FEDRAMP SYSTEM SECURITY PLAN (SSP) LOW BASELINE TEMPLATE

Cloud Service Provider Name

Information System Name

Version #

Version Date

FedRAMP

CONTROLLED UNCLASSIFIED INFORMATION

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INFORMATION SYSTEM NAME/TITLE

This System Security Plan provides an overview of the security requirements for the Information System Name (Enter Information System Abbreviation) 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 Enter Information System Abbreviation information system.

The security safeguards implemented for the Enter Information System Abbreviation 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
233333	FAKE supply chain system	FAKE SCS

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: **Attachment 10, FIPS 199.**

Table 2-1. Security Categorization

System Sensitivity Level:	Low (L)

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 Enter Information System Abbreviation. 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.

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
Goods Acquisition Information Type	C.3.4.1	Low (L)	Low (L)	Low (L)
Inventory Control Information Type	C.3.4.2	Low (L)	Low (L)	Low (L)
Logistics Management Information Type	C.3.4.3	Low (L)	Low (L)	Low (L)
Services Acquisition Information Type	C.3.4.4	Low (L)	Low (L)	Low (L)

2.2. Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2-2. Sensitivity Categorization of Information Types, for the Enter Information System Abbreviation, 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	Low (L)
Integrity	Low (L)
Availability	Low (L)

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

Table 2-4. Baseline Security Configuration

Enter Information System Abbreviation Security Categorization	Low (L)

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 Attachment 3, Digital Identity Worksheet.

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 Level 2: AAL2, IAL2, FAL2

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

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 Enter Information System Abbreviation 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 Enter Information System Abbreviation 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 Enter Information System Abbreviation 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.

9. GENERAL SYSTEM DESCRIPTION

This section includes a general description of the Enter Information System Abbreviation.

9.1. System Function or Purpose

All SCM or central planning processes created to manage an organization's demand/supply network consists of three primary activities：
Demand Management，Supply Planning or Matching Assets with Demand ， Analytics Workbench.

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.

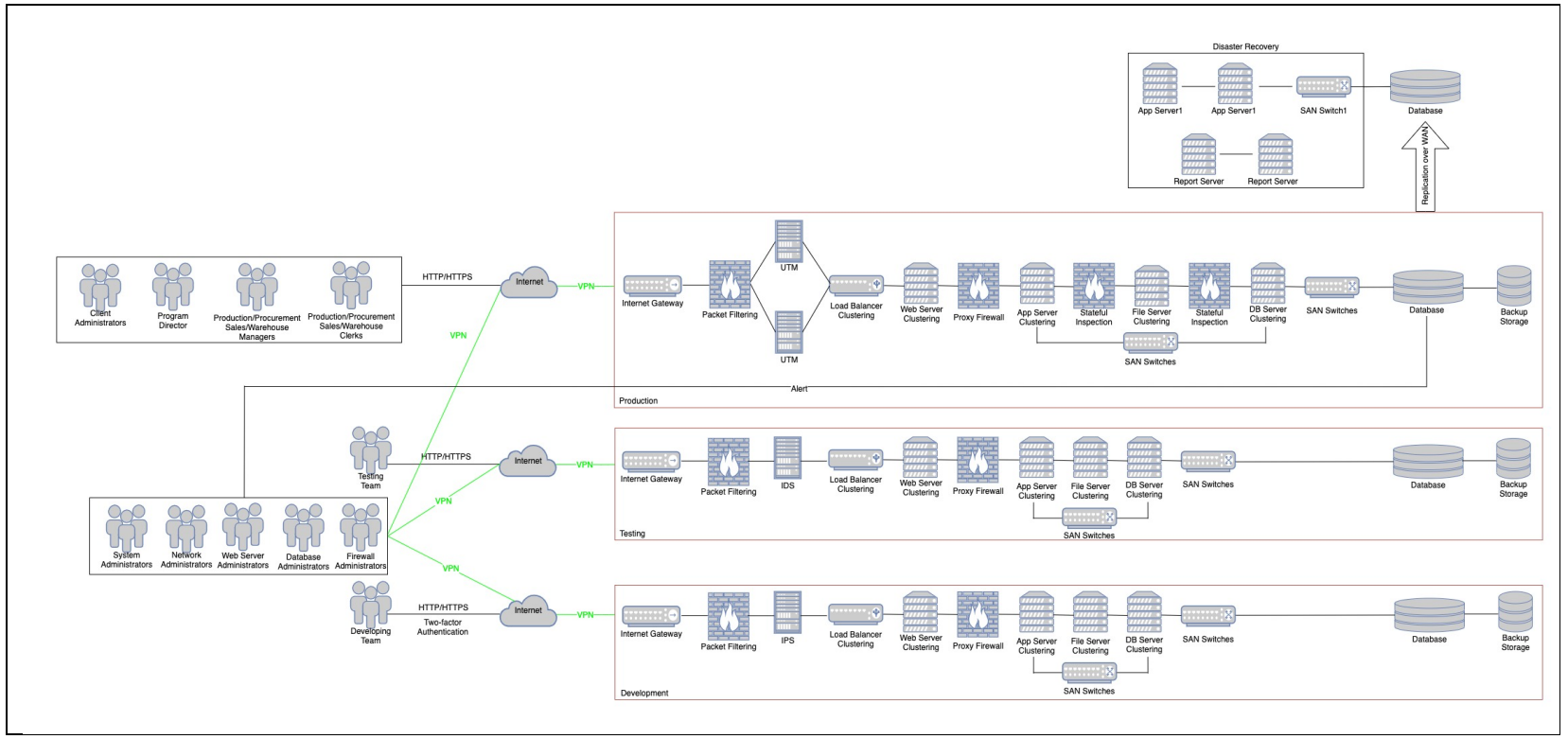


Figure 9-1. Authorization Boundary Diagram

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
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
Web server administrators	Internal	NLA	Moderate	N/A	Maintaining software and security updates, monitoring server activity and ensuring the availability of client/server applications, auditing server security.

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
Network administrators	Internal	NLA	Moderate	N/A	Network administrators are responsible for making sure that computer hardware and network infrastructure related to an organization's data network are effectively maintained.
Firewall administrators	Internal	NLA	Moderate	N/A	Responsible for configuring, installing, maintaining, and monitoring of firewalls.
Program Director	Internal	NLA	Limited	N/A	Reviews, approves and enforces policy.
Developing team	Internal	P	High-Risk	Developing system	Develop and program the system.
Testing team	Internal	NP	Severe	Testing administration	Test the confidentiality, integrity and availability of system.
Database administrator	Internal	NP	High-Risk	Database management	Manage the databases.

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
Production / Procurement / Sales / warehouse managers	External	NP	Moderate	Add and approve data	Approve data from clerks and submit requirements to system administrator to change the data.
Production / Procurement / Sales / warehouse clerks	External	NP	Limited	Read and write data	Read and write data into the system.

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 Enter Information System Abbreviation.

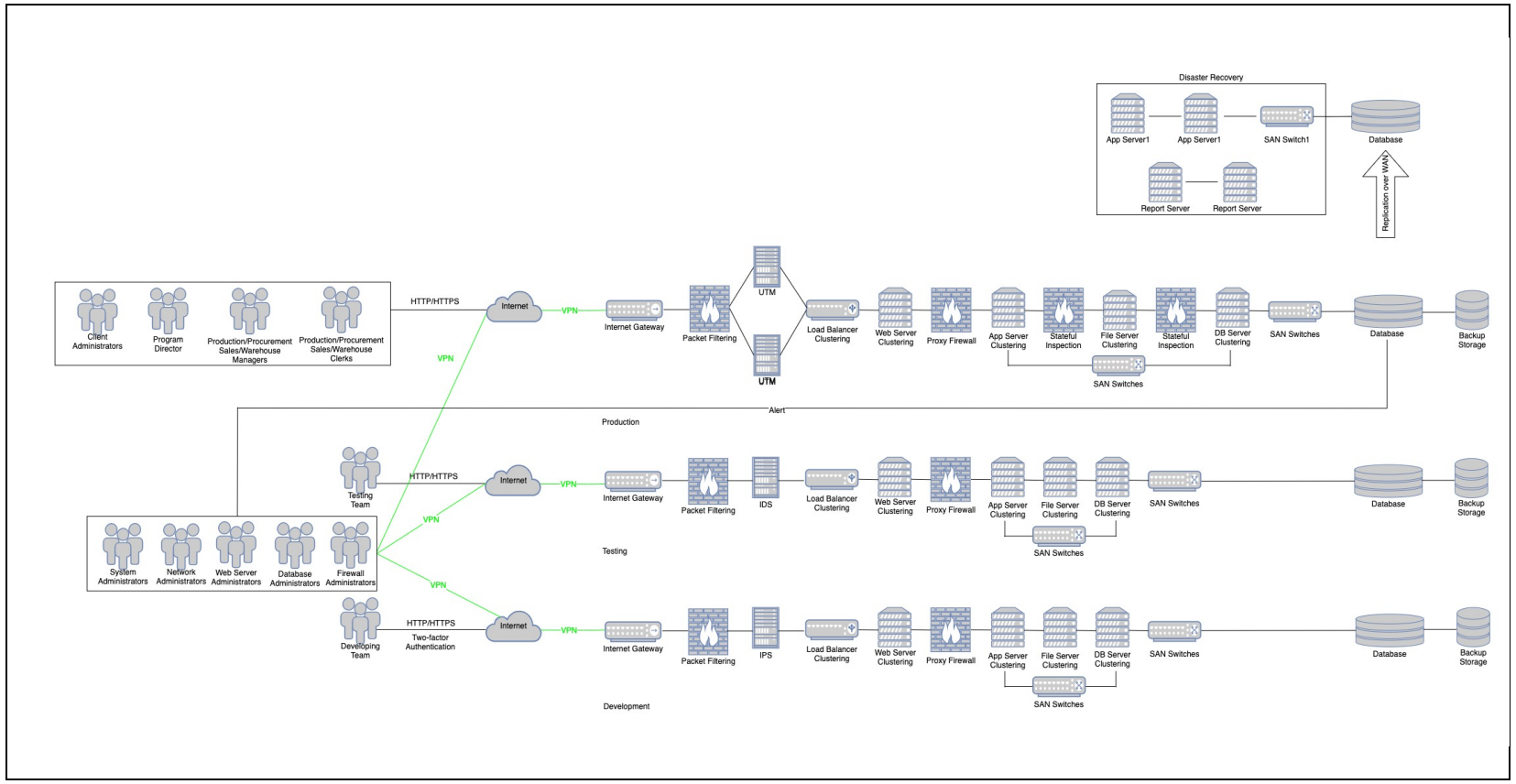
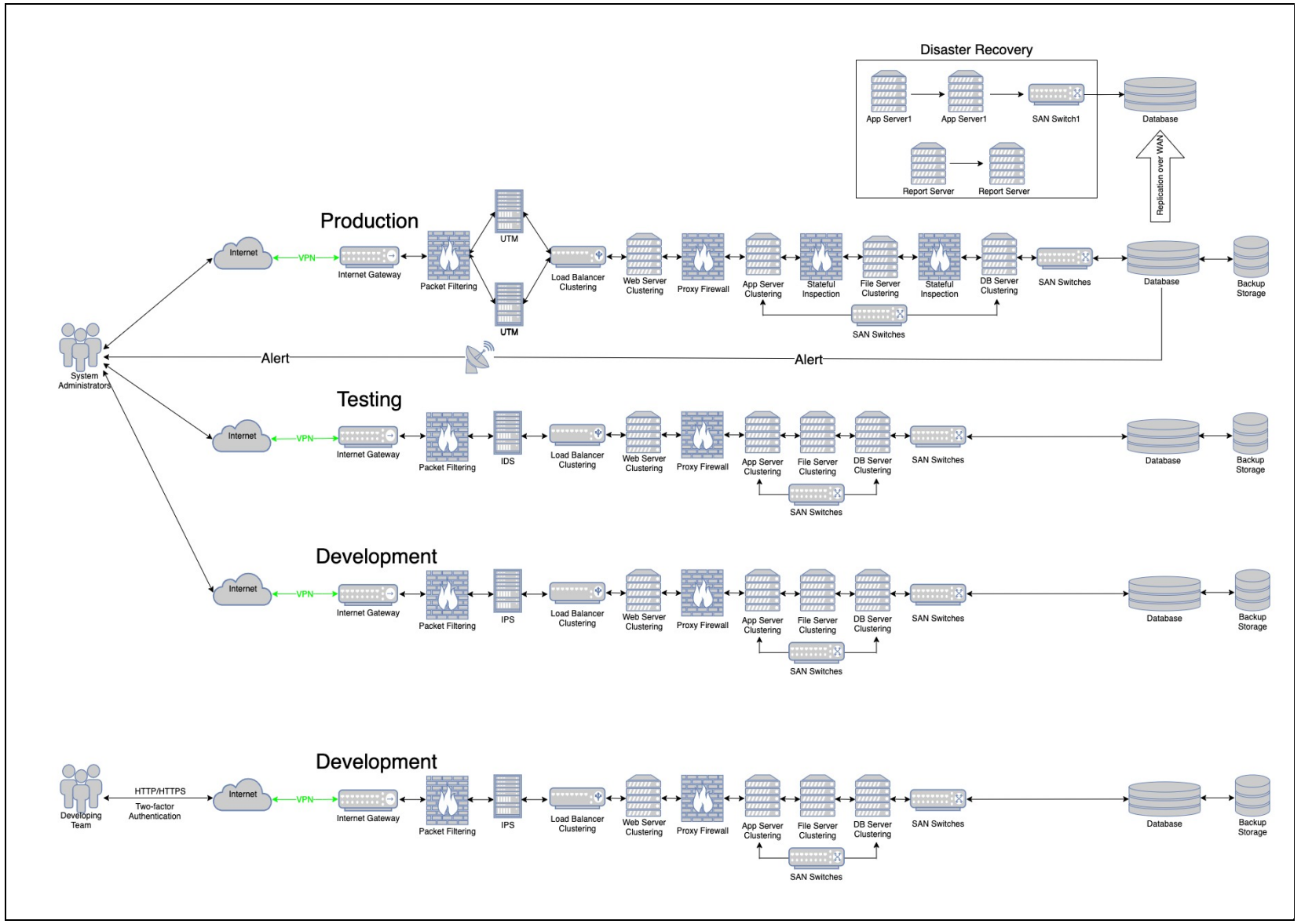


Figure 9-2. Network Diagram

10. SYSTEM ENVIRONMENT AND INVENTORY

Directions for attaching the FedRAMP Inventory Workbook may be found in the following section: Attachment 13, FedRAMP Inventory Workbook. Data Flow

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


Disaster Recovery
App Server1
App Server1
SAN Switch1
Database
Report Server
Report Server
Replication over WAN
Production
Internet
VPN
Internet Gateway
Packet Filtering
UTM
UTM
Load Balancer Clustering
Web Server Clustering
Proxy Firewall
App Server Clustering
Stateful Inspection
File Server Clustering
Stateful Inspection
DB Server Clustering
SAN Switches
Database
Backup Storage
SAN Switches
System Administrators
Alert
Alert
Testing
Internet
VPN
Internet Gateway
Packet Filtering
IDS
Load Balancer Clustering
Web Server Clustering
Proxy Firewall
App Server Clustering
File Server Clustering
DB Server Clustering
SAN Switches
Database
Backup Storage
SAN Switches
Development
Internet
VPN
Internet Gateway
Packet Filtering
IPS
Load Balancer Clustering
Web Server Clustering
Proxy Firewall
App Server Clustering
File Server Clustering
DB Server Clustering
SAN Switches
Database
Backup Storage
SAN Switches
Development
Developing Team
HTTP/HTTPS
Two-factor Authentication
Internet
VPN
Internet Gateway
Packet Filtering
IPS
Load Balancer Clustering
Web Server Clustering
Proxy Firewall
App Server Clustering
File Server Clustering
DB Server Clustering
SAN Switches
Database
Backup Storage
SAN Switches

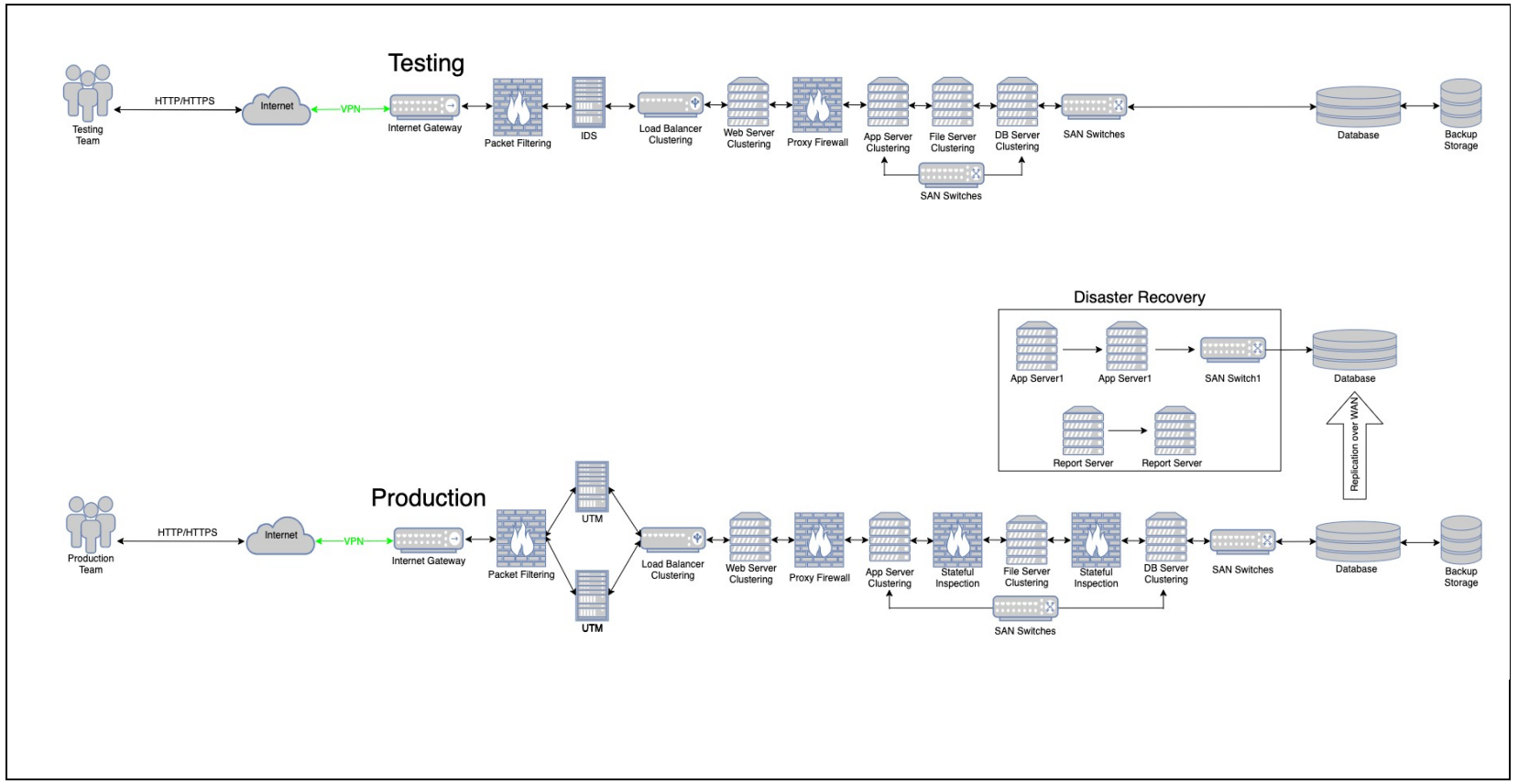


Figure 10-1. Data Flow Diagram

11. SYSTEM INTERCONNECTIONS

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
N/A	Human resources system	Kira 888-888-8888	SSL	outgoing	Personal info (eg: KPI)	N/A
N/A	Finance system	Elva 666-666-6666	SSL	Incoming and outgoing	Financial info (eg: budget, production cost)	N/A
N/A	Administrative system	Alonna 111-111-1111	SSL	Incoming and outgoing	Administrative info	N/A
N/A	Information & Technology Management	Fyo 777-777-7777	SSL	Outgoing	IT info	N/A
N/A	Backup system	Zero 222-222-2222	SSL	Outgoing	All production info	N/A
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>

*Service Processor

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

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 Enter Information System Abbreviation 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

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
AC-22	Publicly Accessible Content	AC-22	AC-22	AC-22
AT	**Awareness and Training**			
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
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 Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	IR-2	IR-2	IR-2 (1) (2)

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
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
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	PE-14	PE-14 (2)	PE-14 (2)

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
	Controls			
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
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	Not Selected	SA-10 (1)	SA-10 (1)

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
	Management			
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
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

ID	Control Description	Sensitivity Level		
		Low	Moderate	High
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.

Instruction: In the sections that follow, describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage and monitor the control. In some cases, the responsibility is shared by a CSP and by the customer. Use the definitions in the table that follows to indicate where each security control originates from.

Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.

For SaaS and PaaS systems that are inheriting controls from an IaaS (or anything lower in the stack), the "inherited" check box must be checked and the implementation description must simply say "inherited." FedRAMP reviewers will determine whether the control-set is appropriate or not.

In Section 13, the NIST term "organization defined" must be interpreted as being the CSP's responsibility unless otherwise indicated. In some cases, the JAB has chosen to define or provide parameters, in others they have left the decision up to the CSP.

Please note: CSPs should not modify the control requirement text, including the parameter assignment instructions and additional FedRAMP requirements. CSP responses must be documented in the "Control Summary Information" and "What is the solution and how is it implemented?" tables.

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

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.

13.3. 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: CISO	
Parameter AU-1(a): system manager	
Parameter AU-1(b)(1): *at every 3 years*	
Parameter AU-1(b)(2): *at least annually*	
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	NIST.SP-800-53r4
Part b	NIST.SP-800-53r4

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*];

(b) 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;

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

(d) 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: System manager	
Parameter AU-2(a): Database server: logging onto/off a system, data deletions, data access, data changes, use of administrator commands, permission changes, capture all security and administrative actions, as well as user activity relative to system Web server: Multiple attempts to log in failed, use of administrator commands, capture all security and administrative actions, as well as user activity relative to system App sever: Multiple attempts to log in failed, use of administrator commands, capture all security and administrative actions, as well as user activity relative to system.	
Parameter AU-2(d): Database server: logging onto/off a system, data deletions, data access, data changes, use of administrator commands, permission changes. Web server: Multiple attempts to log in failed, use of administrator commands App sever: Multiple attempts to log in failed, use of administrator commands	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate	

AU-2	Control Summary Information
☐ 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	

AU-2 What is the solution and how is it implemented?	
Part a	Determine what audit functions of the system include, and provide complete audit contents of the system to the customer
Part b	Agree with third party regulators, auditors on the events about what to be audited.
Part c	Because the system is low-level of sensitivity, the audit events we set up are sufficient to detect the impact on system security.
Part d	Negotiated with the client on the events to be audited, referring to principles.

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: system administrator	
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	

AU-3 What is the solution and how is it implemented?
Summary system log 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 by system admin every day.

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: Database administrator	
Parameter AU-4: Allocates audit record to another storage capacity at every 3 months. Keep in the storage for 5 years.	
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	

AU-4 What is the solution and how is it implemented?
Comply with the policy and procedures of clients for the disposition of historically significant and routine IT management records by system administrators.

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: system administrator	
Parameter AU-5(a): system administrator	
Parameter AU-5(b): overwrite the oldest audit records or automatically shut down	
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	

AU-5 What is the solution and how is it implemented?	
Part a	Send an alert to system administrators within 2 minutes by system admin.
Part b	Overwrite the oldest audit records or automatically shut down; procedures should reflect escalation of priority resolution actions after 3 days.

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: IT auditors	
Parameter AU-6(a)-1: at least monthly	
Parameter AU-6(a)-2: Login in abnormal time, abnormal shutdown, a failed attempt to overstep one's authority, attack firewalls, virus, malware	
Parameter AU-6(b): Information Security Officers	
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	

AU-6 What is the solution and how is it implemented?	
Part a	Review logs on critical systems every month. Examine logs for firewalls, routers, and other network devices shall be time-correlated (to within 1 hour) with logs of other critical systems to determine if any incidents have occurred. Review audit logs for information systems containing PII to determine what data extracts shall be deleted monthly.
Part b	Reports findings to Information Security Officers. Anomalies shall be reported in accordance with incident reporting requirements and procedures.

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: system	
Parameter AU-8(b): 30 second	
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	

AU-8 What is the solution and how is it implemented?	
Part a	Time stamps generated by the information system shall include both the date and time.
Part b	Configure information systems to synchronize the internal system clocks to the authoritative time source when the time difference is greater than 30 seconds.

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: system admin	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate	

AU-9	Control Summary Information
☒ 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	

AU-9 What is the solution and how is it implemented?
Rotate log files to a system other than their source system. Implement cryptographic mechanisms on information systems to protect the integrity of audit information and audit tools. Backup weekly.

AU-11 Audit Record Retention (L) (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: Database admin	
Parameter AU-11: 90 days	
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	

AU-11 What is the solution and how is it implemented?
Archive audit records for a period of no less than one year with 90 days online and the remaining time stored offline. Transfer audit records for remote access devices from the devices to a central log server where they are retained for up to three years.

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: system manager	
Parameter AU-12(a): Desktop and laptop computers (end-user environment), Servers (e.g., file and print, web, firewalls, terminal), Network components (e.g., switches, routers wireless)	
Parameter AU-12(b): Information system owner	
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	

AU-12 What is the solution and how is it implemented?	
Part a	Audit records are to be compiled into a system-wide (logical or physical) audit trail in information system components.
Part b	Information system owner select which auditable events are to be audited by specific components of the information system.
Part c	Generates audit records for the events.

ATTACHMENT 3 DIGITAL IDENTITY WORKSHEET

This Attachment Section has been revised to include the Digital Identity template. Therefore, a separate attachment is not needed. Delete this note and all other instructions from your final version of this document.

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 Level 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 Information System Name (Enter Information System Abbreviation) in accordance with NIST SP 800-63-3.

Table 15-2. Information System Name and Title

Unique Identifier	Information System Name	Information System
233333	FAKE supply chain system	FAKE SCS

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
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 Information System Name 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 10 FIPS 199

This Attachment Section has been revised to include the FIPS 199 Template. Therefore, a separate PTA attachment is not needed. Delete this note and all other instructions from your final version of this document.

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.

Instruction: Insert a brief high-level description of the system, the system environment and the purpose of the system. The description should be consistent with the description found in the System Security Plan (SSP).
Delete this instruction from your final version of this document.

Methodology

Instruction: The CSP should review the NIST Special Publication 800-60 Volume 2 Revision 1 Appendix C Management and Support Information and Information System Impact Levels and Appendix D Impact Determination for Mission-Based Information and Information Systems to assess the recommended impact level for each of the information types. For more information, the CSP should also consult Appendix D.2. After reviewing the NIST guidance on Information Types, the CSP should fill out Table 15-9. CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1.
Delete this instruction from your final version of this document.

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.

Instruction: In the first three columns, put the NIST SP-60 V2 R1 recommended impact level. In the next three columns, put in the CSP determined recommended impact level. If the CSP determined recommended impact level does not match the level recommended by NIST, put in an explanation in the last column as to why this decision was made.
Delete this instruction from your final version of this document.

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
Goods Acquisition Information Type	Low (L)	Low (L)	Low (L)	Moderate (M)	Low (L)	Low (L)	Confidentiality is moderate to protect from unfair access to procurement information before publicly.
Inventory Control Information Type	Low (L)	Low (L)	Low (L)	Low (L)	Low (L)	Moderate (M)	Availability is moderate when emergency requirements to access and distribute materials is necessary for disaster management.
Logistics Management Information Type	Low (L)	Low (L)	Low (L)	Low (L)	Low (L)	Low (L)	Enter text.
Services Acquisition Information Type	Low (L)	Low (L)	Low (L)	Low (L)	Moderate (M)	Low (L)	Unauthorized modification or destruction of information relating to procurement actions

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
							(particularly proposal information) can result in serious disruption of procurement processes and loss of availability of services that can be important or even critical to agency operations.