidance from NIST SP 800-115 Technical Guide and Information Security Testing and Assessment as the basis for its vulnerability management process. & <u>Application, Operating System: </u>2 Twelve Solutions& utilizes Semgrep and Trivy to conduct vulnerability scans for the ORE application. Web application vulnerability scans are conducted on a weekly basis to identify flaws and validate fixes. Identified weaknesses will be manually verified and mitigated within a defined time period. Part b: **<u>2 Twelve Solutions Responsibility:</u>** ORE configuration settings for all system components within the ORE boundary are all configured through automation.& Gitlab is being leveraged to track all changes to automation and the Agile system ticketing system is employed to ensure they have gone through the necessary process of peer review, security impact analysis, and approval before they have been implemented in ORE. If during operation a scan fails, new vulnerabilities are revealed, and/or if unapproved changes to the automation are discovered they are flagged and reviewed by both the Engineering team and Operations team. Part c: **<u>2 Twelve Solutions Responsibility:</u>** It is the responsibility of the Engineering team to review and analyze findings from vulnerability scan report and results from security control assessment within the ORE environment. This includes: • Existing Vulnerabilities – findings from the SAR are documented and tracked through to POA&M to ensure all items are address. Vulnerability Scan findings from the continuous monitoring process are patched within the same month. Vulnerabilities not patched in the same month are documented and tracked in the POA&M. • False positive- Any findings by the vulnerability scanner that does not actually exist on the asset or application. False positive findings are normally submitted for approval via the deviation request form and shifted to a ‘Closed’ tab of the POA&M once approved by the AO. • Operational Requirement- This requirement is submitted when a weakness is identified

	in a system that cannot be remediated without breaking the current and intended functionality of the system. Operational requirement is submitted for approval via the deviation request form which always remains on the 'Open' tab of the POA&M until remediation, even once approved by the AO. • Risk Adjustment- Some weaknesses identified by the vulnerability scanners do not have a score that reflects the current environment. 2 Twelve Solutions uses a CVSS calculator to identify the correct risk rating and request a risk adjustment deviation. Risk adjustment can be combined with an operational requirement to show mitigating factors around weaknesses that cannot be currently fixed or grant larger development windows for remediation on vulnerabilities that are difficult to patch. Part d: **2 Twelve Solutions Responsibility:** Vulnerabilities are classified by risk and applicability to the ORE authorization boundary. All high-risk vulnerabilities are to be remediated within thirty (30) days, medium-risk vulnerabilities are to be remediated within ninety (90) days, and low-risk vulnerabilities are to be remediated within 180 days. In addition, all verified security flaws will be managed and mitigated via the POA&M process. Remediation is applied and validated within a testing environment before promotion to production instances. All remediated vulnerabilities within the ORE environment shall be validated within the production environment to ensure no unexpected changes or results have occurred during the promotion as well as ensure the vulnerabilities have been fully remediated. Part e: **2 Twelve Solutions Responsibility:** When appropriate, vulnerability scan results are shared with System owner, Engineering, and Operations through the Agile system ticket to prevent similar vulnerabilities in future versions of the ORE application.
Part b	
Part b1	
Part b2	
Part b3	
Part c	
Part d	

Part e	
Part f	

RA-5 (1) CONTROL ENHANCEMENT (M) (H)

The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities to be scanned.

{{CONTROL|RA-5.1}}

RA-5 (2) CONTROL ENHANCEMENT (M) (H)

The organization updates the information system vulnerabilities scanned [*Selection (one or more):* [*FedRAMP Assignment: prior to a new scan*]].

RA-5 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
ra-05.02_odp.01:	
ra-05.02_odp.02:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

RA-5 (2) What is the solution and how is it implemented?
Twelve Solutions follows guidance from NIST SP 800-115 Technical Guide and Information Security Testing and Assessment as the basis for its vulnerability management process. & Application: 2 Twelve Solutions& utilizes Semgrep and Trivy to conduct vulnerability scans for the ORE application. Any vulnerabilities that are found will be remediated in a timely manner. Web application vulnerability scans are conducted on a weekly basis to identify flaws and validate fixes. Identified weaknesses will be manually verified and mitigated within a defined time period.

RA-5 (3) CONTROL ENHANCEMENT (M) (H)

The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

{{CONTROL|RA-5.3}}

RA-5 (5) CONTROL ENHANCEMENT (M) (H)

The organization includes privileged access authorization to [*FedRAMP Assignment: operating systems, databases, web applications*] for selected [*FedRAMP Assignment: all scans*].

RA-5 (5)	Control Summary Information
Responsible Role: Fraser, Doug	
ra-05.05_odp.01:	
ra-05.05_odp.02:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

RA-5 (5) What is the solution and how is it implemented?
This control is reviewed annually by the ISSO and SO & **<u>2 Twelve Solutions Responsibility:</u>** Frequent scanning of the ORE components is critical to ensure the overall risk level of the environment is maintained at an acceptable level.& & <u>Application</u>: Semgrep and Trivy are utilized to conduct vulnerability scans for the ORE application. Any vulnerabilities that are found will be remediated in a timely manner.

RA-5 (6) CONTROL ENHANCEMENT (M) (H)

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

{{CONTROL|RA-5.6}}

RA-5 (8) CONTROL ENHANCEMENT (L) (M) (H)

The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

RA-5 (8) Additional FedRAMP Requirements and Guidance:

Requirement: This enhancement is required for all high vulnerability scan findings.

Guidance: While scanning tools may label findings as high or critical, the intent of the control is based around NIST's definition of high vulnerability.

{{CONTROL|RA-5.8}}

13.15. System and Services Acquisition (SA)

SA-1 System and Services Acquisition Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and

(b) Reviews and updates the current:

(1) System and services acquisition policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) System and services acquisition procedures [*FedRAMP Assignment: at least annually*].

SA-1	Control Summary Information
Responsible Role: Fraser, Doug	
sa-01_odp.01:	
sa-01_odp.02:	
sa-01_odp.03:	
sa-01_odp.04:	
sa-01_odp.05:	
sa-01_odp.06:	
sa-01_odp.07:	
sa-01_odp.08:	
Parameter SA-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

SA-1 What is the solution and how is it implemented?

Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & 2 Twelve Solutions ORE Global Information Security Policy directs the activities within the ORE Life-Cycle Management Plan. The plan addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements to meet the control implementation requirements for the System and Services Acquisition control family of a moderate baseline. The ORE Life-Cycle Management Plan also contains the system and services acquisitions procedures or processes related to: • Life-Cycle Management • ORE Knowledge Management • Initiation Phase • Development Phase • Implementation Phase • Operations/Maintenance Phase • Role-Based Security Personnel Requirements • Disposal Phase • Customer Responsibility Matrix & All ORE procedures that are captured in Thanos document management system, 2 Twelve Solutions's document repository management system, are reviewed on an annual basis by the document owner and the ORE Architecture Review Board (ARB). The ARB consists of the Engineering, Operations, and Leadership teams. The ARB is responsible for notifying stakeholders when changes are made and approved by the ARB. This may require the creation of new documentation or reviewing and updating current procedures, annually or as needed; and policies every 3 years or as needed. & The Operations and Engineering team are responsible for reading the document on an annual basis. The team composition includes the following: • Engineering (Product development and engineering, Product management); • Operations (Operations for Applications, Databases, Services); and • ORE Leadership (System Owner; Product Owner;); & The 2 Twelve Solutions ORE ARB and the ISSO is responsible for reviewing and approving the policies and procedures for the ORE environment.& Once approved, the ISSO will sign the policy and procedure. Part b: ORE policies are reviewed and updated every three years by the ARB. The Engineering team updates the

	procedure annually. The Engineering team is responsible for reviewing and making updates to the System and Services Acquisition procedure annually.
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

SA-2 Allocation of Resources (L) (M) (H)

The organization:

(a) Determines information security requirements for the information system or information system service in mission/business process planning;

(b) Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and

(c) Establishes a discrete line item for information security in organizational programming and budgeting documentation.

SA-2	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SA-2 What is the solution and how is it implemented?

Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Part a: & **2 Twelve Solutions Responsibility**: The Engineering team& has meetings with the ORE leadership team for 2 Twelve Solutions to discuss new services, features, requirements and determine the needs for these functions in regard to security for the next two releases of ORE. The information security requirements are based on the moderate security impact categorization of the information system for the application, database and operating system. & **Customer Responsibility:&** It is the customer responsibility to determines information security requirements for the information system or information system service in mission/business process planning for the ORE application. Part b: **2 Twelve Solutions Responsibility**: On an annual basis a roadmap is created for security by the Engineering team and Opertaions team for the application, database and operating system. During this process the Engineering team and Operations team determines, documents, and allocates the resources required to protect ORE as part of its capital planning and investment control process for the application, database and operating system. & **Customer Responsibility:&** It is the customer responsibility to determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process for the ORE application. Part c: **2 Twelve Solutions Responsibility**: On an annual basis a roadmap is created for security by the Engineering team and Operations team.& Through this process the ORE Leadership team establishes a discrete line item for information security in organizational programming and budgeting documentation.& 2 Twelve Solutions has established separate line items for security software licenses, security tools, security certifications, and security consulting.& & **Customer Responsibility:&**

	It is the customer responsibility to establish a discrete line item for information security in organizational programming and budgeting documentation for the ORE application.
Part b	
Part c	

SA-3 System Development Life Cycle (L) (M) (H)

The organization:

(a) Manages the information system using [*Assignment: organization-defined system development life cycle*] that incorporates information security considerations;

(b) Defines and documents information security roles and responsibilities throughout the system development life cycle;

(c) Identifies individuals having information security roles and responsibilities; and

(d) Integrates the organizational information security risk management process into system development life cycle activities.

SA-3	Control Summary Information
Responsible Role: Fraser, Doug	
sa-03_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SA-3 What is the solution and how is it implemented?

Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Part a: & **2 Twelve Solutions Responsibility**: The Engineering team follows the 2 Twelve Solutions& System Development Lifecycle Plan (SDLC) for all development and acquisitions. The 2 Twelve Solutions ORE Lifecycle Management Plan is developed in accordance to NIST Special Publication 800-37: Initiation, Development/Acquisition, Implementations, Operation/Maintenance, and Disposal. ORE has incorporated these five phases into a governance process to ensure all ORE systems deliver high-quality cloud products and services that meet the expectations of the ORE and its customers and the Federal cloud community.& & All proposed changes to ORE must go through the change management process. The Engineering team is responsible for reviewing proposed changes to ORE. They will either approve or disapprove the changes through the Agile system ticketing procedure with explicit consideration for the security impact analysis during the change management process.& Part b: **2 Twelve Solutions Responsibility**: The ORE Global Information Security Policy and the 2 Twelve Solutions System Development Life Cycle Plan document the security roles and responsibilities throughout the ORE development. All personnel have their status categorized with a sensitivity level in accordance with PS-2.& Personnel (employees or contractors) of service providers are considered Internal Users.& All other users are considered External Users.& User privileges (authorization permission after authentication takes place) are described in Table 9 1 Personnel Roles and Privileges.& Part c: **2 Twelve Solutions Responsibility**: The ORE Global Information Security Policy and the 2 Twelve Solutions System Development Life Cycle Plan document the security roles and responsibilities throughout the ORE development lifecycle. The Engineering team is identified as individuals having information system security roles.& Part d:

	2 Twelve Solutions Responsibility: The Engineering and Operations teams follow the 2 Twelve Solutions System Development Lifecycle Plan (SDLC) for all development and acquisitions. The 2 Twelve Solutions ORE Lifecycle Management Plan is developed in accordance to NIST Special Publication 800-37: Initiation, Development/Acquisition, Implementations, Operation/Maintenance, and Disposal. ORE has incorporated these five phases into a governance process to ensure all ORE systems deliver high quality cloud products and services that meet the expectations of the FedRAMP Program Management Office (PMO), ORE and its customers, and the Federal cloud community.& & All proposed changes to ORE must go through the change management process. The Engineering team is responsible for reviewing proposed changes to ORE. They will either approve or disapprove the changes through the Agile system ticketing procedure with explicit consideration for the security impact analysis during the change management process.& In addition, ORE has implemented a continuous monitoring plan to ensure the total risk level of ORE is at an acceptable level.&
Part b	
Part c	
Part d	

SA-4 Acquisitions Process (L) (M) (H)

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

(a) Security functional requirements;

(b) Security strength requirements;

(c) Security assurance requirements;

(d) Security-related documentation requirements;

(e) Requirements for protecting security-related documentation;

(f) Description of the information system development environment and environment in which the system is intended to operate; and

(g) Acceptance criteria.

SA-4 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider must comply with Federal Acquisition Regulation (FAR) Subpart 7.103, and Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (Pub. L. 115-232), and FAR Subpart 4.21, which implements Section 889 (as well as any added updates related to FISMA to address security concerns in the system acquisitions process).

Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred.
See https://www.niap-ccevs.org/Product/

SA-4	Control Summary Information
Responsible Role: Fraser, Doug	
sa-04_odp.01:	
sa-04_odp.02:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SA-4 What is the solution and how is it implemented?

Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Part a:& **2 Twelve Solutions Responsibility**: ORE leverages the following in their standard contract language for all ORE acquisitions. The Engineering team is responsible for reviewing all contract clauses prior to any acquisitions for the ORE information system.& • FedRAMP Standard Contract Clauses - The clauses cover FedRAMP requirements for areas like the security assessment process and related ongoing assessment and authorization. The template also provides basic security requirements identifying Cloud Service Provider responsibilities for privacy and security, protection of government data, personnel background screening and security deliverables with associated frequencies (https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/03/FedRAMP_Standard_Contractual_Clauses_062712_0.pdf) • FedRAMP Control Specific Contract Clauses – The clauses cover FedRAMP security control baselines specify control parameter requirements and organizational parameters specific ORE' control implementation (https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/03/FedRAMP-Control-Specific-Contract-Clauses-v2.1.docx) • FedRAMP Cloud Procurement Best Practices – leverages guidance in effectively implementing the "Cloud First" policy and adopting the "Federal Cloud Computing Strategy" into ORE' operating model by focusing on ways to more effectively promote cloud services within existing regulations and laws (https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/03/Cloud-Best-Practices.pdf)& • FedRAMP Package Validation Process - outlines the process for 2 Twelve Solutions to enable Federal agencies to validate FedRAMP compliance of for ORE (https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/01/FedRAMP-Package-Validation-Process-FINAL.pdf) & **Customer Responsibility:&** It is the customer responsibility to ensure that all acquisition contracts for the ORE application include security functional requirements. Part b:

2 Twelve Solutions Responsibility:

Security strength requirements for ORE& components are detailed by 2 Twelve Solutions in vendor agreements and the Siglite questionnaire either explicitly or by reference to other documentation to assure that ORE security policies are being followed for all ORE acquisitions. The Engineering team is responsible for reviewing all responses to the Siglite questionnaire and contract clauses prior to any acquisitions for the ORE information system.
&
Major or minor acquisitions are subject to obtain approval through the established change management process. Engineering personnel will review the security requirement of the acquisition and evaluate its bearing during the security impact analysis. The final approval of all acquisitions will come from ARB and the Authorized Officer.
&
Customer Responsibility:&
It is the customer responsibility to ensure that all acquisition contracts for the ORE application include security strength requirements.

Part c:

2 Twelve Solutions Responsibility:

Security assurance requirements for ORE& components are detailed by 2 Twelve Solutions in vendor agreements, the Siglite questionnaire, and NIST Special Publication 800-53 (Rev. 4) requirements either explicitly or by reference to other documentation to assure that ORE security policies are being followed for all ORE acquisitions. The Engineering team is responsible for reviewing all contract clauses prior to any acquisitions for the ORE information system.
&
Major or minor acquisitions are subject to obtain approval through the established change management process. Engineering personnel will review the security requirement of the acquisition and evaluate its bearing during the security impact analysis. The final approval of all acquisitions will come from ARB and the Authorized Officer.
&
Customer Responsibility:&
It is the customer responsibility to ensure that all acquisition contracts for the ORE application include security assurance requirements.

Part d:

2 Twelve Solutions Responsibility:

Security-related documentation requirements for ORE& components are detailed by 2 Twelve Solutions in vendor agreements and the Siglite questionnaire either explicitly or by reference to other documentation to assure that 2 Twelve Solutions& security policies are being followed for all ORE acquisitions. The Engineering team is responsible for reviewing all contract clauses prior to any acquisitions for the ORE information system.
&
Major or minor acquisitions are subject to obtain approval through the established change management process. Engineering personnel will review the security requirement of the acquisition and evaluate its bearing during the security impact analysis. The final approval of all acquisitions will come from ARB and the Authorized Officer.
&
Customer Responsibility:&
It is the customer responsibility to ensure that all acquisition contracts for the ORE application include security-related documentation requirements.

Part e:

This control is reviewed at least annually or as needed by the ISSO and SO.

&
2 Twelve Solutions Responsibility:
Requirements for protecting security-related documentation for 2 Twelve Solutions ORE& components are detailed by 2 Twelve Solutions in vendor agreements either explicitly or by reference to other documentation to assure that 2 Twelve Solutions security policies are being followed for all ORE acquisitions. The Engineering team is responsible for reviewing all contract clauses prior to any acquisitions for the ORE information system.
&
Major or minor acquisitions are subject to obtain approval through the established change management process. Engineering personnel will review the security requirement of the acquisition and evaluate its bearing during the security impact analysis. The final approval of all acquisitions will come from ARB and the Authorized Officer.
&
Customer Responsibility:&
It is the customer responsibility to ensure that all acquisition contracts for the ORE application include requirements for protecting security-related documentation for the ORE application.

Part f:

2 Twelve Solutions Responsibility:

	Description of the system development environment and the operating system environment in which the software, hardware or firmware is intended to operate is included in the FedRAMP Standard Contract Clauses, FedRAMP Control Specific Contract Clauses, and the FedRAMP Cloud Procurement Best Practices& clauses as documented in “part a” above. They are documented explicitly or by reference to other documentation to assure that 2 Twelve Solutions& security policies are being followed for all ORE acquisitions. The Engineering team is responsible for reviewing all contract clauses prior to any acquisitions for the ORE information system. & Major or minor acquisitions are subject to obtain approval through the established change management process. Engineering personnel will review the security requirement of the acquisition and evaluate its bearing during the security impact analysis. The final approval of all acquisitions will come from ARB and the Authorized Officer. & **Customer Responsibility:&** It is the customer responsibility to ensure that all acquisition contracts for the ORE application include a description of the information system development environment and environment in which the system is intended to operate. Part g: **2 Twelve Solutions Responsibility**: Acceptance criteria requirements for ORE& components are detailed by 2 Twelve Solutions in vendor agreements and the Siglite questionnaire either explicitly or by reference to other documentation to assure that& 2 Twelve Solutions security policies are being followed for all ORE acquisitions. The Engineering team is responsible for reviewing all contract clauses prior to any acquisitions for the ORE information system. & Major or minor acquisitions are subject to obtain approval through the established change management process. Engineering personnel will review the security requirement of the acquisition and evaluate its bearing during the security impact analysis. The final approval of all acquisitions will come from ARB and the Authorized Officer. & **Customer Responsibility:&** It is the customer responsibility to ensure that all acquisition contracts for the ORE application include some acceptance criteria, such as Common Criteria (ISO/IEC 15408), for the vendor.
Part b	
Part c	
Part d	

Part e	
Part f	
Part g	
Part h	
Part i	

SA-4 (1) CONTROL ENHANCEMENT (M) (H)

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

SA-4 (1)	**Control Summary Information**
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SA-4 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions, using acquisition documents, requires that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services. The Siglite questionnaire provided to vendors/contractors is used as the foundational resource for this information for the ORE acquisitions. The Engineering team is responsible for reviewing all contract clauses prior to any acquisitions for the ORE information system.

SA-4 (2) CONTROL ENHANCEMENT (L) (M)

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [*FedRAMP Selection (one or more): to include security-relevant external system interfaces, and high-level design*]; [*Assignment: organization-defined design/implementation information*] at [*Assignment: organization-defined level of detail*].

SA-4 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
sa-04.02_odp.01:	
sa-04.02_odp.02:	
sa-04.02_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SA-4 (2) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions requires all vendors/contractors to provide a design and implementation plan for all components and services that are going to be implemented into the ORE environment for the application, database and operating system. The vendor documentation includes security-relevant external system interfaces and high-level design of the proposed component, design drawings or documentation at a high level of detail. 2 Twelve Solutions utilizes their SDLC to determine what the requirements are for acceptance criteria to integrate vendor components into the ORE system. The Siglite questionnaire provided to vendors/contractors is used as the foundational resource for this information.

SA-4 (8) CONTROL ENHANCEMENT (M) (H)

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [*FedRAMP Assignment: at least the minimum requirement as defined in control CA-7*].

SA-4 (8) Additional FedRAMP Requirements and Guidance:

Guidance: CSP must use the same security standards regardless of where the system component or information system service is acquired.

{{CONTROL|SA-4.8}}

SA-4 (9) CONTROL ENHANCEMENT (M) (H)

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

SA-4 (9)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SA-4 (9) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions requires all vendors to provide, early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. The Siglite questionnaire provided to vendors/contractors is used as the foundational resource for this information for all ORE acquisitions. Exceptions or modifications to automation due to acquisitions must be approved through the established change management process.

SA-4 (10) CONTROL ENHANCEMENT (M) (H)

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

SA-4 (10)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SA-4 (10) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE only allows approved PIV cards and CACs. The ORE application is able to authenticate a user with a smart card to an upstream identity provider using the identity protocols SAML 2.0 or Open ID Connect. After authentication, SAML assertions or OIDC tokens will be transmitted from the upstream identity management systems to the ORE system.

SA-5 Information System Documentation (L) (M)

The organization:

(a) Obtains administrator documentation for the information system, system component, or information system service that describes:

(1) Secure configuration, installation, and operation of the system, component, or service;
(2) Effective use and maintenance of security functions/mechanisms; and
(3) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

(b) Obtains user documentation for the information system, system component, or information system service that describes:

(1) User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
(2) Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
(3) User responsibilities in maintaining the security of the system, component, or service;

(c) Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [*Assignment: organization-defined actions*] in response;

(d) Protects documentation as required, in accordance with the risk management strategy; and

(e) Distributes documentation to [*Assignment: organization-defined personnel or roles)*].

SA-5	Control Summary Information
Responsible Role: Fraser, Doug	
sa-05_odp.01:	
sa-05_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SA-5 What is the solution and how is it implemented?

Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Part a:& **2 Twelve Solutions Responsibility**: Security documentation for the ORE application, database, and operating system is maintained in& Thanos document management system& and is available to the Engineering team for review and to make updates. The Engineering team is responsible for reviewing and updating documentation on an annual basis.& Operations team has access to security documentation but they cannot modify them. Vendor documentation, including configuration guidelines for secure installation and operation of the information system and administrator documentation are acquired from vendors for system components, including operating systems, databases, and security tools. Access to the most recent administrator documentation, including configuration, known vulnerabilities, installation, and operation of the system, component, and/or service, is made available to the Engineering team and Operations team and then distributed to Customers.& Part b: **2 Twelve Solutions Responsibility**: 2 Twelve Solutions publishes end user documentation in the form of a general user guide for the ORE application. The general user guide outlines methods for user interaction, use of the system, component, or service in a more secure manner, and user responsibilities in maintaining the security of the system, component, or service. The end user documentation is reviewed by the Engineering team on an annual basis and, if necessary, is updated. General users do not have access to security functions/mechanisms as they relate to the ORE environment. Part c: **2 Twelve Solutions Responsibility**: ORE maintains access to vendor documentation for all components within the ORE& application, database and operating system environments. Should documentation become unavailable, ORE will contact the vendor for the updated documentation or addition support. Part d: **2 Twelve Solutions Responsibility**: Security-related documentation, user manuals, user guides, secure configuration management for the ORE application, database, and operating system are stored and maintained on Thanos document management system. The security-related documentation is accessible to the Engineering team for review

	and to make updates. The Engineering team is responsible for reviewing and updating documentation on an annual basis.& Operations team has access to security documentation but they cannot modify them. & Part e: **<u>2 Twelve Solutions Responsibility</u>**: Documentation for ORE is disseminated to Customers and made available for updates/reviews to the Engineering team and& Operations team through the Thanos document management system repository.& The Engineering team is responsible for reviewing and updating documentation on an annual basis.& Updated documents are notified through email for stakeholders.
Part a1	
Part a2	
Part a3	
Part b	
Part b1	
Part b2	
Part b3	
Part c	
Part d	

SA-8 Security Engineering Principles (M) (H)

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

SA-8	Control Summary Information
Responsible Role: Fraser, Doug	
sa-08_odp.01:	
sa-08_odp.02:	
sa-8_prm_1:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SA-8 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: 2 Twelve Solutions ORE applies information system security engineering principles in the specification, design, development, implementation, and modification of 2 Twelve Solutions ORE Application. The following documentation and implementation supports 2 Twelve Solutions ORE's applied security engineering principles for the 2 Twelve Solutions ORE Application: • <u>System Security Plan</u>: provides the implementation of security engineering principles using the NIST 800-53 security controls for a Moderate security baseline. The SSP addresses security controls for the management, technical and operational aspects of the 2 Twelve Solutions ORE Application. • <u>ORE Configuration and Management Plan</u>: Details how ORE applies configuration management for establishing baselines for tracking, controlling, and managing many aspects of business development and operations ORE System Development Life Cycle Plan: Defines and establishes how 2 Twelve Solutions manages the life cycle of 2 Twelve Solutions ORE systems and provides continuous monitoring as part of the operations phase of the system life cycle. & ORE applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.& The 2 Twelve Solutions& Software Development Lifecycle (SDLC) Plan covers: • Initiation Phase • Development Phase • Implementation Phase • Operations/Maintenance Phase • Disposal Phase & The ORE System Development Life Cycle Plan directs use of security principles in the initiation (Section 6), development (Section 7), implementation (Section 8), operations/ maintenance (Section 9), and disposal (Section 10) phases.& The SDLC is accessible to the Engineering team for review and to make updates. The Engineering team is responsible for reviewing and& updating documentation on an annual basis.& Operations team has access to the SDLC Plan but do not have modify access rights.

SA-9 External Information System Services (L) (M) (H)

The organization:

(a) Requires that providers of external information system services comply with organizational information security requirements and employ [*FedRAMP Assignment: FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

(b) Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

(c) Employs [*FedRAMP Assignment: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored*] to monitor security control compliance by external service providers on an ongoing basis.

Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Continuous Monitoring Strategy Guide https://www.FedRAMP.gov/documents

Guidance: Independent Assessors should assess the risk associated with the use of external services. See the FedRAMP page under Key Cloud Service Provider (CSP) Documents>FedRAMP Authorization Boundary Guidance

SA-9	Control Summary Information
Responsible Role: Fraser, Doug	
sa-09_odp.01:	
sa-09_odp.02:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SA-9 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Part a: & **<u>2 Twelve Solutions Responsibility</u>**: 2 Twelve Solutions requires all third-party vendors/contractors and external information system services to comply with ORE's information security requirements and employ FedRAMP security controls baselines. Risk assessments are conducted for all vendors prior to the initiation of any connection through the use of the Siglite questionnaire. The contractual agreements, ISAs, Siglite questionnaire, and MOUs explicitly define the ports, protocols, interconnections, and information flow with external interconnection systems to maintain a secure system. These agreements are overseen by the Engineering team manager to ensure continual compliance. Part b: **<u>2 Twelve Solutions Responsibility</u>**: 2 Twelve Solutions maintains all contractual agreements, ISAs, MOUs and contact details of service providers. Roles and responsibilities pertaining to FedRAMP system interconnections and services are outlined in contracts. All external information connections and services must be approved by the ARB and AO prior to implementation. Part c: **<u>2 Twelve Solutions Responsibility</u>**: 2 Twelve Solutions monitors and reviews agreements with external parties to ensure all parties are adhering to the terms and conditions signed in the agreement. Where Federal information is processed or stored, 2 Twelve Solutions requires an external vendor or system to obtain FedRAMP Moderate ATO and follow the FedRAMP continuous monitoring requirements.
Part b	
Part c	

SA-9 (1) CONTROL ENHANCEMENT (M) (H)

The organization:

(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and

(b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [*Assignment: organization-defined personnel or roles*].

{{CONTROL|SA-9.1}}

SA-9 (2) CONTROL ENHANCEMENT (M) (H)

The organization requires providers of [*FedRAMP Assignment: All external systems where Federal information is processed or stored*] to identify the functions, ports, protocols, and other services required for the use of such services.

SA-9 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
sa-09.02_odp:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SA-9 (2) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility** Where Federal information is processed or stored, 2 Twelve Solutions requires an external vendor or system to obtain FedRAMP Moderate ATO and follow the FedRAMP continuous monitoring requirements. 2 Twelve Solutions will request the CSP or vendor's SSP which identifies all functions, ports, protocols, and other services required for the use of such services. In addition, 2 Twelve Solutions requires vendors/contractors to complete the Siglite questionnaire requesting for similar information.& The Engineering team is responsible for reviewing all responses to the questionnaire and contract clauses prior to any acquisitions for the ORE information system.

SA-9 (4) CONTROL ENHANCEMENT (M) (H)

The organization employs [*Assignment: organization-defined security safeguards*] to ensure that the interests of [*FedRAMP Assignment: All external systems where Federal information is processed or stored*] are consistent with and reflect organizational interests.

{{CONTROL|SA-9.4}}

SA-9 (5) CONTROL ENHANCEMENT (M) (H)

The organization restricts the location of [*FedRAMP Selection: information processing, information data, AND information services*] to [*Assignment: organization-defined locations*] based on [*Assignment: organization-defined requirements or conditions*].

Additional FedRAMP Requirements and Guidance

Guidance: System services refer to FTP, Telnet, and TFTP, etc.

{{CONTROL|SA-9.5}}

SA-10 Developer Configuration Management (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

(a) Perform configuration management during system, component, or service [*FedRAMP Selection: development, implementation, AND operation*];

(b) Document, manage, and control the integrity of changes to [*Assignment: organization-defined configuration items under configuration management*];

(c) Implement only organization-approved changes to the system, component, or service;

(d) Document approved changes to the system, component, or service and the potential security impacts of such changes; and

(e) Track security flaws and flaw resolution within the system, component, or service and report findings to [*Assignment: organization-defined personnel*].

SA-10 (e) Additional FedRAMP Requirements and Guidance:

Requirement: For JAB authorizations, track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP.

SA-10	Control Summary Information
Responsible Role: Fraser, Doug	
sa-10_odp.01:	
sa-10_odp.02:	
sa-10_odp.03:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SA-10 What is the solution and how is it implemented?

Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Part a:& **<u>2 Twelve Solutions Responsibility</u>** The 2 Twelve Solutions Engineering& team follows the 2 Twelve Solutions System Development Lifecycle Plan (SDLC) for all development and acquisitions. The 2 Twelve Solutions ORE Lifecycle Management Plan is developed in accordance to NIST Special Publication 800-37: Initiation, Development/Acquisition, Implementations, Operation/Maintenance, and Disposal. ORE has incorporated these five phases into a governance process to ensure all ORE systems deliver high-quality cloud products and services that meet the expectations of the ORE and its customers and the Federal cloud community.& & All proposed changes to ORE must go through the change management process. The Engineering team is responsible for reviewing proposed changes to ORE. They will either approve or disapprove the changes through the Agile system ticketing procedure with explicit consideration for the security impact analysis during the change management process.& Part b: **<u>2 Twelve Solutions Responsibility</u>** When a change is being considered it must first be input into a Agile system ticket by all stakeholders. Once the ticket is created the proposed change is then peer reviewed by another member of the Engineering or Operations team (depending on change). The implementer and reviewer is never the same person. Once the ticket is signed through peer review the next step is that it goes to a member of the Engineering team for review and approval. The member of the Engineering team then does a security impact analysis of the proposed change to determine if it will adversely affect the security stature of ORE. If there isn't a risk to the security posture of ORE the member of the Engineering team will then approve the change which will then send the ticket back to the initial engineer. The engineer will then institute the change and close the ticket with all steps captured.& All Agile system tickets related to the change management process are retained indefinitely by 2 Twelve Solutions. & <u>Application and Database</u>: New versions of ORE package may include version upgrade to both ORE Application and database. When a ORE release is created, the installation files have a SHA256 checksum. This checksum is manually verified by the Operations prior to deployment. & <u>Operating System</u>: The Engineering team uses gpg signature checking. The signature check used is called "gpgcheck" and is used to validate the digital signature, "gpgcheck=1" is set to ensure all packages' signatures are checked. In addition, authorized sources and vendor sites are whitelisted for updates and patches.

	Part c: **2 Twelve Solutions Responsibility** Operations team& is the only users that have the ability to implement approved changes to the ORE environment. All changes are executed through the SSH Bastion after the change has been officially approved by the ARB through the change management process. Requests and approved changes are documented and retained through the Agile system ticketing system. Unapproved changes are captured and alerted through the logging system. Part d: **2 Twelve Solutions Responsibility** The Engineering team is responsible for reviewing proposed changes to ORE. They will either approve or disapprove the changes through the Agile system ticketing procedure with explicit consideration for the security impact analysis during the change management process. All Agile system tickets related to the change management process are retained indefinitely by 2 Twelve Solutions. They are responsible for this review and approval process when a new change is requested. Part e: **2 Twelve Solutions Responsibility** Flaws are identified through logging alerts, CI pipeline outputs, internal testing, or customer reports. All endeavors for remediation are the same regardless of the vulnerability source. The ORE vulnerability team tracks the system flaws in Agile system ticketing systems. Vulnerabilities are compiled and reported to the AO in the Plan of Actions and Milestones (POA&M). High-risk vulnerabilities are remediated within thirty days, moderate risk vulnerabilities are mitigated within ninety days and low risk vulnerabilities are mitigated within one hundred and eighty days.
Part b	
Part c	
Part d	
Part e	

SA-10 (1) CONTROL ENHANCEMENT (M) (H)

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

{{CONTROL|SA-10.1}}

SA-11 Developer Security Testing and Evaluation (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

(a) Create and implement a security assessment plan;

(b) Perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation at [*Assignment: organization-defined depth and coverage*];

(c) Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;

(d) Implement a verifiable flaw remediation process; and

(e) Correct flaws identified during security testing/evaluation.

SA-11	Control Summary Information
Responsible Role: Fraser, Doug	
sa-11_odp.01:	
sa-11_odp.02:	
sa-11_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SA-11 What is the solution and how is it implemented?

Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & Part a: **2 Twelve Solutions Responsibility** The Engineering team follows the 2 Twelve Solutions System Development Lifecycle Plan (SDLC) for all development and acquisitions. The 2 Twelve Solutions ORE Lifecycle Management Plan is developed in accordance to NIST Special Publication 800-37: Initiation, Development/Acquisition, Implementations, Operation/Maintenance, and Disposal. ORE has incorporated these five phases into a governance process to ensure all ORE systems deliver high-quality cloud products and services that meet the expectations of the ORE and its customers and the Federal cloud community.& & The Engineering team follows best practices to include peer-to-peer review, static code analysis through Semgrep, unit/integration/system/regression testing, and input validation. ORE source codes are maintained, controlled, and tracked within Gitlab.& Part b: **2 Twelve Solutions Responsibility** The Engineering& team& follows the established change management process and is responsible for doing unit, integration, system, and regression testing for proposed changes to ORE before each new release. Fail results are rerouted back to the engineer to remediate errors. Part c: **2 Twelve Solutions Responsibility** The Engineering& team& follows the established change management process and is responsible for doing unit, integration, system, and regression testing for proposed changes to ORE before each new release. Fail results are rerouted back to the engineer to remediate errors. Part d: **2 Twelve Solutions Responsibility** Identified flaws within the ORE application are verified through additional testing or scanning. Testing results are tracked and documented within Gitlab and Agile. The reviewer (someone other than the Engineer) verifies the testing result and either approves the code or sends it back to the Engineer. &

	Part e: **2 Twelve Solutions Responsibility** The Engineering& team& follows the established change management process and is responsible for doing unit, integration, system, and regression testing for proposed changes to ORE before each new release. Fail results are rerouted back to the engineer to remediate errors. The process continues until code testing does not contain fail results.
Part b	
Part c	
Part d	
Part e	

SA-11 (1) CONTROL ENHANCEMENT (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

SA-11 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

{{CONTROL|SA-11.1}}

SA-11 (2) CONTROL ENHANCEMENT (M) (H)

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

{{CONTROL|SA-11.2}}

SA-11 (8) CONTROL ENHANCEMENT (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

{{CONTROL|SA-11.8}}

13.16. System and Communications Protection (SC)

SC-1 System and Communications Protection Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

(b) Reviews and updates the current:

(1) System and communications protection policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) System and communications protection procedures [*FedRAMP Assignment: at least annually*].

SC-1	Control Summary Information
Responsible Role: Fraser, Doug	
sc-01_odp.01:	
sc-01_odp.02:	
sc-01_odp.03:	
sc-01_odp.04:	
sc-01_odp.05:	
sc-01_odp.06:	
sc-01_odp.07:	
sc-01_odp.08:	
Parameter SC-1(a)):	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

SC-1 What is the solution and how is it implemented?	
Part a	2 Twelve Solutions ORE Information Security Policy directs the activities within the ORE& system and communication controls. The policy addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements to meet the FedRAMP control implementation requirements for this family of controls. & All ORE procedures that are captured in Thanos document management system, 2 Twelve Solutions' document repository management system, are reviewed on an annual basis by the document owner and the ORE Architecture Review Board (ARB). The ARB consists of the Engineering and Operations teams. The ARB is responsible for notifying stakeholders when changes are made and approved by the ARB. This may require the creation of new documentation or reviewing and updating current procedures, annually or as needed; and policies every 3 years or as needed. & The Operations and Engineering team are responsible for reading the document on an annual basis. The team composition includes the following: • Engineering (Product development and engineering, Product management); • Operations (Operations for Applications, Databases, Services); and • ORE Leadership (System Owner; Product Owner;);
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

SC-2 Application Partitioning (M) (H)

The information system separates user functionality (including user interface services) from information system management functionality.

SC-2	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-2 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions hosts the ORE within Provider data centers and uses appropriate network segmentation to establish the authorization boundary. 2 Twelve Solutions uses Security Groups to partition customer functions and management functions. Customers can only access the ORE web application over HTTPS. Management functions are accessed through the Bastion Host or a management console by the Operations team. Application:& Operations team and the Engineering team are designated as account managers for infrastructure tools. All ORE/Provider infrastructure remote access is provided through SSH connections to the bastion host.& & Database:& 2 Twelve Solutions admins have access to the OS, instance that holds database to perform backup, apply patches and make updates through automation. & Operating System:& Operations team and the Engineering team are considered as privileged users in ORE environment. Engineering team is a dedicated account manager with limited privilege and Operations team has full privileges.& Authentication to this system leverages multiple factors to ensure a strong authentication. The SSH configuration enforces the user to public-private key authentication. This entails that each user has a unique set of SSH Keys where the public key is added to the SSH Bastion host through automation. Once connected to the system, all changes are handled by executing the prepared automation from the change management process against the scope of the change and the status of the change ticket.

SC-4 Information in Shared Resources (M) (H)

The information system prevents unauthorized and unintended information transfer via shared system resources.

SC-4	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-4 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Information flow is enforced through the use of Firewall rules, which define the allowed traffic flows throughout the ORE environment and across the boundary. Security groups are configured to deny-by-default and only allow by exception. Security Groups are used to prevent unauthorized communication between customer servers. & Application:& Information flow for the ORE application is enforced through the use of Firewall rules. Security groups are configured to deny by default and only allow by exception policy. The ORE application& provides customers with a highly secure environment backed by an "always secure" architecture that is based on a multilayered security model that maximizes data security and ensures service continuity.& • All data in transit into or outside of the authorization boundary is encrypted with a FIPS 140-2 validated method. • Application-to-application communication is protected by certificates/trust relationships. • During the authentication and authorization process, the application uses TLS 1.3 to secure the data in transit. • Separation of accounts has been established so that administrative level access functions are tightly controlled between ORE application administrators and customer accounts. • Access to ORE environment is restricted through a Reverse Proxy/Load Balancer that allocates connections. • S3 is used by 2 Twelve Solutions to store data in an encrypted way using AES-256, and to store installation files required for the installation of new ORE platform instances. • Every instance in the environment has been assigned a security group with both inbound and outbound rules configured to prevent all unauthorized connections. • The customer will connect to the ORE platform through a web browser over HTTPS. & Operating System:& Information flow for the ORE operating system is enforced through the use of Firewall rules. Security groups are configured to deny by default and only allow by exception.

SC-5 Denial of Service Protection (L) (M) (H)

The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined types of denial of service attacks or reference to source for such information*] by employing [*Assignment: organization-defined security safeguards*].

SC-5	Control Summary Information
Responsible Role: Fraser, Doug	
sc-05_odp.01:	
sc-05_odp.02:	
sc-05_odp.03:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-5 What is the solution and how is it implemented?

Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Application: ORE implements the following methods to protect against or limit the effects of Denial of Service Attacks (DOS) including Distributed Denial of Service (DDOS) attacks, flooding attacks including bandwidth exhausting (e.g., UDP floods), protocol exhausting (e.g., SYN flood) and application exhausting attacks (e.g., HTTP GET/POST floods). & 1. Minimizing the Attack Surface Area – Use of Private Cloud enclaves allows the obscuring of instances from the Internet by ensuring non-public instances are only available on a private subnet and private DNS entries are only accessible internally. Security Groups act as a firewall for instances while Network ACLs act as a firewall for associated subnets. & 2. Scaling to Absorb the Attack - DDoS attacks are about scale. Most attackers achieve their purpose by sending a level of traffic that the application cannot accommodate. ORE utilizes auto scaling to add capacity when needed which requires more time and resources on the part of the attacker to overcome. Scaling& provides four direct benefits against DDoS attacks: • The attack is dispersed over a wider area. • Attackers have to expend more resources to scale up the attack. • Scaling buys time to analyze the DDoS attack and respond with countermeasures. • Scaling provides an additional layer of redundancy for other failure scenarios. & 3. Safeguard Exposed Resources – External access to ORE resources is severely limited. All customer traffic comes through Load Balancers. Because the Load Balanccers only forward valid TCP requests, DDoS attacks such as UDP and SYN floods are not able to reach ORE server instances. & 4. System monitoring – Regular monitoring of all system audit logs allows the Operations team to know the levels and patterns on normal usage of the system. This includes monitoring of audit logs from applications, web servers, operating systems, and databases.& Logs are especially germane to DOS attacks as they provide significant ability to monitor the network. & 5. Active Response – After the attack is detected and analyzed, offending IP addresses that make excessive repeated attempts to access system resources would have their IP addresses blocked at the Reverse Proxys. & Database:& Database is not internet facing and can only be accessed through the ORE application. & Operating System:& Authorized 2 Twelve Solutions administrators access operating systems by authenticating through the bastion host. All users must have a valid SSH key. After authentication through the bastion host, users must have a matching public SSH key on the instance to establish connection with

	that host. Whitelisting at the bastion host is implemented to only open connection to a specific set of IP ranges.&
Part b	

SC-6 Resource Availability (M) (H)

The information system protects the availability of resources by allocating [*Assignment: organization-defined resources*] by [*Selection (one or more); priority; quota;* [*Assignment: organization-defined security safeguards*]].

{{CONTROL|SC-6}}

SC-7 Boundary Protection (L) (M) (H)

The information system:

(a) Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and

(b) Implements subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and

(c) Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

SC-7	Control Summary Information
Responsible Role: Fraser, Doug	
sc-07_odp:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-7 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions uses Grafana for network monitoring capabilities of the external and internal network traffic. External traffic through the Reverse Proxy is captured in logs and forwarded to Grafana for near real time monitoring and alerting. & 2 Twelve Solutions also employs a defense in depth strategy for boundary protection using Security Groups, and the NAT Gateway. Security Groups are configured on each system within the boundary to limit both inbound and outbound traffic. Outbound communication initiated by ORE over HTTPS connections routed via a NAT gateway and controlled using Firewall rules. Security Groups are configured for all network interfaces to provide stateful inbound/outbound port/protocol and IP CIDR restrictions. & Application:& 2 Twelve Solutions ORE auditable events are selected using a risk-based approach that takes into account their information security standards. The following are deemed to be auditable events: • All administrator privileged functions • Authentication checks • Authorization checks • Data deletions, data access, data changes, and permission changes & Databases: ORE generates audit records for the following events which are then transported to Grafana. • Database events • SQL statements • Privileges • Schemas • Objects & Operating System: 2 Twelve Solutions ORE monitors industry-wide security threats and has defined the following events as auditable events that should be captured in system audit logs based on mission/business needs: • Failed logon attempts • File integrity monitoring • Account and/or profile changes and deletions • Changes to system security settings and parameters • System shutdowns/restarts • Use of privileged accounts and/or activities
Part b	

Part c	

SC-7 (3) CONTROL ENHANCEMENT (M) (H)

The organization limits the number external network connections to the information system.

SC-7 (3)	**Control Summary Information**
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-7 (3) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions& limits the number external network connections to the ORE& environment. Infrastructure access to the ORE& environment is only permitted via the bastion host; authenticate through SSH key. No ORE Application components permit direct SSH connections.& All external connections are controlled through the Security Groups and firewalls.& Security group denies all traffic by default and connections in Firewall rules are whitelisted. 2 Twelve Solutions documents all internal connections to the ORE environments in the authorization boundary, data flow, ports, and protocol, services in Section 9 and 10 of the SSP. & 2 Twelve Solutions also employs a defense in depth strategy for boundary protection using Security Groups, and the NAT Gateway. Security Groups are configured on each system within the boundary to limit both inbound and outbound traffic. Outbound communication initiated by ORE over HTTPS connections routed via an NAT gateway and controlled using Firewall rules. Security Groups are configured for all network interfaces to provide stateful inbound/outbound port/protocol and IP CIDR restrictions.

SC-7 (4) CONTROL ENHANCEMENT (M)

The organization:

(a) Implements a managed interface for each external telecommunication service;

(b) Establishes a traffic flow policy for each managed interface;

(c) Protects the confidentiality and integrity of the information being transmitted across each interface;

(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and

(e) Reviews exceptions to the traffic flow policy [*FedRAMP Assignment: at least at least annually*] and removes exceptions that are no longer supported by an explicit mission/business need.

SC-7 (4)	Control Summary Information
Responsible Role: Fraser, Doug	
sc-07.04_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-7 (4) What is the solution and how is it implemented?

Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Part a:& **2 Twelve Solutions Responsibility**: 2 Twelve Solutions does not actively manage telecommunication services. Part b:& **2 Twelve Solutions Responsibility**: 2 Twelve Solutions has established a traffic flow policy for each managed interfaces through the use of firewalls and Security Groups. The traffic control policies detail what traffic is approved, what ports and protocols are allowed and the nature of the data transmitted. Details of these traffic flow are further explained in Section 9 & 10 of this SSP. Modification to the traffic flow policy must be requested and approved through the established change management process in Agile system. & 2 Twelve Solutions also employs a defense in depth strategy for boundary protection using Security Groups, and the NAT Gateway. Security Groups are configured on each system within the boundary to limit both inbound and outbound traffic. Outbound communication initiated by ORE over HTTPS connections routed via an NAT gateway and controlled using Firewall rules. Security Groups are configured for all network interfaces to provide stateful inbound/outbound port/protocol and IP CIDR restrictions. Part c:& **2 Twelve Solutions Responsibility**: ORE ensures the confidentiality and integrity of transmitted information by employing cryptographic protection. All access to the applications is through reverse proxies which enforce HTTPS via TLS v1.3 only. 2 Twelve Solutions relies on a third-party trusted Certificate Authority (CA) Let's Encrypt for external TLS certificates. All TLS certificates are a minimum of RSA 2048-bit certificates. & Application: By default, the Reverse Proxy accepts TLS 1.3 for HTTPS connections. & Database: ORE databases are not public facing and only accessible internally through ORE components. ORE databases can be accessed through the ORE application or SSH. & Operating System:& Authorized 2 Twelve Solutions administrators access operating systems by authenticating through the bastion host.& For admins, ORE accepts only remote SSH connections to the bastion host. 2 Twelve Solutions utilizes SSH key pairs generated using RSA 2048 bit size key. &

	Outbound communication initiated by ORE are over HTTPS connections and controlled using Firewall rules. Security Groups are configured for all network interfaces to provide stateful inbound/outbound port/protocol and IP CIDR restrictions. Part d:& **2 Twelve Solutions Responsibility**: Approved traffic flow policy rules are specific traffic rules required and approved for ORE. Exception rule to the traffic flow policy must be documented with a supporting mission/business need and its duration. Exceptions to the traffic flow policy must be requested though a Agile system ticket and must obtain approval from the established change management process. If the request is approved by the ARB, Operations will modify the associated AWS security group and add the nature of the connection to the whitelisting. Exception to traffic flow policy must be reviewed at least annually. Part e:& **2 Twelve Solutions Responsibility**: 2 Twelve Solutions's Operations and Engineering teams review and update Security Groups at least annually. The Operations team removes exceptions that are no longer supported by an explicit mission/business need. Removal of traffic flow exceptions must go through the same change management process through Agile system. If the request is approved by the ARB, the Operations team will modify the associated security group and remove the connection from applicable Firewall rules and resources. Part f:& **2 Twelve Solutions Responsibility**: 2 Twelve Solutions does not actively manage telecommunication services. Part g:& **2 Twelve Solutions Responsibility**: 2 Twelve Solutions does not actively manage telecommunication services. Part h:

	2 Twelve Solutions Responsibility: 2 Twelve Solutions does not actively manage telecommunication services.
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	

SC-7 (5) CONTROL ENHANCEMENT (M) (H)

The information system at managed interfaces denies network traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

SC-7 (5)	Control Summary Information
Responsible Role: Fraser, Doug	
sc-07.05_odp.01:	
sc-07.05_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-7 (5) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: 2 Twelve Solutions& ORE employs a deny-all, permit by exception strategy for restricting connections to the ORE environment. 2 Twelve Solutions prohibits external connections outside of the defined boundary in Section 10.1. All external connections are controlled through the Security Groups and firewalls.& Security group denies all traffic by default and connections in Firewall rules are whitelisted. 2 Twelve Solutions documents all internal connections to the ORE environments in the authorization boundary, data flow, ports, and protocol, services in Section 9 and 10 of the SSP.

SC-7 (7) CONTROL ENHANCEMENT (M) (H)

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

SC-7 (7)	Control Summary Information
Responsible Role: Fraser, Doug	
sc-07.07_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-7 (7) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Infrastructure administrators access the system via the Bastion hosts utilizing SSH. There is no client VPN in use in the system and thus split tunneling (establishing non-remote connections with the system and communicating via some other connection to resources in external networks) is prevented. & Workstations are not part of the ORE authorization boundary.

SC-7 (8) CONTROL ENHANCEMENT (M) (H)

The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers at managed interfaces.

SC-7 (8)	Control Summary Information
Responsible Role: Fraser, Doug	
sc-07.08_odp.01:	
sc-07.08_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-7 (8) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions controls the routing of internal traffic to the internet with a NAT gateway. This allows authorized servers to initiate outbound connections to the internet but prevent servers from receiving inbound traffic from the internet. In addition, ORE inbound traffic must first go through a reverse proxy server. & Application: Firewall rules are leveraged to enforce access flow and provide logical separation. Application front end users are able to authenticate through MFA. The Reverse Proxy enforces TLS 1.3 encryption to protect the communication session.& Database: Databases are not internet facing and direct connections cannot be established with external sources.& Operating System: Authorized 2 Twelve Solutions administrators access operating systems by authenticating through the bastion host. All users must have a valid SSH key. After authentication through the bastion host, users must have a matching public SSH key on the instance to establish a connection with that host. & Outbound communication initiated by ORE are over HTTPS connections and controlled using Firewall rules. Security Groups are configured for all network interfaces to provide stateful inbound/outbound port/protocol and IP CIDR restrictions.

SC-7 (12) CONTROL ENHANCEMENT (M)

The organization implements [*Assignment: organization-defined host-based boundary protection mechanisms*] at [*Assignment: organization-defined information system components*].

{{CONTROL|SC-7.12}}

SC-7 (13) CONTROL ENHANCEMENT (M)

The organization isolates [*FedRAMP Assignment: See SC-7 (13) additional FedRAMP Requirements and Guidance*] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

SC-7 (13) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

{{CONTROL|SC-7.13}}

SC-7 (18) CONTROL ENHANCEMENT (M) (H)

The information system fails securely in the event of an operational failure of a boundary protection device.

{{CONTROL|SC-7.18}}

SC-8 Transmission confidentiality and Integrity (M) (H)

The information system protects the [*FedRAMP Assignment: confidentiality AND integrity*] of transmitted information.

SC-8	Control Summary Information
Responsible Role: Fraser, Doug	
sc-08_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-8 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE ensures the confidentiality and integrity of transmitted information by employing cryptographic protection. All access to the applications is through reverse proxies which enforce HTTPS via TLS v1.3 only. 2 Twelve Solutions relies on a third-party trusted Certificate Authority (CA) Let's Encrypt for external TLS certificates. All TLS certificates are a minimum of RSA 2048-bit certificates. & Application: By default, the Reverse Proxy accepts TLS 1.3 for HTTPS connections. & Database: ORE databases are not public facing and only accessible internally through ORE components. ORE databases can be accessed through the ORE application or SSH. & Operating System:& Authorized 2 Twelve Solutions administrators access operating systems by authenticating through the bastion host.& For admins, ORE accepts only remote SSH connections to the bastion host. 2 Twelve Solutions utilizes SSH key pairs generated using RSA 2048 bit size key. & Outbound communication initiated by ORE are over HTTPS connections and controlled using Firewall rules. Security Groups are configured for all network interfaces to provide stateful inbound/outbound port/protocol and IP CIDR restrictions.

SC-8 (1) CONTROL ENHANCEMENT (M) (H)

The information system implements cryptographic mechanisms to [*FedRAMP Assignment: prevent unauthorized disclosure of information AND detect changes to information*] during transmission unless otherwise protected by [*FedRAMP Assignment: a hardened or alarmed carrier Protective Distribution System (PDS)*].

SC-8 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
sc-08.01_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-8 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: As discussed in control SC-8, ORE implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission. ORE does not utilize a hardened or alarmed carrier Protective Distribution System (PDS).& All access to the applications is through reverse proxies which enforce HTTPS via TLS v1.3 only. 2 Twelve Solutions relies on a third-party trusted Certificate Authority (CA) Let's Encrypt for external TLS certificates. All TLS certificates are a minimum of RSA 2048-bit certificates. & Application: By default, the Reverse Proxy accepts TLS 1.3 for HTTPS connections. & Database: ORE databases are not public facing and only accessible internally through ORE components. ORE databases can be accessed through the ORE application or SSH. & Operating System:& Authorized 2 Twelve Solutions administrators access operating systems by authenticating through the bastion host.& For admins, ORE accepts only remote SSH connections to the bastion host. 2 Twelve Solutions utilizes SSH key pairs generated using RSA 2048 bit size key. & Outbound communication initiated by ORE are over HTTPS connections and controlled using Firewall rules. Security Groups are configured for all network interfaces to provide stateful inbound/outbound port/protocol and IP CIDR restrictions.

SC-10 Network Disconnect (M)

The information system terminates the network connection associated with a communications session at the end of the session or after [*FedRAMP Assignment: no longer than thirty (30) minutes for RAS-based sessions and no longer than sixty (60) minutes for non-interactive user sessions*] of inactivity.

SC-10	Control Summary Information
Responsible Role: Fraser, Doug	
sc-10_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-10 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The bastion host disconnects the user SSH session automatically after 5 minutes, or upon request from the user. Timeout settings for all hosts within the boundary are configured through automation to 300 seconds. After 300 seconds of inactivity, the user is disconnected from ORE. & A customer connection to the ORE Application is a customer responsibility. ORE has the capability to terminate inactive session, but it is the customer's responsibility to define the inactivity time. & Application, Operating System:& For all infrastructure access, the bastion host disconnects the user SSH session automatically after 5 minutes, or upon request from the user. This is enforced by "ClientAliveInterval 300" and "Client AliveCountMax 0" configured on each host within the boundary including the bastion host. & Database:& Access to database is through ORE application and 2 Twelve Solutions admins do not have direct access to database.

SC-12 Cryptographic Key Establishment & Management (L) (M) (H)

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

SC-12 Additional FedRAMP Requirements and Guidance:

Guidance: Federally approved and validated cryptography.

SC-12	Control Summary Information
Responsible Role: Fraser, Doug	
sc-12_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-12 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: All access to the ORE environment is encrypted. 2 Twelve Solutions enforces the use of TLS v1.3 on HTTPS connections or SSH for infrastructure access. & <u>Application</u>:& ORE leverages a third-party trusted Certificate Authority (CA) Let's Encrypt for external TLS certificates. All TLS certificates are a minimum of RSA 2048-bit certificates. 2 Twelve Solutions does not manage certificates, when these certificates expire, 2 Twelve Solutions will request a new certificate.& & <u>Database</u>: ORE utilizes AWS KMS keys data at rest protection. AWS KMS keys are protected by FIPS 140-2 validated cryptographic modules and fully managed by AWS.& AWS KMS is a FedRAMP High authorized service. AWS KMS keys are enabled by default for all EBS volume and S3 encryption. & <u>Operating System</u>:& ORE utilizes SSH keys. The key pairs for administrative access to the boundary are generated during onboarding. The tool used for this is SSH-Keygen using FIPS 140-2 cryptographic module. SSH public keys are then distributed to the necessary servers through the use of automation scripts. This automates the process of transferring a user's public to the necessary servers within the environment.& SSH keys are generated by SSH-Keygen with RSA 2048 key length. Private SSH keys are installed on the user's .ssh directory and the public keys are installed on authorized host within ORE through automation. Private keys are further protected with a passphrase to encrypt the private key.

SC-12 (2) CONTROL ENHANCEMENT (M) (H)

The organization produces, controls, and distributes symmetric cryptographic keys using [*FedRAMP Selection: NIST FIPS-compliant*] key management technology and processes.

{{CONTROL|SC-12.2}}

SC-12 (3) CONTROL ENHANCEMENT (M) (H)

The organization produces, controls, and distributes asymmetric cryptographic keys using [*Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or* *prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key*].

{{CONTROL|SC-12.3}}

SC-13 Use of Cryptography (L) (M) (H)

The information system implements [*FedRAMP Assignment: FIPS-validated or NSA-approved cryptography]* in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

SC-13	Control Summary Information
Responsible Role: Fraser, Doug	
sc-13_odp.01:	
sc-13_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-13 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: 2 Twelve Solutions has implemented federally approved cryptography in multiple places within the environment. All access to the ORE environment is encrypted. 2 Twelve Solutions enforces the use of TLS v1.3 on HTTPS connections or SSH for infrastructure access. ORE leverage a third-party trusted Certificate Authority (CA) Let's Encrypt for external TLS certificates. All TLS certificates are a minimum of RSA 2048-bit certificates. 2 Twelve Solutions does not manage certificates, when these certificates expire, 2 Twelve Solutions will request a new certificate.& & Database: ORE utilize AWS KMS keys data at rest protection. AWS KMS keys are protected by FIPS 140-2validated cryptographic modules and fully managed by AWS.& AWS KMS is a FedRAMP High authorized service. AWS KMS keys are enabled by default for all EBS volume and S3 encryption. & Operating System:& ORE utilizes SSH keys. The key pairs for administrative access to the boundary are generated during onboarding. The tool used for this is SSH-Keygen using FIPS 140-2 cryptographic module. SSH public keys are then distributed to the necessary servers through the use of automation scripts. This automates the process of transferring a user's public to the necessary servers within the environment.& SSH keys are generated by SSH-Keygen with RSA 2048 key length. Private SSH keys are installed on the user's .ssh directory and the public keys are installed on authorized host within ORE through automation. Private keys are further protected with a passphrase to encrypt the private key.
Part b	

SC-15 Collaborative Computing Devices (M) (H)

The information system:

(a) Prohibits remote activation of collaborative computing devices with the following exceptions:[*FedRAMP Assignment: no exceptions*]; and

(b) Provides an explicit indication of use to users physically present at the devices.

SC-15 Additional FedRAMP Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

SC-15	Control Summary Information
Responsible Role: Fraser, Doug	
sc-15_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-15 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: There are no collaborative computing devices within the ORE boundary. 2 Twelve Solutions does not have access to physical assets for the ORE environment.
Part b	

SC-15 Additional FedRAMP Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

SC-15 Req.	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-15 What is the solution and how is it implemented?	
Req. 1	

SC-17 Public Key Infrastructure Certificates (M) (H)

The organization issues public key certificates under an [*Assignment: organization-defined certificate policy*] or obtains public key certificates from an approved service provider.

SC-17	Control Summary Information
Responsible Role: Fraser, Doug	
sc-17_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-17 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: Internet facing instances for ORE Application uses a PKI certificate from Let's Encrypt. These certificates are used by default as public endpoints of ORE for customers. 2 Twelve Solutions does not manage certificates, when these certificates expire, 2 Twelve Solutions will request a new certificate. Authority to request certificates from the certificate vendor is limited to members of the operations team. ORE customer connections go through Reverse Proxy, which enforces the use of TLS v1.3. Connection attempts of using TLS v1.1 or lower will be rejected.& &
Part b	

SC-18 Mobile Code (M) (H)

The organization:

(a) Defines acceptable and unacceptable mobile code and mobile code technologies;

(b) Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

(c) Authorizes, monitors, and controls the use of mobile code within the information system.

SC-18	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-18 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: The 2 Twelve Solutions DevOps team follows the 2 Twelve Solutions System Development Lifecycle Plan (SDLC) for all development and acquisitions. The 2 Twelve Solutions ORE Lifecycle Management Plan is developed in accordance to NIST Special Publication 800-37: Initiation, Development/Acquisition, Implementations, Operation/Maintenance, and Disposal. ORE has incorporated these five phases into a governance process to ensure all ORE systems deliver high quality cloud products and services that meet the expectations of the FedRAMP Program Management Office (PMO), ORE and its customers and the Federal cloud community.& & All mobile code and third-party code is reviewed according to its use case, licensing requirements for associated libraries, and security considerations before use or deployment. In the event a new mobile code technology was required or needed based on business requirements and functionality justifications, explicit approval would be required before coding could begin. & Proposed changes to ORE must go through the change management process. The Engineering team is responsible for reviewing proposed changes to ORE. They will either approve or disapprove the changes through the Agile system ticketing procedure with explicit consideration for the security impact analysis during the change management process.&
Part b	

SC-19 Voice Over Internet Protocol (M) (H)

The organization:

(a) Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

(b) Authorizes, monitors, and controls the use of VoIP within the information system.

{{CONTROL|SC-19}}

SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H)

The information system:

(a) Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

(b) Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

SC-20	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-20 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. & **<u>2 Twelve Solutions Responsibility</u>**: DNS requests made inside the ORE systems are sent to DNS Servers running on server instances within the system boundary. DNSSEC is enabled through BIND. These DNS servers perform all recursive requests to external authoritative DNS servers. DNS forwarder will verify the trust anchors at least hourly (3600 seconds) to ensure trust keys are up to date. The ORE DNS servers are configured to request and perform data origin authentication and data integrity verification on the DNS responses the system receives from authoritative DNS sources.&
Part b	

SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H)

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

SC-21	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-21 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: DNS requests made inside the ORE systems are sent to DNS Servers running on server instances within the system boundary. DNSSEC is enabled through BIND. These DNS servers perform all recursive requests to external authoritative DNS servers. DNS forwarder will verify the trust anchors at least hourly (3600 seconds) to ensure trust keys are up to date. The ORE DNS servers are configured to request and perform data origin authentication and data integrity verification on the DNS responses the system receives from authoritative DNS sources.&

SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H)

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

SC-22	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-22 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: DNS requests made inside the ORE systems are sent to DNS servers running on server instances within the system boundary. These DNS servers are in fail-over mode and have multiple upstream DNS servers for contingency purposes.& 2 Twelve Solutions maintains a secondary DNS server in another availability zone to allow fault-tolerant if the primary DNS server is unavailable. Both DNS servers have identical configurations and utilize DNSSEC to ensure security is not compromised during any fail-over.

SC-23 Session Authenticity (M) (H)

The information system protects the authenticity of communications sessions.

SC-23	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-23 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. & **2 Twelve Solutions Responsibility**: ORE implements FIPS-validated cryptographic modules, which provide mechanisms for authentication to a cryptographic module which meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. All access to the applications via web service and API are through reverse proxies and Reverse Proxy which enforce HTTPS via TLS v1.3. & Application: ORE application accepts and electronically verifies PIV cards and CAC through interaction with customer identity management solutions. & Database: ORE databases are not public facing and only accessible internally through ORE components. ORE databases can be accessed through the ORE application by the customer or by automation through SSH and bastion host. &

SC-28 Protection of Information at Rest (M) (H)

The information system protects the [*FedRAMP Selection: confidentiality AND integrity*]] of [*Assignment: organization-defined information at rest*].

SC-28 Additional FedRAMP Requirements and Guidance:

Guidance: The organization supports the capability to use cryptographic mechanisms to protect information at rest.

SC-28	Control Summary Information
Responsible Role: Fraser, Doug	
sc-28_odp.01:	
sc-28_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-28 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. 2 Twelve Solutions utilizes Amazon Elastic Block Store (EBS) Encryption for all data. Amazon EBS Encryption uses AWS KMS keys utilizing AES-256. For S3 buckets, encryption is enabled by default. AWS KMS keys utilizing AES-256 is used for S3 encryption as well.

SC-28 (1) CONTROL ENHANCEMENT (M)

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] on [*Assignment: organization-defined information system components*]

SC-28 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
sc-28.01_odp.01:	
sc-28.01_odp.02:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-28 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. 2 Twelve Solutions utilizes Amazon Elastic Block Store (EBS) Encryption for all data. Amazon EBS Encryption uses AWS KMS keys utilizing AES-256. For S3 buckets, encryption is enabled by default. AWS KMS keys utilizing AES-256 is used for S3 encryption as well.

SC-39 Process Isolation (L) (M) (H)

The information system maintains a separate execution domain for each executing process.

SC-39	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SC-39 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. 2 Twelve Solutions ORE components run on modern Linux operating systems. The Linux OS maintains a separate execution domain for each executing process by assigning a private virtual address space to each process. Each information system process is assigned a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes is achieved in the ORE environment by implementing commercial operating systems that employ multi-state processor technologies.

13.17. System and Information Integrity (SI)

SI-1 System and Information Integrity Policy and Procedures (L) (M)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

(b) Reviews and updates the current:

(1) System and information integrity policy [*FedRAMP Assignment: at least every three (3) years*]; and

(2) System and information integrity procedures [*FedRAMP Assignment: at least at least annually*].

SI-1	Control Summary Information
Responsible Role: Fraser, Doug	
si-01_odp.01:	
si-01_odp.02:	
si-01_odp.03:	
si-01_odp.04:	
si-01_odp.05:	
si-01_odp.06:	
si-01_odp.07:	
si-01_odp.08:	
Parameter SI-1(a)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific)	

SI-1 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO.& The ORE Information Security Policy directs the activities and procedures. The policy addresses purpose, scope, responsibilities (including management commitment), coordination among organizational entities, and compliance requirements to meet the control implementation requirements for the system and information integrity control family of a moderate baseline. All ORE procedures that are captured in ORE's document repository management system, are reviewed at least annually by the document owner and the Architecture Review Board (ARB). The ARB is responsible for notifying stakeholder when changes are made and approved by the ARB. This may require the creation of new documentation or reviewing and updating current procedures, annually or as needed; and policies every 3 years or as needed. The Engineering and Operations teams are responsible for reviewing policies and procedures. The team composition includes the following: • Engineering (Product development and engineering, Product management); • Operations (Operations for Applications, Databases, Services); and • ORE Leadership (System Owner; Product Owner;);
Part a1	
Part a1a	
Part a1b	
Part a2	
Part b	
Part c	
Part c1	
Part c2	

SI-2 Flaw Remediation (L) (M) (H)

The organization:

(a) Identifies, reports, and corrects information system flaws;

(b) Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

(c) Installs security-relevant software and firmware updates within [*FedRAMP Assignment: thirty 30 days of release of updates*] of the release of the updates; and

(d) Incorporates flaw remediation into the organizational configuration management process.

SI-2	Control Summary Information
Responsible Role: Fraser, Doug	
si-02_odp:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SI-2 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Much of the automated flaw remediation will be provided by platform services. The ORE uses Trivy to scan application container images for any vulnerabilities. Any vulnerabilities that are found will be remediated in a timely manner and an updated version will be released alongside the standard regular updates.
Part b	
Part c	
Part d	

SI-2 (2) CONTROL ENHANCEMENT (M) (H)

The organization employs automated mechanisms [*FedRAMP Assignment: at least monthly*] to determine the state of information system components with regard to flaw remediation.

SI-2 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
si-02.02_odp.01:	
si-02.02_odp.02:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SI-2 (2) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. Much of the automated flaw remediation will be provided by platform services. The ORE uses Trivy to scan application container images for any vulnerabilities. Any vulnerabilities that are found will be remediated in a timely manner and an updated version will be released alongside the standard regular updates.

SI-2 (3) CONTROL ENHANCEMENT (M) (H)

The organization:

(a) Measures the time between flaw identification and flaw remediation; and

(b) Establishes [*Assignment: organization-defined benchmarks*] for taking corrective actions.

{{CONTROL|SI-2.3}}

SI-3 Malicious Code Protection (L) (M)

The organization:

(a) Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

(b) Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

(c) Configures malicious code protection mechanisms to:

(1) Perform periodic scans of the information system [*FedRAMP Assignment: at least weekly*] and real-time scans of files from external sources at [*FedRAMP Assignment: to include endpoints*] as the files are downloaded, opened, or executed in accordance with organizational security policy; and

(2) [*FedRAMP Assignment: to include alerting administrator or defined security personnel*] in response to malicious code detection; and

(d) Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

SI-3	Control Summary Information
Responsible Role: Fraser, Doug	
si-03_odp.01:	
si-03_odp.02:	
si-03_odp.03:	
si-03_odp.04:	
si-03_odp.05:	
si-03_odp.06:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SI-3 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Much of the malicious code protection will be provided by platform services. The ORE uses Trivy to scan application container images for any vulnerabilities. When a false positive is identified, ORE will continue to operate as the finding is being assessed. For validated findings, ORE follows the Incident Response plan for valid findings or security incidents. If an alert is determined to be a false positive, appropriate tuning measures are taken (vulnerability/triage documentation, etc.).
Part b	
Part c	
Part c1	
Part c2	
Part d	

SI-3 (1) CONTROL ENHANCEMENT (M) (H)

The organization centrally manages malicious code protection mechanisms.

{{CONTROL|SI-3.1}}

SI-3 (2) CONTROL ENHANCEMENT (M) (H)

The information system automatically updates malicious code protection mechanisms.

{{CONTROL|SI-3.2}}

SI-3 (7) CONTROL ENHANCEMENT (M) (H)

The information system implements nonsignature-based malicious code detection mechanisms.

{{CONTROL|SI-3.7}}

SI-4 Information System Monitoring (L) (M) (H)

The organization:

(a) Monitors the information system to detect:

(1) Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and

(2) Unauthorized local, network, and remote connections;

(b) Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];

(c) Deploys monitoring devices (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;

(d) Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

(e) Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

(f) Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

(g) Provides [*Assignment: organization-defined information system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed;* [*Assignment: organization-defined frequency*]].

SI-4 Additional FedRAMP Requirements and Guidance:

Guidance: See US-CERT Incident Response Reporting Guidelines.

{{CONTROL|SI-3.7}}

SI-4 (1) CONTROL ENHANCEMENT (M) (H)

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

{{CONTROL|SI-4.1}}

SI-4 (2) CONTROL ENHANCEMENT (M) (H)

The organization employs automated tools to support near real-time analysis of events.

SI-4 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SI-4 (2) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. Application, Operating System, and Database: ORE collects web server and application logs that are readily available to be collected by a centralized logging server.

SI-4 (4) CONTROL ENHANCEMENT (M) (H)

The information system monitors inbound and outbound communications traffic [*FedRAMP Assignment: continuously]* for unusual or unauthorized activities or conditions.

SI-4 (4)	Control Summary Information
Responsible Role: Fraser, Doug	
si-04.04_odp.01:	
si-04.04_odp.02:	
si-04.04_odp.03:	
si-04.04_odp.04:	
Parameter SI-4(4)):	
si-4.4_prm_2:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SI-4 (4) What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Application, Operating System, and Database: The web server and application monitor inbound and outbound communication within ORE continuously for unusual or unauthorized activities or conditions.
Part b	

SI-4 (5) CONTROL ENHANCEMENT (M) (H)

The information system alerts [*Assignment: organization-defined personnel or roles*] when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined compromise indicators*].

SI-4(5) Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with the incident response plan.

SI-4 (5)	Control Summary Information
Responsible Role: Fraser, Doug	
si-04.05_odp.01:	
si-04.05_odp.02:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SI-4 (5) What is the solution and how is it implemented?

This control is reviewed at least annually or as needed by the ISSO and SO.

Application, Operating System, and Database: TBD

Existing Writeup:

The Engineering and Operations team are alerted by DGC through the OSSEC IPS when it detects errors from invalid source, unknown users, attempts at root access, multiple use errors, integrity check warning, warning messages from the kernel, common attack patterns, and all activities outlined in the OSSEC classification level rule sets. The following security events established by SecOps team trigger alerts for compromise or potential compromise of the information system:

Authorized/Unauthorized access, including:

o Failed or rejected user actions

o Failed or rejects actions involving data, files, and other resources

o Access policy violations and notifications for network gateways/firewalls

o Alerts from OSSEC, rkhunter, ClamAV and health monitoring tools

All Privileged Operations, including:

o Use of privileged accounts, e.g. root, administrator

o System start-up and stop

o I/O device attachment/detachment

System Alerts or Failures, including:

o Console alerts or messages

o System log exceptions

o Network management alarms

Changes to, or attempts to change, system security settings and controls

SI-4 (14) CONTROL ENHANCEMENT (M) (H)

The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

{{CONTROL|SI-4.14}}

SI-4 (16) CONTROL ENHANCEMENT (M) (H)

The organization correlates information from monitoring tools employed throughout the information system.

{{CONTROL|SI-4.16}}

SI-4 (23) CONTROL ENHANCEMENT (M) (H)

The organization implements [*Assignment: organization-defined host-based monitoring mechanisms*] at [*Assignment: organization-defined information system components*].

{{CONTROL|SI-4.23}}

SI-5 Security Alerts & Advisories (L) (M) (H)

The organization:

(a) Receives information system security alerts, advisories, and directives from [*FedRAMP Assignment: to include US-CERT*] on an ongoing basis;

(b) Generates internal security alerts, advisories, and directives as deemed necessary;

(c) Disseminates security alerts, advisories, and directives to [*FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities*]; and

(d) Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

SI-5	Control Summary Information
Responsible Role: Fraser, Doug	
si-05_odp.01:	
si-05_odp.02:	
si-05_odp.03:	
si-05_odp.04:	
si-05_odp.05:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SI-5 What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. Application, Operating System, and Database: ORE receives security alerts and maintenance updates from vendor security bulletins. ORE also receives alerts from US-CERT (http://www.us-cert.gov/). Part b: This control is reviewed at least annually or as needed by the ISSO and SO. Application, Operating System and Database: Internal security alerts are issued to the Engineering and Operations team in the form of tickets or emails. Part c: This control is reviewed at least annually or as needed by the ISSO and SO. Application, Operating System and Database: Security alerts, advisories, and directives are disseminated to the Engineering and Operations team. ORE uses internal email groups to distribute security alerts to appropriate personnel, including engineers in charge of the remediation. Part d: This control is reviewed at least annually or as needed by the ISSO and SO. Application, Operating System and Database: The Engineering and Operations team will implement security directives from US-Cert or the Customer as directed within established criteria as documented in SI-2.
Part b	
Part c	
Part d	

SI-6 Security Functionality Verification (M) (H)

The information system:

(a) Verifies the correct operation of [*Assignment: organization-defined security functions*];

(b) Performs this verification [*FedRAMP Assignment: to include upon system startup and/or restart at least monthly*];

(c) Notifies [*FedRAMP Assignment: to include system administrators and security personnel*] of failed security verification tests; and

(d) [*Selection (one or more): shuts the information system down; restarts the information system;* [*FedRAMP Assignment: to include notification of system administrators and security personnel*] when anomalies are discovered.

{{CONTROL|SI-6}}

SI-7 Software & Information Integrity (M) (H)

The organization employs integrity verification tools to detect unauthorized changes to [*Assignment: organization-defined software, firmware, and information*].

SI-7	Control Summary Information
Responsible Role: Fraser, Doug	
si-07_odp.01:	
si-07_odp.02:	
si-07_odp.03:	
si-07_odp.04:	
si-07_odp.05:	
si-07_odp.06:	
Parameter SI-7):	
si-7_prm_2:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SI-7 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Application: The hash value of each application update/upgrade is manually checked to ensure the integrity of the source file is correct. Operating System and Database: TBD Engineering and Operations personnel investigate integrity violations and work to determine the cause and required remediation actions.
Part b	

SI-7 (1) CONTROL ENHANCEMENT (M) (H)

The information system performs an integrity check of [*Assignment: organization-defined software, firmware, and information*] [*FedRAMP Selection (one or more): at startup; at [FedRAMP Assignment: to include security-relevant events*]; [*FedRAMP Assignment: at least monthly*]].

SI-7 (1)	Control Summary Information
Responsible Role: Fraser, Doug	
si-07.01_odp.01:	
si-07.01_odp.02:	
si-07.01_odp.03:	
si-07.01_odp.04:	
si-07.01_odp.05:	
si-07.01_odp.06:	
si-07.01_odp.07:	
si-07.01_odp.08:	
si-07.01_odp.09:	
si-07.01_odp.10:	
si-07.01_odp.11:	
si-07.01_odp.12:	
Parameter SI-7(1)-1):	
Parameter SI-7(1)-2):	
Parameter SI-7(1)-3):	
Parameter SI-7(1)):	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	

Control Origination (check all that apply):
☒Service Provider Corporate
☒Service Provider System Specific
☒Service Provider Hybrid (Corporate and System Specific)
☒Configured by Customer (Customer System Specific)
☒Provided by Customer (Customer System Specific)
☒Shared (Service Provider and Customer Responsibility)
☒Inherited from pre-existing FedRAMP Authorization

SI-7 (1) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. Application: The hash value of each application update/upgrade is manually checked to ensure the integrity of the source file is correct. Operating System and Database: TBD.

SI-7 (7) CONTROL ENHANCEMENT (M) (H)

The organization incorporates the detection of unauthorized [*Assignment: organization-defined security-relevant changes to the information system*] into the organizational incident response capability.

SI-7 (7)	Control Summary Information
Responsible Role: Fraser, Doug	
si-07.07_odp:	
Implementation Status (check all that apply): ☒Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SI-7 (7) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. Application: The hash value of each application update/upgrade is manually checked to ensure the integrity of the source file is correct. Operating System and Database: TBD.

SI-8 Spam Protection (M) (H)

The organization:

(a) Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and

(b) Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policies and procedures.

SI-8	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☒Not applicable	
Control Origination (check all that apply): ☐Service Provider Corporate ☐Service Provider System Specific ☐Service Provider Hybrid (Corporate and System Specific) ☐Configured by Customer (Customer System Specific) ☐Provided by Customer (Customer System Specific) ☐Shared (Service Provider and Customer Responsibility) ☐Inherited from pre-existing FedRAMP Authorization	

SI-8 What is the solution and how is it implemented?	
Part a	Part a: This control is reviewed at least annually or as needed by the ISSO and SO. Application, Operating System and Database: Not Applicable. ORE sends outbound notification emails only, no inbound email is allowed. Part b: This control is reviewed at least annually or as needed by the ISSO and SO. Application, Operating System and Database: Not Applicable. ORE sends outbound notification emails only, no inbound email is allowed.
Part b	

SI-8 (1) CONTROL ENHANCEMENT (M) (H)

The organization centrally manages spam protection mechanisms.

{{CONTROL|SI-8.1}}

SI-8 (2) CONTROL ENHANCEMENT (M) (H)

The organization automatically updates spam protection mechanisms.

SI-8 (2)	Control Summary Information
Responsible Role: Fraser, Doug	
si-08.02_odp:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☒Not applicable	
Control Origination (check all that apply): ☐Service Provider Corporate ☐Service Provider System Specific ☐Service Provider Hybrid (Corporate and System Specific) ☐Configured by Customer (Customer System Specific) ☐Provided by Customer (Customer System Specific) ☐Shared (Service Provider and Customer Responsibility) ☐Inherited from pre-existing FedRAMP Authorization	

SI-8 (2) What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. Application, Operating System and Database: Not Applicable. ORE sends outbound notification emails only, no inbound email is allowed.

SI-10 Information Input Validation (M) (H)

The information system checks the validity of [*Assignment: organization-defined information inputs*].

SI-10	Control Summary Information
Responsible Role: Fraser, Doug	
si-10_odp:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SI-10 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. Input validation is conducted by the Engineering team as part of the application development cycle. In addition, static code analysis by Semgrep and peer review is also conducted for each code commit. Rules for checking the valid syntax and semantics of information system inputs are in place to verify that inputs match specified definitions for format and content. ORE's input validation framework performs all input checking to verify length, format, and HTML syntax. It also checks and validates user input (URL, parameters, user fields etc.). Invalid input will generate an error message displayed to users

SI-11 Error Handling (M) (H)

The information system:

(a) Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and

(b) Reveals error messages only to [*Assignment: organization-defined personnel or roles*].

SI-11	Control Summary Information
Responsible Role: Fraser, Doug	
si-11_odp:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☐Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SI-11 What is the solution and how is it implemented?	
Part a	This control is reviewed at least annually or as needed by the ISSO and SO. Part a: The ORE generates error messages that provide information necessary for corrective actions without revealing user name and password combinations, attributes used to validate a password reset request, such as security questions, personally identifiable information (excluding unique username identifiers provided as a normal part of a transactional record), or content related to internal security functions: private encryption keys, white list or blacklist rules, object permission attributes and settings. Part b: Error messages are only revealed to authorized system users, except for errors on login pages. Errors exclude customer information, specific technology and versions, usernames and passwords.
Part b	

SI-12 Information Output Handling and Retention (L) (M) (H)

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

SI-12	Control Summary Information
Responsible Role: Fraser, Doug	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☒Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SI-12 What is the solution and how is it implemented?
This control is reviewed at least annually or as needed by the ISSO and SO. The ORE handles and retains both information within and output from the information systems in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

SI-16 Memory Protection (M) (H)

The information system implements [*Assignment: organization-defined fail-safe procedures*] to protect its memory from unauthorized code execution.

SI-16	**Control Summary Information**
Responsible Role: Fraser, Doug	
si-16_odp:	
Implementation Status (check all that apply): ☐Implemented ☐Partially implemented ☒Planned ☐Alternative implementation ☐Not applicable	
Control Origination (check all that apply): ☒Service Provider Corporate ☒Service Provider System Specific ☒Service Provider Hybrid (Corporate and System Specific) ☒Configured by Customer (Customer System Specific) ☒Provided by Customer (Customer System Specific) ☒Shared (Service Provider and Customer Responsibility) ☒Inherited from pre-existing FedRAMP Authorization	

SI-16 What is the solution and how is it implemented?
This control should be provided by the platform provider and be fully inherited.

14. ACRONYMS

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website Documents page.

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.

SYSTEMS SECURITY PLAN ATTACHMENTS

15. ATTACHMENTS

A recommended attachment file naming convention is <information system abbreviation> <attachment number> <document abbreviation> <version number> (for example, "Information System Abbreviation A8 IRP v1.0"). Use this convention to generate names for the attachments. Enter the appropriate file names and file extensions in Table 15-1 to describe the attachments provided. Make only the following additions/changes to Table 15-1:

- The first item, Information Security Policies and Procedures (ISPP), may be fulfilled by multiple documents. If that is the case, add lines to Table 15-1. to differentiate between them using the "xx" portion of the File Name. *Example* ORE *A1 ISPP xx v1.0*. Delete the "xx" if there is only one document.
- Enter the file extension for each attachment.
- Do not change the Version Number in the File Name in Table 15-1. . (Information System Abbreviation, attachment number, document abbreviation, version number)

Table 15-1. Names of Provided Attachments

Attachment	File Name	File Extension
Information Security Policies and Procedures	ORE A1 ISPP xx v1.0	. enter extension
User Guide	ORE A2 UG v1.0	. enter extension
Digital Identity Worksheet	Included in Section 15	
PTA	Included in Section 15	
PIA If needed)	ORE A4 PIA v1.0	. enter extension
Rules of Behavior	ORE A5 ROB v1.0	. enter extension
Information System Contingency Plan	ORE A6 ISCP v1.0	. enter extension
Configuration Management Plan	ORE A7 CMP v1.0	. enter extension
Incident Response Plan	ORE A8 IRP v1.0	. enter extension
CIS Workbook	ORE A9 CIS Workbook v1.0	. enter extension
FIPS 199	Included in Section 15	
Inventory	ORE A13 INV v1.0	. enter extension

ATTACHMENT I INFORMATION SECURITY POLICIES AND PROCEDURES

All Authorization Packages must include an Information Security Policies and Procedures attachment, which will be reviewed for quality.

{{ATTACHMENT|01}}

ATTACHMENT 2 USER GUIDE

All Authorization Packages must include a User Guide attachment, which will be reviewed for quality.

ATTACHMENT 3 DIGITAL IDENTITY WORKSHEET

The Digital Identity section explains the objective for selecting the appropriate Digital Identity levels for the candidate system. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63, Revision 3, Digital Identity Guidelines.

Introduction and Purpose

This document provides guidance on digital identity services (Digital Identity, which is the process of establishing confidence in user identities electronically presented to an information system). Authentication focuses on the identity proofing process (IAL), the authentication process (AAL), and the assertion protocol used in a federated environment to communicate authentication and attribute information (if applicable) (FAL). NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.

NIST SP 800-63-3 can be found at the following URL: NIST SP 800-63-3

Information System Name/Title

This Digital Identity Plan provides an overview of the security requirements for the Orchestrated Repository for the Enterprise (ORE) in accordance with NIST SP 800-63-3.

Table 15-2. Information System Name and Title

Unique Identifier	Information System Name	Information System Abbreviation
Enter FedRAMP Application Number.	Orchestrated Repository for the Enterprise	ORE

Digital Identity Level Definitions

NIST SP 800-63-3 defines three levels in each of the components of identity assurance to categorize a federal information system's Digital Identity posture. NIST SP 800-63-3 defines the Digital Identity levels as:

- IAL – refers to the identity proofing process.
- AAL – refers to the authentication process.
- FAL – refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).

FedRAMP maps its system categorization levels to NIST 800-63-3's levels as shown in Table 15-3:

Table 15-3. Mapping FedRAMP Levels to NIST SP 800-63-3 Levels

FedRAMP System Categorization	Identity Assurance Level (IAL)	Authenticator Assurance Level (AAL)	Federation Assurance Level (FAL)
High	IAL3: In-person, or supervised remote identity proofing	AAL3: Multi-factor required based on hardware-based cryptographic authenticator and approved cryptographic techniques	FAL3: The subscriber (user) must provide proof of possession of a cryptographic key, which is referenced by the assertion. The assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it
Moderate	IAL2: In-person or remote, potentially involving a "trusted referee"	AAL2: Multi-factor required, using approved cryptographic techniques	FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it
Low	IAL1: Self-asserted	AAL1: Single-factor or multi-factor	FAL1: Assertion is digitally signed by the identity provider
FedRAMP Tailored LI-SaaS	IAL1: Self-asserted	AAL1: Single-factor or multi-factor	FAL1: Assertion is digitally signed by the identity provider

Selecting the appropriate Digital Identity level for a system enables the system owner to determine the right system authentication technology solution for the selected Digital Identity levels. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63-3.

Review Maximum Potential Impact Levels

CSP Name has assessed the potential risk from Digital Identity errors, or Digital Identity misuse, related to a user's asserted identity. CSP Name has taken into consideration the potential for harm (impact) and the likelihood of the occurrence of the harm and has identified an impact profile as found in Table 15-4. Potential Impacts for Assurance Levels.

Assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Table 15-4. Potential Impacts for Assurance Levels

	Assurance Level Impact Profile		
Potential Impact Categories	**1**	**2**	**3**
Inconvenience, distress or damage to standing or reputation	Low	Mod	High

	Assurance Level Impact Profile		
Potential Impact Categories	**1**	**2**	**3**
Financial loss or agency liability	Low	Mod	High
Harm to agency programs or public interests	N/A	Low/Mod	High
Unauthorized release of sensitive information	N/A	Low/Mod	High
Personal Safety	N/A	Low	Mod/High
Civil or criminal violations	N/A	Low/Mod	High

Digital Identity Level Selection

The CSP Name has identified that they support the Digital Identity Level that has been selected for the Orchestrated Repository for the Enterprise as noted in Table 15-5. Digital Identity Level. The selected Digital Identity Level indicated is supported for federal agency consumers of the cloud service offering. Implementation details of the Digital Identity mechanisms are provided in the System Security Plan under control IA-2.

Table 15-5. Digital Identity Level

Digital Identity Level	Maximum Impact Profile	Selection
Level 1: AAL1, IAL1, FAL1	Low	☐
Level 2: AAL2, IAL2, FAL2	Moderate	☐
Level 3: AAL3, IAL3, FAL3	High	☐

ATTACHMENT 4 PTA / PIA

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: Templates.

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in **Error! Reference source not found.**.

Privacy Overview and Point of Contact (POC)

The Table 15-6. - Orchestrated Repository for the Enterprise; Privacy POC individual is identified as the Orchestrated Repository for the Enterprise Privacy Officer and POC for privacy at CSP Name.

Table 15-6. - Orchestrated Repository for the Enterprise; Privacy POC

Name	Click here to enter text.
Title	Click here to enter text.
CSP / Organization	Click here to enter text.
Address	Click here to enter text.
Phone Number	Click here to enter text.
Email Address	Click here to enter text.

APPLICABLE LAWS AND REGULATIONS

The FedRAMP Laws and Regulations may be found on: Templates. A summary of FedRAMP Laws and Regulations is included in the System Security Plan (SSP) **Error! Reference source not found.**.

Table 12-1. Orchestrated Repository for the Enterprise Laws and Regulations include additional laws and regulations that are specific to Orchestrated Repository for the Enterprise. These will include laws and regulations from the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law (PL), United States Code (USC), and Homeland Security Presidential Directives (HSPD).

Table 15-7. Orchestrated Repository for the Enterprise Laws and Regulations

Identification Number	Title	Date	Link
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

APPLICABLE STANDARDS AND GUIDANCE

The FedRAMP Standards and Guidance may be found on: Templates. The FedRAMP Standards and Guidance is included in the System Security Plan (SSP) ATTACHMENT 12 – FedRAMP Laws and Regulations. For more information, see the FedRAMP website.

Table 12-2. Orchestrated Repository for the Enterprise Standards and Guidance includes any additional standards and guidance that are specific to <Information System Name>. These will include standards and guidance from Federal Information Processing Standard (FIPS) and National Institute of Standards and Technology (NIST) Special Publications (SP).

Table 15-8. Orchestrated Repository for the Enterprise Standards and Guidance

Identification Number	Title	Date	Link
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

- Social Security numbers
- Passport numbers
- Driver's license numbers
- Biometric information
- DNA information
- Bank account numbers

PII does not refer to business information or government information that cannot be traced back to an individual person.

Privacy Threshold Analysis

CSP Name performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the <Information System Name> (ORE) components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by CSP Name can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

QUALIFYING QUESTIONS

Select One	Does the ISA collect, maintain, or share PII in any identifiable form?
Select One	Does the ISA collect, maintain, or share PII information from or about the public?
Select One	Has a Privacy Impact Assessment ever been performed for the ISA?
Select One	Is there a Privacy Act System of Records Notice (SORN) for this ISA system? If yes; the SORN identifier and name is: Enter SORN ID/Name.

If answers to Questions 1-4 are all “No” then a Privacy Impact Assessment may be omitted. If any of the answers to Question 1-4 are “Yes” then complete a Privacy Impact Assessment.

DESIGNATION

Check one.

☐ A Privacy Sensitive System

☐ Not a Privacy Sensitive System (in its current version)

The Privacy Impact Assessment Template can be found on the following FedRAMP website page: Templates.

ATTACHMENT 5 RULES OF BEHAVIOR

All Authorization Packages must include a Rules of Behavior (RoB) attachment, which will be reviewed for quality.

The RoB describes controls associated with user responsibilities and certain expectations of behavior for following security policies, standards and procedures. Security control PL-4 requires a CSP to implement rules of behavior.

The Rules of Behavior Template can be found on the following FedRAMP website page: Templates.

The Template provides two example sets of rules of behavior: one for Internal Users and one for External Users. The CSP should modify each of these two sets to define the rules of behavior necessary to secure their system.

ATTACHMENT 6 INFORMATION SYSTEM CONTINGENCY PLAN

All Authorization Packages must include an Information System Contingency Plan attachment, which will be reviewed for quality.

The Information System Contingency Plan Template can be found on the following FedRAMP website page: Templates.

The Information System Contingency Plan Template is provided for CSPs, 3PAOs, government contractors working on FedRAMP projects, government employees working on FedRAMP projects and any outside organizations that want to make use of the FedRAMP Contingency Planning process.

ATTACHMENT 7 CONFIGURATION MANAGEMENT PLAN

All Authorization Packages must include a Configuration Management Plan attachment, which will be reviewed for quality.

ATTACHMENT 8 INCIDENT RESPONSE PLAN

All Authorization Packages must include an Incident Response Plan attachment, which will be reviewed for quality.

ATTACHMENT 9 CIS WORKBOOK

All Authorization Packages must include Control Implementation Summary (CIS) Workbook attachment, which will be reviewed for quality.

The Template can be found on the following FedRAMP website page: Templates.

ATTACHMENT 10 FIPS 199

All Authorization Packages must include a Federal Information Processing Standard (FIPS) 199 Section, which will be reviewed for quality.

The FIPS-199 Categorization report includes the determination of the security impact level for the cloud environment that may host any or all of the service models: IaaS, PaaS and SaaS. The ultimate goal of the security categorization is for the CSP to be able to select and implement the FedRAMP security controls applicable to its environment.

Introduction and Purpose

This section is intended to be used by service providers who are applying for an Authorization through the U.S. federal government FedRAMP program.

The Federal Information Processing Standard 199 (FIPS 199) Categorization (Security Categorization) report is a key document in the security authorization package developed for submission to the Federal Risk and Authorization Management Program (FedRAMP) authorizing officials. The FIPS199 Categorization report includes the determination of the security impact level for the cloud environment that may host any or all of the service models (Information as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The ultimate goal of the security categorization is for the cloud service provider (CSP) to be able to select and implement the FedRAMP security controls applicable to its environment.

The purpose of the FIPS199 Categorization report is for the CSP to assess and complete the categorization of their cloud environment, to provide the categorization to the System Owner/Certifier and the FedRAMP Joint Authorization Board (JAB) and in helping them to make a determination of the CSP's ability to host systems at that level. The completed security categorization report will aid the CSP in selection and implementation of FedRAMP security controls at the determined categorization level.

Scope

The scope of the FIPS199 Categorization report includes the assessment of the information type categories as defined in the NIST Special Publication 800-60 Volume II Revision 1 Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.

System Description

The <Information System Name> system has been determined to have a security categorization of Choose level.

Methodology

Impact levels are determined for each information type based on the security objectives (confidentiality, integrity, availability). The confidentiality, integrity, and availability impact levels define the security sensitivity category of each information type. The FIPS PUB 199 is the high watermark for the impact level of all the applicable information types.

The FIPS PUB 199 analysis represents the information type and sensitivity levels of the CSP's cloud service offering (and is not intended to include sensitivity levels of agency data). Customer agencies will be expected to perform a separate FIPS 199 Categorization report analysis for their own data hosted on the CSP's cloud environment. The analysis must be added as an appendix to the SSP and drive the results for the Categorization section.

The Table 15-9. CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1below uses the NIST SP 800-60 V2 R1 Volume II Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories to identify information types with the security impacts.

Table 15-9. CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1

Information Type	NIST SP 800-60 V2 R1 Recommended Confidentiality Impact Level	NIST SP 800-60 V2 R1 Recommended Integrity Impact Level	NIST SP 800-60 V2 R1 Recommended Availability Impact Level	CSP Selected Confidentiality Impact Level	CSP Selected Integrity Impact Level	CSP Selected Availability Impact Level	Statement for Impact Adjustment Justification
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.
Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.	Enter text.

ATTACHMENT 11 SEPARATION OF DUTIES MATRIX

All Authorization Packages have the option to provide a Separation of Duties Matrix attachment, which will be reviewed for quality.

Error! Reference source not found. is referenced in the following controls.

AC-5 Separation of Duties (M) (H) Additional FedRAMP Requirements and Guidance

ATTACHMENT 12 FEDRAMP LAWS AND REGULATIONS

The Table 15-10. FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance lists all of the FedRAMP templates in which FedRAMP laws, regulations, standards and guidance are referenced.

Table 15-10. FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance

Phase		Document Title	
Document Phase		SSP	System Security Plan
	SSP Attachment 4	PTA/PIA	Privacy Threshold Analysis and Privacy Impact Assessment
	SSP Attachment 6	ISCP	Information System Contingency Plan
	SSP Attachment 10	FIPS 199	FIPS 199 Categorization
Assess Phase		SAP	Security Assessment Plan
Authorize Phase		SAR	Security Assessment Report

The FedRAMP Laws and Regulations can be submitted as an appendix or an attachment. The attachment can be found on this page: Templates.

Note: All NIST Computer Security Publications can be found at the following URL: http://csrc.nist.gov/publications/PubsSPs.html

ATTACHMENT 13 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: Templates.

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.