

Template

StateRAMP System Security Plan (SSP)

Service Provider Name

Information System Name

**VERSION:**

X.X

**DATE:**

YYYYMMDD

This template contains a number of features to facilitate data entry. As you go through the template entering data, you will see prompts for you to enter different types of data.

Repeatable Field

Some multiple-occurring data fields have been linked together and you need only enter the data once. Enter the data once; then click outside the data entry field and all occurrences of that field will be populated. For example, when you see “Information System Abbreviation” and replace it with your system abbreviation, all instances of the abbreviation throughout the document will be replaced with the value you entered. This document contains the following repeatable fields:

Service Provider Name

Information System Name

Version Number

Version Date

Information System Abbreviation

If you find a data field from the above list that has not populated, then press the F9 key to refresh the data. If you make a change to one of the above data fields, you may also have to press the F9 key to refresh the data throughout the document. Remember to save the document after refreshes. The one exception to the repeatable fields is information system names for StateRAMP or leveraged authorizations that are identified as “Leveraged information system name:

Date Selection

Data fields that must contain a date will present a date selection menu.

Item Choice

Data fields that have a limited number of value choices will present a selection list.

Number Entry

Data fields that must have numeric values display “number.”

Text Entry

Many data fields, particularly in tables, that can contain any text display “Enter text” or “Click here to enter text.”

Delete this instruction from your final version of this document.

SYSTEM SECURITY PLAN

Prepared by:

|  |  |  |
| --- | --- | --- |
| Identification of Organization that Prepared this Document | | |
|  | Organization Name | <Enter Company/Organization>. |
| Street Address | <Enter Street Address> |
| Suite/Room/Building | <Enter Suite/Room/Building> |
| City, State Zip | <Enter Zip Code> |

Prepared for:

|  |  |  |
| --- | --- | --- |
| Identification of Cloud Service Provider | | |
|  | Organization Name | <Enter Company/Organization>. |
| Street Address | <Enter Street Address> |
| Suite/Room/Building | <Enter Suite/Room/Building> |
| City, State Zip | <Enter Zip Code> |

Template Revision History

| Date | Description |
| --- | --- |
| 3/31/2021 | Original publication |

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 StateRAMP, or for technical questions about this document including how to use it, contact [*pmo@StateRAMP.org*](mailto:pmo@stateramp.org). For more information about the StateRAMP project, see [www.StateRAMP.org](https://www.stateramp.org/).

TABLE OF CONTENTS

[1. Information System Name/Title 1](#_Toc71710295)

[2. Information System Categorization 1](#_Toc71710296)

[2.1 Information Types 1](#_Toc71710297)

[2.1.1 Category 1 1](#_Toc71710298)

[2.1.2 Category 3 2](#_Toc71710299)

[2.2 Security Objectives Categorization 2](#_Toc71710300)

[2.3 Digital Identity Determination 2](#_Toc71710301)

[3. Information System Owner 3](#_Toc71710302)

[4. Authorizing Official 3](#_Toc71710303)

[5. Other Designated Contacts 3](#_Toc71710304)

[6. Assignment of Security Responsibility 5](#_Toc71710305)

[7. Information System Operational Status 6](#_Toc71710306)

[8. Information System Type 6](#_Toc71710307)

[8.1 Cloud Service Models 6](#_Toc71710308)

[8.2 Cloud Deployment Models 7](#_Toc71710309)

[8.3 Leveraged Authorizations 8](#_Toc71710310)

[9. General System Description 9](#_Toc71710311)

[9.1 System Function or Purpose 9](#_Toc71710312)

[9.2 Information System Components and Boundaries 9](#_Toc71710313)

[9.3 Types of Users 10](#_Toc71710314)

[9.4 Network Architecture 11](#_Toc71710315)

[9.5 Data Flow 12](#_Toc71710316)

[9.6 Ports, Protocols and Services 12](#_Toc71710317)

[10. System Interconnections 14](#_Toc71710318)

[11. Minimum Security Controls 16](#_Toc71710319)

[12. SYSTEM SECURITY PLAN ATTACHMENTS 23](#_Toc71710320)

[13. Attachments 23](#_Toc71710321)

[14. Digital Identity Worksheet 25](#_Toc71710322)

[14.1 Introduction and Purpose 25](#_Toc71710323)

[14.2 Information system name/title 25](#_Toc71710324)

[14.3 Digital Identity Level Definitions 25](#_Toc71710325)

[14.4 Review Maximum Potential Impact Levels 26](#_Toc71710326)

[14.5 Digital Identity Level Selection 27](#_Toc71710327)

[15. PTA and PIA 28](#_Toc71710328)

[15.1 Privacy Overview and Point of Contact (POC) 28](#_Toc71710329)

[15.2 Personally Identifiable Information (PII) 29](#_Toc71710330)

[15.3 Privacy Designation 29](#_Toc71710331)

[15.4 Threshold Analysis 29](#_Toc71710332)

[15.5 Privacy Impact Assessment Talking Points 29](#_Toc71710333)

[15.6 PII Mapping of Components (SE-1, DM-1) 30](#_Toc71710334)

[15.7 Prospective PII Use 31](#_Toc71710335)

[15.8 Sources of PII and Purpose 31](#_Toc71710336)

[15.9 Access to PII and Sharing 31](#_Toc71710337)

[15.10 PII Safeguards and Liabilities 32](#_Toc71710338)

[15.11 Contracts, Agreements, and Ownership 33](#_Toc71710339)

[15.12 Accuracy of the PII and Redress 33](#_Toc71710340)

[15.13 Maintenance and Administrative Controls 33](#_Toc71710341)

[15.14 Business Processes and Technology 34](#_Toc71710342)

[15.15 Privacy Policy 34](#_Toc71710343)

[15.16 SIGNATURES 35](#_Toc71710344)

[16. Security Categorization 36](#_Toc71710345)

[16.1 Instructions 36](#_Toc71710346)

[16.2 Survey Questions 36](#_Toc71710347)

List of Figures

[Figure 9‑2 Network Diagram 11](#_Toc71710373)

[Figure 10‑1 Data Flow Diagram 12](#_Toc71710374)

List of Tables

[Table 1. Information System Name and Title 1](#_Toc71710348)

[Table 2. Security Categorization 1](#_Toc71710349)

[Table 3. Security Impact Level 2](#_Toc71710350)

[Table 4. Baseline Security Configuration 2](#_Toc71710351)

[Table 5. Information System Owner 3](#_Toc71710352)

[Table 6. Information System Management Point of Contact 4](#_Toc71710353)

[Table 7. Information System Technical Point of Contact 4](#_Toc71710354)

[Table 8. CSP Name Internal ISSO (or Equivalent) Point of Contact 5](#_Toc71710355)

[Table 9. AO Point of Contact 5](#_Toc71710356)

[Table 10. System Status 6](#_Toc71710357)

[Table 11. Service Layers Represented in this SSP 7](#_Toc71710358)

[Table 12. Cloud Deployment Model Represented in this SSP 7](#_Toc71710359)

[Table 13. Leveraged Authorizations 8](#_Toc71710360)

[Table 14. Personnel Roles and Privileges 10](#_Toc71710361)

[Table 15 Ports, Protocols, and Services 13](#_Toc71710362)

[Table 16. System Interconnections 14](#_Toc71710363)

[Table 17. Summary of Required Security Controls 16](#_Toc71710364)

[Table 18. Control Origination and Definitions 22](#_Toc71710365)

[Table 19. Names of Provided Attachments 23](#_Toc71710366)

[Table 20. Information System Name and Title 25](#_Toc71710367)

[Table 21. Mapping StateRAMP Levels to NIST SP 800-63-3 Levels 26](#_Toc71710368)

[Table 22. Potential Impacts for Assurance Levels 26](#_Toc71710369)

[Table 23. Digital Identity Level 27](#_Toc71710370)

[Table 24. Information System Name; Privacy POC 28](#_Toc71710371)

[Table 25 PII Mapped to Components 30](#_Toc71710372)

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 | | |
|  | |  | | |

# 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 . Information System Name and Title

| **Unique Identifier** | **Information System Name** | **Information System Abbreviation** |
| --- | --- | --- |
| Enter StateRAMP Package ID | Enter Information System Name | Enter Information System Abbreviation |

# Information System Categorization

The overall information system sensitivity categorization is recorded in Table 2 Security Categorization that follows.

Table . Security Categorization

|  |  |
| --- | --- |
| **System Sensitivity Level:** | Choose level. |

## Information Types

### Category 1

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.

### Category 3

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.

## Security Objectives Categorization

For the <Enter Information System Abbreviation>, default to the high-water mark for the Information Types as identified in Table 3 Security Impact Level below.

Table . Security Impact Level

| **Security Objective** | **Low, Moderate, or High** |
| --- | --- |
| Confidentiality | Choose level. |
| Integrity | Choose level. |
| Availability | Choose level. |

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 4 Baseline Security Configuration that follows.

Table . Baseline Security Configuration

|  |  |
| --- | --- |
| **Enter Information System Abbreviation Security Categorization** | Choose level |

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.

## Digital Identity Determination

The digital identity information may be found in Section 15 – 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 Choose an item.

# Information System Owner

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

Table . 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> |

# Authorizing Official

Instruction: The Authorizing Official is determined by the path that the CSP is using to obtain an authorization.

JAB P-ATO: StateRAMP, JAB, as comprised of member representatives from the General Services Administration (GSA), Department of Defense (DoD) and Department of Homeland Security (DHS). Agency Authority to Operate (ATO): Agency Authorizing Official name, title and contact information. Delete this and all other instructions from your final version of this document.

The Authorizing Official (AO) for this information system is the <Insert AO information as instructed above>.

# Other Designated Contacts

Instruction: AOs should use the following section to identify points of contact that understand the technical implementations of the identified cloud system. AOs should edit, add, or modify the contacts in this section as they see fit.

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

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

Table . 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 . 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> |

# 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 . CSP Name Internal ISSO (or Equivalent) Point of Contact

| **CSP Name Internal ISSO (or Equivalent) 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 . AO Point of Contact

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

# Information System Operational Status

The system is currently in the lifecycle phase shown in Table 10 System Status that follows. (Only operational systems can be granted an ATO).

Table . 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. |

Instruction: Select as many status indicators as apply. If more than one status is selected, list which components of the system are covered under each status indicator.

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

# Information System Type

The <Enter Information System Abbreviation> makes use of unique managed service provider architecture layer(s).

## 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 11 Service Layers Represented in this SSP that follows.

Instruction: Check all layers that apply. Delete this and all other instructions from your final version of this document.

Table . 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.

## 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 StateRAMP Authorizations, are indicated in Table 12 Cloud Deployment Model Represented in this SSP that follows.

Instruction: Check deployment model that applies. Delete this and all other instructions from your final version of this document.

Table . 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. |

## Leveraged Authorizations

Instruction: The StateRAMP program qualifies different service layers for Authorizations. One or multiple service layers can be qualified in one System Security Plan. If a lower level layer has been granted an Authorization and another higher-level layer represented by this SSP plans to leverage a lower layer’s Authorization, this System Security Plan must clearly state that intention.

If an information system does not leverage any pre-existing Authorizations, write “None” in the first column of the table that follows. Add as many rows as necessary in the table that follows. Delete this and all other instructions from your final version of this document.

The <Enter Information System Abbreviation> Choose an item leverages a pre-existing StateRAMP Authorization. StateRAMP Authorizations leveraged by this <Enter Information System Abbreviation> are listed in Table 13 Leveraged Authorizations that follows.

Table . 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> |

# General System Description

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

## System Function or Purpose

Instruction: In the space that follows, describe the purpose and functions of this system. Delete this and all other instructions from your final version of this document.

## Information System Components and Boundaries

Instruction: In the space that follows, provide an explicit definition of the system’s Authorization Boundary. Provide a diagram that portrays this Authorization Boundary and all its connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system. Address all components and managed interfaces of the information system authorized for operation (e.g., routers, firewalls).

The diagram must include a predominant border drawn around all system components and services included in the authorization boundary. The diagram must be easy to read and understand.

Formal names of components as they are known at the service provider organization in functional specifications, configuration guides, other documents and live configurations shall be named on the diagram and described. Components identified in the Boundary diagram should be consistent with the Network diagram and the inventory(ies). Provide a key to symbols used. Ensure consistency between the boundary and network diagrams and respective descriptions (Section 9.2) and the appropriate Security Controls [AC-20, CA-3(1)].

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

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9‑2 Authorization Boundary Diagram below.

|  |
| --- |
|  |

Figure 9‑2 Authorization Boundary Diagram

## 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 14 Personnel Roles and Privileges that follows.

Instruction: For an External User, write “Not Applicable” in the Sensitivity Level Column. This table must include all roles including systems administrators and database administrators as a role types. (Also include web server administrators, network administrators and firewall administrators if these individuals have the ability to configure a device or host that could impact the CSP service offering.)

This table must also include whether these roles are fulfilled by foreign nationals or systems outside the United States. Delete this and all other instructions from your final version of this document.

Table . 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. |  |  |

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.

## Network Architecture

Instruction: Insert a network architectural diagram in the space that follows. Ensure that the following items are labeled on the diagram: hostnames, Domain Name System (DNS) servers, DHCP servers, authentication and access control servers, directory servers, firewalls, routers, switches, database servers, major applications, storage, Internet connectivity providers, telecom circuit numbers, network interfaces and numbers, VLANs. Major security components should be represented. If necessary, include multiple network diagrams.

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

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

## Data Flow

Instruction: In the space that follows, describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. Include data flows for privileged and non-privileged authentication/authorization to the system for internal and external users. If necessary, include multiple data flow diagrams.

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

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

## Ports, Protocols and Services

Table 15 Ports, Protocols, and Services below lists the ports, protocols and services enabled in this information system.

Instruction: In the column labeled “Used By” please indicate the components of the information system that make use of the ports, protocols, and services. In the column labeled “Purpose” indicate the purpose for the service (e.g., system logging, HTTP redirector, load balancing). This table should be consistent with CM-6 and CM-7. You must fill out this table, even if you are leveraging a pre-existing StateRAMP Authorization. Add more rows as needed.

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

Table Ports, Protocols, and Services

| **Ports (TCP/UDP)\*** | **Protocols** | **Services** | **Purpose** | **Used By** |
| --- | --- | --- | --- | --- |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |

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

# System Interconnections

Instruction: List all interconnected systems. Provide the IP address and interface identifier (eth0, eth1, eth2) for the CSP system that provides the connection. Name the external organization and the IP address of the external system. Provide a point of contact and phone number for the external organization.

For Connection Security indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number. Add additional rows as needed.

Table . 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 |
| --- | --- | --- | --- | --- | --- | --- |
| <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> |
| <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> |
| <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> |
| <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> |
| <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> |
| <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)

# Minimum Security Controls

Security controls must meet minimum security control baseline requirements. Upon categorizing a system as Category 1,2, or 3 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 StateRAMP 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.

A summary of which security standards pertain to which sensitivity level is found in Table 17 Summary of Required Security Controls that follows.

Table . Summary of Required Security Controls

| ID | Control Description | Impact Level | | |
| --- | --- | --- | --- | --- |
| Category 1 | | Category 3 |
| **AC** | | | | |
| AC-1 | Access Control Policy and Procedures | AC-1 | | AC-1 |
| AC-2 | Account Management | AC-2 | | AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12) |
| AC-3 | Access Enforcement | AC-3 | | AC-3 |
| AC-4 | Information Flow Enforcement | Not Selected | | AC-4 (21) |
| AC-5 | Separation of Duties | Not Selected | | AC-5 |
| AC-6 | Least Privilege | Not Selected | | AC-6 (1) (2) (5) (9) (10) |
| AC-7 | Unsuccessful Logon Attempts | AC-7 | | AC-7 |
| AC-8 | System Use Notification | AC-8 | | AC-8 |
| AC-10 | Concurrent Session Control | Not Selected | | AC-10 |
| AC-11 | Session Lock | Not Selected | | AC-11 (1) |
| AC-12 | Session Termination | Not Selected | | AC-12 |
| AC-14 | Permitted Actions Without Identification or Authentication | AC-14 | | AC-14 |
| AC-17 | Remote Access | AC-17 | | AC-17 (1) (2) (3) (4) (9) |
| AC-18 | Wireless Access | AC-18 | | AC-18 (1) |
| AC-19 | Access Control For Mobile Devices | AC-19 | | AC-19 (5) |
| AC-20 | Use of External Information Systems | AC-20 | | AC-20 (1) (2) |
| AC-21 | Information Sharing | Not Selected | | AC-21 |
| AC-22 | Publicly Accessible Content | AC-22 | | AC-22 |
| **AT** |
| AT-1 | Security Awareness and Training Policy and Procedures | AT-1 | | AT-1 |
| AT-2 | Security Awareness Training | AT-2 | | AT-2 (2) |
| AT-3 | Role-Based Security Training | AT-3 | | AT-3 |
| AT-4 | Security Training Records | AT-4 | | AT-4 |
| **AU** |
| AU-1 | Audit and Accountability Policy and Procedures | AU-1 | | AU-1 |
| AU-2 | Audit Events | AU-2 | | AU-2 (3) |
| AU-3 | Content of Audit Records | AU-3 | | AU-3 (1) |
| AU-4 | Audit Storage Capacity | AU-4 | | AU-4 |
| AU-5 | Response to Audit Processing Failures | AU-5 | | AU-5 |
| AU-6 | Audit Review, Analysis and Reporting | AU-6 | | AU-6 (1) (3) |
| AU-7 | Audit Reduction and Report Generation | Not Selected | | AU-7 (1) |
| AU-8 | Time Stamps | AU-8 | | AU-8 (1) |
| AU-9 | Protection of Audit Information | AU-9 | | AU-9 (2) (4) |
| AU-10 | Non-repudiation | Not Selected | | Not Selected |
| AU-11 | Audit Record Retention | AU-11 | | AU-11 |
| AU-12 | Audit Generation | AU-12 | | AU-12 |
| **CA** |
| CA-1 | Security Assessment and Authorization Policies and Procedures | CA-1 | | CA-1 |
| CA-2 | Security Assessments | CA-2 (1) | | CA-2 (1) (2) (3) |
| CA-3 | System Interconnections | CA-3 | | CA-3 (3) (5) |
| CA-5 | Plan of Action and Milestones | CA-5 | | CA-5 |
| CA-6 | Security Authorization | CA-6 | | CA-6 |
| CA-7 | Continuous Monitoring | CA-7 | | CA-7 (1) |
| CA-8 | Penetration Testing | Not Selected | | CA-8 (1) |
| CA-9 | Internal System Connections | CA-9 | | CA-9 |
| **CM** |
| CM-1 | Configuration Management Policy and Procedures | CM-1 | | CM-1 |
| CM-2 | Baseline Configuration | CM-2 | | CM-2 (1) (2) (3) (7) |
| CM-3 | Configuration Change Control | Not Selected | | CM-3 (2) |
| CM-4 | Security Impact Analysis | CM-4 | | CM-4 |
| CM-5 | Access Restrictions For Change | Not Selected | | CM-5 (1) (3) (5) |
| CM-6 | Configuration Settings | CM-6 | | CM-6 (1) |
| CM-7 | Least Functionality | CM-7 | | CM-7 (1) (2) (5)\* |
| CM-8 | Information System Component Inventory | CM-8 | | CM-8 (1) (3) (5) |
| CM-9 | Configuration Management Plan | Not Selected | | CM-9 |
| CM-10 | Software Usage Restrictions | CM-10 | | CM-10 (1) |
| CM-11 | User-Installed Software | CM-11 | | CM-11 |
| **CP** |
| CP-1 | Contingency Planning Policy and Procedures | CP-1 | | CP-1 |
| CP-2 | Contingency Plan | CP-2 | | CP-2 (1) (2) (3) (8) |
| CP-3 | Contingency Training | CP-3 | | CP-3 |
| CP-4 | Contingency Plan Testing | CP-4 | | CP-4 (1) |
| CP-6 | Alternate Storage Site | Not Selected | | CP-6 (1) (3) |
| CP-7 | Alternate Processing Site | Not Selected | | CP-7 (1) (2) (3) |
| CP-8 | Telecommunications Services | Not Selected | | CP-8 (1) (2) |
| CP-9 | Information System Backup | CP-9 | | CP-9 (1) (3) |
| CP-10 | Information System Recovery and Reconstitution | CP-10 | | CP-10 (2) |
| **IA** |
| IA-1 | Identification and Authentication Policy and Procedures | 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-3 | Device Identification and Authentication | Not Selected | | IA-3 |
| IA-4 | Identifier Management | IA-4 | | IA-4 (4) |
| IA-5 | Authenticator Management | IA-5 (1) (11) | | IA-5 (1) (2) (3) (4) (6) (7) (11) |
| IA-6 | Authenticator Feedback | IA-6 | | IA-6 |
| IA-7 | Cryptographic Module Authentication | IA-7 | | IA-7 |
| IA-8 | Identification and Authentication (Non-Organizational Users) | IA-8 (1) (2) (3) (4) | | IA-8 (1) (2) (3) (4) |
| **IR** |
| IR-1 | Incident Response Policy and Procedures | IR-1 | | IR-1 |
| IR-2 | Incident Response Training | IR-2 | | IR-2 |
| IR-3 | Incident Response Testing | Not Selected | | IR-3 (2) |
| IR-4 | Incident Handling | IR-4 | | IR-4 (1) |
| IR-5 | Incident Monitoring | IR-5 | | IR-5 |
| IR-6 | Incident Reporting | IR-6 | | IR-6 (1) |
| IR-7 | Incident Response Assistance | IR-7 | | IR-7 (1) (2) |
| IR-8 | Incident Response Plan | IR-8 | | IR-8 |
| IR-9 | Information Spillage Response | Not Selected | | IR-9 (1) (2) (3) (4) |
| **MA** |
| MA-1 | System Maintenance Policy and Procedures | MA-1 | | MA-1 |
| MA-2 | Controlled Maintenance | MA-2 | | MA-2 |
| MA-3 | Maintenance Tools | Not Selected | | MA-3 (1) (2) (3) |
| MA-4 | Nonlocal Maintenance | MA-4 | | MA-4 (2) |
| MA-5 | Maintenance Personnel | MA-5 | | MA-5 (1) |
| MA-6 | Timely Maintenance | Not Selected | | MA-6 |
| **MP** |
| MP-1 | Media Protection Policy and Procedures | MP-1 | | MP-1 |
| MP-2 | Media Access | MP-2 | | MP-2 |
| MP-3 | Media Marking | Not Selected | | MP-3 |
| MP-4 | Media Storage | Not Selected | | MP-4 |
| MP-5 | Media Transport | Not Selected | | MP-5 (4) |
| MP-6 | Media Sanitization | MP-6 | | MP-6 (2) |
| MP-7 | Media Use | MP-7 | | MP-7 (1) |
| **PE** |
| PE-1 | Physical and Environmental Protection Policy and Procedures | PE-1 | | PE-1 |
| PE-2 | Physical Access Authorizations | PE-2 | | PE-2 |
| PE-3 | Physical Access Control | PE-3 | | PE-3 |
| PE-4 | Access Control For Transmission Medium | Not Selected | | PE-4 |
| PE-5 | Access Control For Output Devices | Not Selected | | PE-5 |
| PE-6 | Monitoring Physical Access | PE-6 | | PE-6 (1) |
| PE-8 | Visitor Access Records | PE-8 | | PE-8 |
| PE-9 | Power Equipment and Cabling | Not Selected | | PE-9 |
| PE-10 | Emergency Shutoff | Not Selected | | PE-10 |
| PE-11 | Emergency Power | Not Selected | | PE-11 |
| PE-12 | Emergency Lighting | PE-12 | | PE-12 |
| PE-13 | Fire Protection | PE-13 | | PE-13 (2) (3) |
| PE-14 | Temperature and Humidity Controls | PE-14 | | PE-14 (2) |
| PE-15 | Water Damage Protection | PE-15 | | PE-15 |
| PE-16 | Delivery and Removal | PE-16 | | PE-16 |
| PE-17 | Alternate Work Site | Not Selected | | PE-17 |
| PE-18 | Location of Information System Components | Not Selected | | Not Selected |
| **PL** |
| PL-1 | Security Planning Policy and Procedures | PL-1 | | PL-1 |
| PL-2 | System Security Plan | PL-2 | | PL-2 (3) |
| PL-4 | Rules of Behavior | PL-4 | | PL-4 (1) |
| PL-8 | Information Security Architecture | Not Selected | | PL-8 |
| **PS** |
| PS-1 | Personnel Security Policy and Procedures | PS-1 | | PS-1 |
| PS-2 | Position Risk Designation | PS-2 | | PS-2 |
| PS-3 | Personnel Screening | PS-3 | | PS-3 (3) |
| PS-4 | Personnel Termination | PS-4 | | PS-4 |
| PS-5 | Personnel Transfer | PS-5 | | PS-5 |
| PS-6 | Access Agreements | PS-6 | | PS-6 |
| PS-7 | Third-Party Personnel Security | PS-7 | | PS-7 |
| PS-8 | Personnel Sanctions | PS-8 | | PS-8 |
| **RA** |
| RA-1 | Risk Assessment Policy and Procedures | RA-1 | | RA-1 |
| RA-2 | Security Categorization | RA-2 | | RA-2 |
| RA-3 | Risk Assessment | RA-3 | | RA-3 |
| RA-5 | Vulnerability Scanning | RA-5 | | RA-5 (1) (2) (3) (5) (6) (8) |
| **SA** |
| SA-1 | System and Services Acquisition Policy and Procedures | SA-1 | | SA-1 |
| SA-2 | Allocation of Resources | SA-2 | | SA-2 |
| SA-3 | System Development Life Cycle | SA-3 | | SA-3 |
| SA-4 | Acquisition Process | SA-4 (10) | | SA-4 (1) (2) (8) (9) (10) |
| SA-5 | Information System Documentation | SA-5 | | SA-5 |
| SA-8 | Security Engineering Principles | Not Selected | | SA-8 |
| SA-9 | External Information System Services | SA-9 | | SA-9 (1) (2) (4) (5) |
| SA-10 | Developer Configuration Management | Not Selected | | SA-10 (1) |
| SA-11 | Developer Security Testing and Evaluation | Not Selected | | SA-11 (1) (2) (8) |
| SA-12 | Supply Chain Protection | Not Selected | | Not Selected |
| SA-15 | Development Process, Standards and Tools | Not Selected | | Not Selected |
| SA-16 | Developer-Provided Training | Not Selected | | Not Selected |
| SA-17 | Developer Security Architecture and Design | Not Selected | | Not Selected |
| **SC** |
| SC-1 | System and Communications Protection Policy and Procedures | | SC-1 | SC-1 |
| SC-2 | Application Partitioning | | Not Selected | SC-2 |
| SC-3 | Security Function Isolation | | Not Selected | Not Selected |
| SC-4 | Information In Shared Resources | | Not Selected | SC-4 |
| SC-5 | Denial of Service Protection | | SC-5 | SC-5 |
| SC-6 | Resource Availability | | Not Selected | SC-6 |
| SC-7 | Boundary Protection | | SC-7 | SC-7 (3) (4) (5) (7) (8) (12) (13) (18) |
| SC-8 | Transmission Confidentiality and Integrity | | Not Selected | SC-8 (1) |
| SC-10 | Network Disconnect | | Not Selected | SC-10 |
| SC-12 | Cryptographic Key Establishment and Management | | SC-12 | SC-12 (2) (3) |
| SC-13 | Cryptographic Protection | | SC-13 | SC-13 |
| SC-15 | Collaborative Computing Devices | | SC-15 | SC-15 |
| SC-17 | Public Key Infrastructure Certificates | | Not Selected | SC-17 |
| SC-18 | Mobile Code | | Not Selected | SC-18 |
| SC-19 | Voice Over Internet Protocol | | Not Selected | SC-19 |
| SC-20 | Secure Name / Address Resolution Service (Authoritative Source) | | SC-20 | SC-20 |
| SC-21 | Secure Name / Address Resolution Service (Recursive or Caching Resolver) | | SC-21 | SC-21 |
| SC-22 | Architecture and Provisioning for Name / Address Resolution Service | | SC-22 | SC-22 |
| SC-23 | Session Authenticity | | Not Selected | SC-23 |
| SC-24 | Fail in Known State | | Not Selected | Not Selected |
| SC-28 | Protection of Information At Rest | | Not Selected | SC-28 (1) |
| SC-39 | Process Isolation | | SC-39 | SC-39 |
| **SI** |
| SI-1 | System and Information Integrity Policy and Procedures | | SI-1 | SI-1 |
| SI-2 | Flaw Remediation | | SI-2 | SI-2 (2) (3) |
| SI-3 | Malicious Code Protection | | SI-3 | SI-3 (1) (2) (7) |
| SI-4 | Information System Monitoring | | SI-4 | SI-4 (1) (2) (4) (5) (14) (16) (23) |
| SI-5 | Security Alerts, Advisories and Directives | | SI-5 | SI-5 |
| SI-6 | Security Function Verification | | Not Selected | SI-6 |
| SI-7 | Software, Firmware, and Information Integrity | | Not Selected | SI-7 (1) (7) |
| SI-8 | Spam Protection | | Not Selected | SI-8 (1) (2) |
| SI-10 | Information Input Validation | | Not Selected | SI-10 |
| SI-11 | Error Handling | | Not Selected | SI-11 |
| SI-12 | Information Handling and Retention | | SI-12 | SI-12 |
| SI-16 | Memory Protection | | SI-16 | SI-16 |

The definitions in Table 18 Control Origination and Definitions indicate where each security control originates.

Table . 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 StateRAMP Authorization | A control that is inherited from another CSP Name system that has already received a StateRAMP Authorization. | A PaaS or SaaS provider inherits PE controls from an IaaS provider. |

# SYSTEM SECURITY PLAN ATTACHMENTS

Instruction: Attach any documents that are referred to in the Information System Name (Enter Information System Abbreviation) System Security Plan. Documents and attachments should, provide the title, version, and exact file name, including the file extension. All attachments and associated documents must be delivered separately. No embedded documents will be accepted.

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

# Attachments

A recommended attachment file naming convention is <information system abbreviation> <attachment identifier> <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 19 to describe the attachments provided. Make only the following additions/changes to Table 19:

* The first item, Information Security Policies and Procedures (ISPP) may be fulfilled by multiple documents. If that is the case, add lines to Table 19. Attachment File Naming Convention to differentiate between them using the “xx” portion of the File Name. Enter Information System Abbreviation 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 19. Names of Provided Attachments. (Information System Abbreviation, attachment number, document abbreviation, version number)

Table . Names of Provided Attachments

| **Attachment** | **File Name** | **StateRAMP Template Required?** |
| --- | --- | --- |
| **SSP Operations Matrix**  **(Includes Control Implementations, CIS Matrix, Inventory Workbook, Laws & Regulations)** | Information System Abbreviation\_SSP\_A\_OPM\_V#\_YYYYMMDD | Yes |
| **Information Security Policies** | Information System Abbreviation\_Control Family Name\_POL\_V#\_YYYYMMDD | No |
| **Information Security Procedures** | Information System Abbreviation\_Control Family Name\_PROC\_V#\_YYYYMMDD | No |
| **Configuration Management Plan** | Information System Abbreviation\_SSP\_A\_CMP\_V#\_YYYYMMDD | Yes |
| **Information System Contingency Plan** | Information System Abbreviation\_SSP\_A\_ISCP\_V#\_YYYYMMDD | Yes |
| **Incident Response Plan** | Information System Abbreviation\_SSP\_A\_IRP\_V#\_YYYYMMDD | Yes |
| **Rules of Behavior** | Information System Abbreviation\_SSP\_A\_ROB\_V#\_YYYYMMDD | Yes |
| **Separation of Duties Matrix** | Information System Abbreviation\_SSP\_A\_SDM\_V#\_YYYYMMDD | No |
| **User Guide** | Information System Abbreviation\_SSP\_A\_UG\_V#\_YYYYMMDD | No |
| **Continuous Monitoring Plan** | Information System Abbreviation\_SSP\_A\_ConMon\_V#\_YYYYMMDD | Yes |

# 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 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](https://pages.nist.gov/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 . Information System Name and Title

| **Unique Identifier** | **Information System Name** | **Information System Abbreviation** |
| --- | --- | --- |
| Enter StateRAMP Application Number. |  | Enter Information System Abbreviation |

## 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 Digital Identity levels below. StateRAMP maps its system categorization levels to NIST 800-63-3’s levels as shown in Table 21.

* 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).

Table . Mapping StateRAMP Levels to NIST SP 800-63-3 Levels

| StateRAMP 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 |
| Category 3 | 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 |
| Category 1 | 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 22 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 . Potential Impacts for Assurance Levels

|  | **Assurance Level Impact Profile** | | |
| --- | --- | --- | --- |
| **Potential Impact Categories** | **1** | **2** | **3** |
| Inconvenience, distress, or damage to standing or reputation | Category 1 | Category 3 | High |
| Financial loss or agency liability | Category 1 | Category 3 | High |
| Harm to agency programs or public interests | N/A | Category 1/3 | High |
| Unauthorized release of sensitive information | N/A | Category 1/3 | High |
| Personal Safety | N/A | Category 1 | Mod/High |
| Civil or criminal violations | N/A | Category 1/3 | High |

## Digital Identity Level Selection

Instruction: Select the lowest level that will cover all potential impact identified from Table 22 Potential Impacts for Assurance Levels.

Delete this instruction from your final version of this document.

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 23 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 . Digital Identity Level

| **Digital Identity Level** | **Maximum Impact Profile** | **Selection** |
| --- | --- | --- |
| Level 1: AAL1, IAL1, FAL1 | Category 1 |  |
| Level 2: AAL2, IAL2, FAL2 | Category 3 |  |
| Other |  |  |

# PTA and PIA

This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA/PIA attachment is not needed. If any of the answers to Question 1-4 are “Yes” then complete the Privacy Impact Assessment.

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

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 StateRAMP website. The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues.

## Privacy Overview and Point of Contact (POC)

The Table 24 Information System Name; Privacy POC individual is identified as the Information System Name; Privacy Officer and POC for privacy at CSP Name.

Table . Information System Name; 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. |

## 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
* Voice recordings

PII refers to information that can be traced back to an individual person.

## Privacy Designation

Service providers perform an annual analysis to determine if PII is collected by any of the system components. Clouds that do not collect PII and would like to opt-out of hosting privacy information may elect to do so and are not required to fill out the Privacy Impact Assessment Questions. If a CSP is willing to host PII, the Privacy Impact Assessment Questions should be answered given the current knowledge of the CSP. A CSP is not required to solicit customers for the information.

Cloud customers (data owner/system owners) are required to perform their own Privacy Impact Assessments and may share this information with the CSP if they so desire (for informational purposes and/or to work with the CSP to develop processes and procedures for managing their PII).

## Threshold Analysis

Check one.

|  |  |
| --- | --- |
|  | Opt-out. This cloud will not host privacy information. |
|  | This cloud is willing to host privacy information.  Select the cloud layers that are represented by <System Name>. Select all that apply. |
|  | This cloud includes Software as a Service (SaaS). |
|  | This cloud includes Platform as a Service (PaaS). |
|  | This cloud includes Infrastructure as a Service (IaaS). |

## Privacy Impact Assessment Talking Points

According to NIST SP 800-122, Appendix D, there must be no personal data record-keeping systems whose very existence is secret. Additionally, NIST SP 800-122, Appendix D states, “There should be a general policy of openness about developments, practices, and policies with respect to personal data.” Means should be readily available to establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

In light of the NIST guidance, Privacy Impact Assessment talking points have been developed for the purpose of ensuring full disclosure between stakeholders. Identifiers in parenthesis after a section title indicate NIST SP 800-53, controls that are related to the particular talking point. These mapping to Appendix J privacy controls are not considered a replacement for Appendix J controls.

## PII Mapping of Components (SE-1, DM-1)

<Information System Name> consists of <Enter Number> key components. Each component has been analyzed to determine if any elements of that component collect and/or store PII. The type of PII collected and/or stored by System Name and the functions that collect it are recorded in Table 25.

Table PII Mapped to Components

| **Components** | **Does this Component Collect or Store PII?**  **(Yes/No)** | **Type of PII** | **Reason for Collection of PII** | **Safeguards** |
| --- | --- | --- | --- | --- |
| Click here to enter text. | Select One | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Select One | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Select One | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Select One | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Select One | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Select One | Click here to enter text. | Click here to enter text. | Click here to enter text. |

## Prospective PII Use

Respond to the following questions:

|  |  |  |
| --- | --- | --- |
| 1. Are there any data fields in the platform or application that have been targeted for the collection or storage of PII? If yes, please name those fields. (SE-1, DM-1, IP-1) | | |
| Click here to enter explanation. | | |
| If PII fields are used, can individuals “opt-out” of PII fields by declining to provide PII or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)? (IP-1) | | |
| Click here to enter explanation. | | |
|  | Yes | Explain the circumstances of being able to opt-out of PII fields (either for specific data elements or specific uses of the data). (IP-1) |
|  |  | Click here to enter explanation. |
|  | No | It is not possible to opt-out. |

## Sources of PII and Purpose

1. Does CSP Name have knowledge of existing federal agencies that provide PII that gets imported into the system? (AP-2)

|  |
| --- |
| Click here to enter explanation. |

1. Has any agency that is known to provide PII to the system provided a stated purpose for populating the system with PII? (AP-1, AP-2)

|  |
| --- |
| Click here to enter explanation. |

1. Does CSP Name currently populate the system with PII? If yes, where does the PII come from and what is the purpose? (AP-1, AP-2)

|  |
| --- |
| Click here to enter explanation. |

1. Will any third party sources be providing PII that will be imported into the system (if known)? Please explain. (AP-1, AP-2)

|  |
| --- |
| Click here to enter explanation. |

## Access to PII and Sharing

1. What third-party organizations will have access to the PII (if known)? Who establishes the criteria for what PII can be shared? (AP-1, AP-2, AR-8, IP-1, UL-2)

|  |
| --- |
| Click here to enter explanation. |

1. What CSP Name personnel roles will have access to PII fields (e.g., users, managers, system administrators, developers, contractors, other)? Explain the need for CSP Name personnel to have access to the PII. (AR-8, UL-2)

|  |
| --- |
| Click here to enter explanation. |

1. For CSP support staff, how is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access to PII require manager approval? (IP-2)

|  |
| --- |
| Click here to enter explanation. |

1. Do other systems that interconnect to the system share, transmit, or access the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing of PII. (UL-2)

|  |
| --- |
| Click here to enter explanation. |

## PII Safeguards and Liabilities

1. What controls are in place to prevent the misuse (e.g., browsing) of PII by those having access? (AR-2)

|  |
| --- |
| Click here to enter explanation. |

1. Who will be responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or shared on the system? Have policies and/or procedures been established for this responsibility and accountability? (AR-1, AR-2)

|  |
| --- |
| Click here to enter explanation. |

1. Does the CSP Name provide annual security training include privacy training? Does CSP Name require their contractors that have access to the PII to take the training? (AR-5)

|  |
| --- |
| Click here to enter explanation. |

1. Who is privacy officer responsible for assuring safeguards for the PII? (AR-1)

|  |
| --- |
| Click here to enter explanation. |

1. What is the magnitude of harm to the individuals if privacy related data is disclosed, intentionally or unintentionally? (AR-2)

|  |
| --- |
| Click here to enter explanation. |

1. What involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system? (AR-3)

|  |
| --- |
| Click here to enter explanation. |

1. Is the PII owner advised about what federal agencies or other organizations share or have access to the data? (AR-1)

|  |
| --- |
| Click here to enter explanation. |

## Contracts, Agreements, and Ownership

1. NIST SP 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this accountability described in contracts with customers? Why or why not? (AR-3)

|  |
| --- |
| Click here to enter explanation. |

1. Do contracts with customers establish who has ownership rights over data including PII? (AR-2, AR-3)

|  |
| --- |
| Click here to enter explanation. |

1. Do contracts with customers require that customers notify CSP Name if the customer intends to populate the service platform with PII? Why or why not? (AR-3)

|  |
| --- |
| Click here to enter explanation. |

1. Do CSP Name contracts with customers establish record retention responsibilities for both the customer and CSP Name? (AR-2, AR-3)

|  |
| --- |
| Click here to enter explanation. |

1. Is the degree to which CSP Name will accept liability for exposure of PII clearly defined in agreements with customers? (AR-3)

|  |
| --- |
| Click here to enter explanation. |

## Accuracy of the PII and Redress

1. Is the PII collected verified for accuracy? Why or why not? (DI-1)

|  |
| --- |
| Click here to enter explanation. |

1. Is the PII current? How is this determined? (DI-1)

|  |
| --- |
| Click here to enter explanation. |

1. Is there a process for individuals to have inaccurate PII that is maintained by the system corrected or amended, as appropriate?

|  |
| --- |
| Click here to enter explanation. |

## Maintenance and Administrative Controls

1. If the system is operated in more than one site, how is consistent use of the PII maintained in all sites? Are the same controls used?

|  |
| --- |
| Click here to enter explanation. |

1. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? (AR-2, AR-3, DM-2)

|  |
| --- |
| Click here to enter explanation. |

1. What are the procedures for disposition of the PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the decommissioning procedures? (AR-2, DM-2)

|  |
| --- |
| Click here to enter explanation. |

1. Is the system using new technologies that contain PII in ways that have not previously deployed? (e.g., smart cards, caller-ID, biometrics, PIV cards, etc.)?

|  |
| --- |
| Click here to enter explanation. |

1. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology?

|  |
| --- |
| Click here to enter explanation. |

1. Is access to the PII being monitored, tracked, or recorded? (AR-4)

|  |
| --- |
| Click here to enter explanation. |

1. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision? (TR-2)

|  |
| --- |
| Click here to enter explanation. |

## Business Processes and Technology

1. Have the talking points found herein resulted in circumstances that requires changes to business processes?

|  |
| --- |
| Click here to enter explanation. |

1. Does the outcome of these talking points require that technology or operational changes be made to the system?

|  |
| --- |
| Click here to enter explanation. |

## Privacy Policy

1. Is there a system privacy policy and is it provided to all individuals whose PII you collect, maintain or store? (IP-1, TR-1, TR-3)

|  |
| --- |
| Click here to enter explanation. |

1. Is the privacy policy publicly viewable? If yes, provide the URL. (TR-1, TR-3)

|  |
| --- |
| Click here to enter explanation. |

## SIGNATURES

The information found herein has been documented by *Name of organization* and has been reviewed by the CSP Name, Chief Privacy Officer for accuracy.

|  |  |  |  |
| --- | --- | --- | --- |
| Assessor Signature | | | |
| Name | Enter Name | Date | Select date. |

|  |  |  |  |
| --- | --- | --- | --- |
| Chief Privacy Officer Signature | | | |
| Name | Enter Name | Date | Select date. |

# Security Categorization

This document is intended to be used by state governments and procurement officials as a tool for determining the appropriate StateRAMP or FedRAMP security requirements in a request for proposal (RFP) with the intent of procuring a service provider using or offering IaaS, SaaS, and/or PaaS solutions that process, store, and/or transmit government data including PII, PHI, and/or PCI.

According to the Federal Information Security Management Act (FISMA) requirements, there are three distinct security objectives for information and information systems: confidentiality, integrity, and availability. These standards are used as the foundation to ensure service providers are providing solutions that meet the minimum-security requirements to process, store, and transmit certain types of government data.

It is necessary for States to accurately determine their required security baseline prior to publishing an RFP so that the State can select a service provider that meets the State’s needs and provides the appropriate security controls to protect the State’s data. This data classification self-assessment is based on the NIST 800-53 Revision 4 requirements and designed to help state and local governments easily identify the appropriate StateRAMP security category to include in an RFP.

## Instructions

Answer the questions in the survey section to determine what StateRAMP security category requirements you need to include in your RFP to ensure your data is protected. Because of the level of reciprocity between StateRAMP and FedRAMP, a StateRAMP Category 1 requirement is equivalent to a FedRAMP Low Impact and a StateRAMP Category 3 requirement is equivalent to a FedRAMP Moderate Impact.

## Survey Questions

1. Will the service provider process, transmit, and/or store non-sensitive State data, metadata, and/or data that may be released to the public that requires no additional levels of protection?
   1. If yes, StateRAMP Category 1 is required.
2. Will the service provider process, transmit, and/or store personally identifiable information (PII) as defined by the U.S. Department of Labor (DOL)?
   1. If yes, StateRAMP Category 3 is required.
3. Will the service provider process, transmit, and/or store protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA)?
   1. If yes, StateRAMP Category 3 is required.
4. Will the service provider process, transmit, and/or store payment card industry (PCI) data as defined by the PCI Security Standards Council (PCI SSC)?
   1. If yes, StateRAMP Category 3 is required.
5. Will the loss or unavailability of the data that is processed, transmitted, and/or stored by the service provider result in a disruption to government operations?
   1. If yes, StateRAMP Category 3 is required.
6. Will the loss or unavailability of the data that is processed, transmitted, and/or stored by the service provider result in a loss of confidence or trust in the government?
   1. If yes, StateRAMP Category 3 is required.
7. Will the service provider process, transmit, and/or store criminal justice information (CJI), foreign affairs information, federal critical infrastructure information, national security information, and/or global trade information?
   1. If yes, FedRAMP High Impact is required.