|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  |  | |  |
|  | FedRAMP® {{SSP|SECURITYPLAN.OVERALLCATEGORIZATION}} Baseline System Security Plan (SSP)  for {{SSP|SECURITYPLAN.CSPORGNAME}}  {{SSP|SECURITYPLAN.SYSTEMNAME}}  {{SSP|SECURITYPLAN.VERSION}}  {{SSP|SECURITYPLAN.DATESUBMITTED}} | |  |
|
|  |  | |  |
|  |  | Controlled Unclassified Information info@fedramp.gov  fedramp.gov |  |

TEMPLATE REVISION HISTORY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Pages | Description | Author |
| 06/30/2023 | 1.0 | All | Initial publication after combining "front matter" sections of the FedRAMP System Security Plan (SSP) High Baseline Template, FedRAMP System Security Plan (SSP) Moderate Baseline Template, FedRAMP System Security Plan (SSP) Low Baseline Template, and Appendix B - FedRAMP Tailored LI-SaaS Template. | FedRAMP PMO |
|  |  |  |  |  |

**How to contact us**

For questions about FedRAMP, or for questions about this document including how to use it, contact [info@FedRAMP.gov.](mailto:info@FedRAMP.gov)

For more information about FedRAMP, see [www.FedRAMP.gov](http://www.fedramp.gov).

Delete this Template Revision History page and all other instructional text from your final version of this document.

SYSTEM SECURITY PLAN

Prepared by

|  |  |
| --- | --- |
| Identification of Organization that Prepared this Document | |
| **Organization Name** | {{SSP|SECURITYPLAN.PREPORGNAME}} |
| **Street Address** | {{SSP|SECURITYPLAN.PREPADDRESS}} |
| **Suite/Room/Building** | {{SSP|SECURITYPLAN.PREPOFFICE}} |
| **City, State, Zip** | {{SSP|SECURITYPLAN.PREPCITYSTATE}} |

Prepared for

|  |  |
| --- | --- |
| Identification of Cloud Service Provider | |
| **Organization Name** | {{SSP|SECURITYPLAN.CSPORGNAME}} |
| **Street Address** | {{SSP|SECURITYPLAN.CSPADDRESS}} |
| **Suite/Room/Building** | {{SSP|SECURITYPLAN.CSPOFFICE}} |
| **City, State, Zip** | {{SSP|SECURITYPLAN.CSPCITYSTATE}} |

Document Revision History

| **Date** | **Description** | **Version** | **Author** |
| --- | --- | --- | --- |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |

TABLE OF CONTENTS

[1 Introduction 8](#_Toc132928029)

[2 Purpose 8](#_Toc132928030)

[3 System Information 8](#_Toc132928031)

[4 System Owner 10](#_Toc132928032)

[5 Assignment of Security Responsibility 11](#_Toc132928033)

[6 Leveraged FedRAMP-Authorized Services 12](#_Toc132928034)

[7 External Systems and Services Not Having FedRAMP Authorization 15](#_Toc132928035)

[8 Illustrated Architecture and Narratives 19](#_Toc132928036)

[8.1 Illustrated Architecture 19](#_Toc132928037)

[8.2 Narrative 22](#_Toc132928038)

[9 Services, Ports, and Protocols 24](#_Toc132928039)

[10 Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT) 27](#_Toc132928040)

[11 Separation of Duties 29](#_Toc132928041)

[12 SSP Appendices List 31](#_Toc132928042)

[Appendix A {{SSP|SECURITYPLAN.SYSTEMNAME}} FedRAMP Security Controls 33](#_Toc132928043)

[Appendix B {{SSP|SECURITYPLAN.SYSTEMNAME}} Related Acronyms 35](#_Toc132928044)

[Appendix C {{SSP|SECURITYPLAN.SYSTEMNAME}} Information Security Policies and Procedures 36](#_Toc132928045)

[Appendix D {{SSP|SECURITYPLAN.SYSTEMNAME}} User Guide 37](#_Toc132928046)

[Appendix E {{SSP|SECURITYPLAN.SYSTEMNAME}} Digital Identity Worksheet 37](#_Toc132928047)

[Appendix F {{SSP|SECURITYPLAN.SYSTEMNAME}} Rules of Behavior (RoB) 40](#_Toc132928048)

[Appendix G {{SSP|SECURITYPLAN.SYSTEMNAME}} Information System Contingency Plan (ISCP) 40](#_Toc132928049)

[Appendix H {{SSP|SECURITYPLAN.SYSTEMNAME}} Configuration Management Plan (CMP) 41](#_Toc132928050)

[Appendix I {{SSP|SECURITYPLAN.SYSTEMNAME}} Incident Response Plan (IRP) 42](#_Toc132928051)

[Appendix J {{SSP|SECURITYPLAN.SYSTEMNAME}} Control Implementation Summary (CIS) and Customer Responsibilities Matrix (CRM) Workbook 43](#_Toc132928052)

[Appendix K {{SSP|SECURITYPLAN.SYSTEMNAME}} Federal Information Processing Standard (FIPS) 199 Categorization 44](#_Toc132928053)

[Appendix L {{SSP|SECURITYPLAN.SYSTEMNAME}}-Specific Laws and Regulations 47](#_Toc132928054)

[Appendix M {{SSP|SECURITYPLAN.SYSTEMNAME}} Integrated Inventory Workbook (IIW) 47](#_Toc132928055)

[Appendix N {{SSP|SECURITYPLAN.SYSTEMNAME}} Continuous Monitoring Plan 48](#_Toc132928056)

[Appendix O {{SSP|SECURITYPLAN.SYSTEMNAME}} POA&M 49](#_Toc132928057)

[Appendix P {{SSP|SECURITYPLAN.SYSTEMNAME}} Supply Chain Risk Management Plan (SCRMP) 49](#_Toc132928058)

[Appendix Q {{SSP|SECURITYPLAN.SYSTEMNAME}} Cryptographic Modules Table 50](#_Toc132928059)

SYSTEM SECURITY PLAN APPROVALS

**Cloud Service Provider (CSP) Signatures**

By signing this System Security Plan (SSP), we agree that it is complete and is the current version to be used for the security assessment. [The FedRAMP-specific Laws and Regulations Document](https://www.fedramp.gov/assets/resources/templates/SSP-A12-FedRAMP-Laws-and-Regulations-Template.xlsx), as of the date of this SSP, is {{SSP|SECURITYPLAN.VERSION}}, dated {{SSP|SECURITYPLAN.DATESUBMITTED}}, and is posted on the [FedRAMP Documents and Templates webpage](https://www.fedramp.gov/documents-templates/). The CSO-related laws and regulations, beyond those required by FedRAMP, are captured in Appendix L.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| <Sign Here> | | | | |
| Name | <Enter Name> | | Date | <Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | <CSP Name> | | |
|  | | | | |
|  | | | | |
| <Sign Here> | | | | |
| Name | <Enter Name> | | Date | <Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | <CSP Name> | | |
|  | | | | |
|  | | | | |
| <Sign Here> | | | | |
| Name | <Enter Name> | | Date | <Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | <CSP Name> | | |
|  | |  | | |

# Introduction

The SSP is the “security blueprint” of a CSO. The SSP defines a CSO’s authorization boundary and describes the security controls in place to protect the confidentiality, integrity, and availability (CIA) of the system and federal data it holds.

# Purpose

This document is intended to be used by CSPs that are pursuing a Joint Authorization Board (JAB) provisional authorization to operate (P-ATO) or an agency authorization to operate (ATO) through the Federal Risk and Authorization Management Program (FedRAMP).

# System Information

Table 3.1 provides a summary of the key attributes of the CSO.

Table 3.1 System Information

|  |  |
| --- | --- |
| System Information | |
| **CSP Name:** | {{SSP|SECURITYPLAN.CSPORGNAME}} |
| **CSO Name:** | {{SSP|SECURITYPLAN.SYSTEMNAME}} {{SSP|SECURITYPLAN.OTHERIDENTIFIER}} |
| **FedRAMP Package ID:** | {{SSP|SECURITYPLAN.FEDRAMPID}} |
| **Service Model:** | {{SERVICE}} |
| **Digital Identity Level (DIL) Determination (SSP Appendix E):** | {{DIL}} |
| **FIPS PUB 199 Level (SSP Appendix K):** | {{SSP|SECURITYPLAN.OVERALLCATEGORIZATION}} |
| **Fully Operational as of:** | {{SSP|SECURITYPLAN.DATESUBMITTED}} |
| **Deployment Model:** | {{MODEL}} |
| **Authorization Path:** | {{SSP|SECURITYPLAN.FEDRAMPAUTHORIZATIONTYPE}} |
| **General System Description:** | {{SSP|SECURITYPLAN.SYSTEMNAME}} is delivered as {{SERVICE}} offering using a multi-tenant {{MODEL}} cloud computing environment. {{SSP|SECURITYPLAN.DESCRIPTION}} |

# System Owner

The following individual is identified as the system owner or functional proponent/advocate for this system. The system owner is the official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Table 4.1 {{SSP|SECURITYPLAN.SYSTEMNAME}} Owner

| System Owner Information | |
| --- | --- |
| **Name** | {{SSP|SECURITYPLAN.SYSTEMOWNER.FULLNAME}} |
| **Title** | {{SSP|SECURITYPLAN.SYSTEMOWNER.JOBTITLE}} |
| **Company / Organization** | {{SSP|SECURITYPLAN.SYSTEMOWNER.COMPANY}} |
| **Address** | {{SSP|SECURITYPLAN.SYSTEMOWNER.ADDRESS}} |
| **Phone Number** | {{SSP|SECURITYPLAN.SYSTEMOWNER.WORKPHONE}} |
| **Email Address** | {{SSP|SECURITYPLAN.SYSTEMOWNER.EMAIL}} |

# Assignment of Security Responsibility

The {{SSP|SECURITYPLAN.CSPORGNAME}} {{SSP|SECURITYPLAN.SYSTEMNAME}} Information System Security Officer (ISSO), or equivalent, identified below, has been ***appointed in writing*** and is deemed to have significant cyber security and operational role responsibilities.

Table 5.1 {{SSP|SECURITYPLAN.CSPORGNAME}} ISSO (or Equivalent) Point of Contact

| **ISSO (or Equivalent) Point of Contact** | |
| --- | --- |
| **Name** | {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.FULLNAME}} |
| **Title** | {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.JOBTITLE}} |
| **Company / Organization** | {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.COMPANY}} |
| **Address** | {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.ADDRESS}} |
| **Phone Number** | {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.WORKPHONE}} |
| **Email Address** | {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.EMAIL}} |

# Leveraged FedRAMP-Authorized Services

The {{SSP|SECURITYPLAN.SYSTEMNAME}} leverages the FedRAMP Authorized services depicted in Table 6.1 below.

*Table 6.1 Leveraged FedRAMP Authorized Services*

{{REV5TABLE|6-1}}

# External Systems and Services Not Having FedRAMP Authorization

External systems/services, interconnections, application programming interfaces (APIs), and command line interfaces (CLIs) that do not have a FedRAMP authorization, at the same or greater impact level as {{SSP|SECURITYPLAN.SYSTEMNAME}}, are described in Table 7.1 below.

Table 7.1 External Systems/Services, Interconnections, APIs, and CLIs Without FedRAMP Authorizations

{{REV5TABLE|7-1}}

*\*\*1- Non-FedRAMP Authorized Cloud Services, 2- Corporate Shared Services, 3- Update Services for In-Boundary Software/Services*

# Illustrated Architecture and Narratives

This section contains the diagrams and narratives for the {{SSP|SECURITYPLAN.SYSTEMNAME}} authorization boundary, network, and data flows. Section 8.1 provides the diagrams, and Section 8.2 provides the associated narratives.

## Illustrated Architecture

This section contains the diagrams that represent the authorization boundary, network, and data flows. Following each of the diagrams, there is a narrative that describes the {{SSP|SECURITYPLAN.SYSTEMNAME}} boundary components, functionality, as well as interactions and flows among internal components and external systems/services. If using several illustrations, each must have a narrative.

Figure 8.1 {{SSP|SECURITYPLAN.SYSTEMNAME}} Authorization Boundary Diagram

|  |
| --- |
| {{IMAGES|SECURITYPLAN.AUTHORIZATIONBOUNDARY}} |
| {{UPLOAD|SECURITYPLAN.AUTHORIZATIONBOUNDARY}} |

Figure 8.1 {{SSP|SECURITYPLAN.SYSTEMNAME}} Network Diagram

|  |
| --- |
| {{IMAGES|SECURITYPLAN.NETWORKARCHITECTURE}} |
| {{UPLOAD|SECURITYPLAN.NETWORKARCHITECTURE}} |

Figure 8.1 {{SSP|SECURITYPLAN.SYSTEMNAME}} Data Flow Diagram

|  |
| --- |
| {{IMAGES|SECURITYPLAN.DATAFLOW}} |
| {{UPLOAD|SECURITYPLAN.DATAFLOW}} |

## Narrative

***Authorization Boundary Description****:*

{{SSP|SECURITYPLAN.AUTHORIZATIONBOUNDARY}}

***Network Description:***

{{SSP|SECURITYPLAN.NETWORKARCHITECTURE}}

***Data Flow Description:***

{{SSP|SECURITYPLAN.DATAFLOW}}

Table 8.1 {{SSP|SECURITYPLAN.SYSTEMNAME}} Security and Management Technologies

|  |  |
| --- | --- |
| Category | Technical Solution / Vendor |
| Operating Systems |  |
| IAM/Access Management |  |
| Endpoint/Antivirus (AV), File Integrity Monitoring (FIM) |  |
| Code Repository |  |
| Ticketing |  |
| Configuration Management |  |
| Firewall/VPN |  |
| MFA |  |
| SIEM |  |
| Secrets Management |  |
| Vulnerability Scanning |  |

# Services, Ports, and Protocols

Table 9.1 lists the service names, port numbers, and transport protocols enabled in {{SSP|SECURITYPLAN.SYSTEMNAME}}. These must be specifically called out per the security control requirements in CM-7, CM-7(1), RA-5, SA-4, SA-9(2), and SA-9(4).

Table 9.1 {{SSP|SECURITYPLAN.SYSTEMNAME}} Services, Ports, and Protocols

{{REV5TABLE|9-1}}

# Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT)

The use of cryptography is critical for all systems that process and/or store federal data. Federal policy requires that anywhere that cryptography is required, it must employ FIPS 140-validated cryptographic modules. The Appendix Q cryptographic modules tables specify the encryption status for {{SSP|SECURITYPLAN.SYSTEMNAME}}. These tables include reference numbers that are specified in <Insert Figure Number(s) (refer to the diagrams in the SSP depicting encryption status, typically data flow, if not combined)> in Section 8 of this SSP that depict the specific data stores and flows related to {{SSP|SECURITYPLAN.SYSTEMNAME}}.

{{SSP|SECURITYPLAN.CSPORGNAME}} confirms, except where clearly noted in Appendix Q, that {{SSP|SECURITYPLAN.SYSTEMNAME}} employs FIPS-validated cryptographic modules (CMs) that are configured in an approved mode, which is documented in the associated Cryptographic Module Validation Program (CMVP) security policy for the FIPS-validated certificate number. Only algorithms listed, as approved, in the CM’s security policy are used. The encryption discussed, in Appendix Q, is validated by an IA during a security assessment.

# Separation of Duties

Security control AC-5, Separation of Duties, requires that CSPs identify and document the roles of ***all*** individuals who access the system and define the access authorizations that support protections from bad actors, employee collusion, fraud, etc. before damage occurs. Table 11.1 captures the roles and access privileges for all individuals or roles that access {{SSP|SECURITYPLAN.SYSTEMNAME}}.

Table 11.1 {{SSP|SECURITYPLAN.SYSTEMNAME}} Separation of Duties

**The {{SSP|SECURITYPLAN.SYSTEMNAME}} Separation of Duties Matrix is included as an Appendix available separately.**

# SSP Appendices List

Table 12.1 SSP Required Appendices

| Appendix Name | Filename |
| --- | --- |
| **Appendix A: FedRAMP Security Controls**  (FedRAMP-provided; different template for each impact level) |  |
| **Appendix B: Related Acronyms**  (CSP-provided) | Included within the SSP |
| **Appendix C: Security Policies and Procedures**  (CSP-provided in a zip file; not required for LI-SaaS) |  |
| **Appendix D: User Guide**  (CSP-provided; not required for LI-SaaS) |  |
| **Appendix E: Digital Identity Worksheet**  (FedRAMP-provided) | Included within the SSP |
| **Appendix F: Rules of Behavior**  (FedRAMP-provided; not required for LI-SaaS) |  |
| **Appendix G: Information System Contingency Plan (ISCP)**  (FedRAMP-provided; not required for LI-SaaS) |  |
| **Appendix H: Configuration Management Plan (CMP)**  (CSP-provided; not required for LI-SaaS) |  |
| **Appendix I: Incident Response Plan (IRP)**  (CSP-provided; not required for LI-SaaS) |  |
| **Appendix J: CIS and CRM Workbook**  (FedRAMP-provided; different template for each impact level) |  |
| **Appendix K: FIPS 199 Worksheet**  (FedRAMP-provided) | Included within the SSP |
| **Appendix L: CSO-Specific Required Laws and Regulations**  (CSP-provided) | Included within the SSP. |
| **Appendix M: Integrated Inventory Workbook**  (FedRAMP-provided) |  |
| **Appendix N: Continuous Monitoring Plan**  (CSP-provided) |  |
| **Appendix O: POA&M**  (FedRAMP-provided) |  |
| **Appendix P: Supply Chain Risk Management Plan (SCRMP)**  (CSP-provided) |  |
| **Appendix Q: Cryptographic Module Table**  (FedRAMP-provided) |  |

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} FedRAMP Security Controls

Please see Appendix A (separate document) for the security controls applicable to {{SSP|SECURITYPLAN.SYSTEMNAME}}.

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Related Acronyms

The acronyms that appear in this section are specific to the {{SSP|SECURITYPLAN.SYSTEMNAME}} SSP. Here are any links if provided:

{{REV5TABLE|B-1}}

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Information Security Policies and Procedures

The {{SSP|SECURITYPLAN.SYSTEMNAME}} policies and procedures are included in Appendix C, available separately. Here are any links if provided:

{{REV5TABLE|C-1}}

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} User Guide

The {{SSP|SECURITYPLAN.SYSTEMNAME}} user guide is included in Appendix D, available separately.

or

The {{SSP|SECURITYPLAN.SYSTEMNAME}} user guide website address is <https://regscale.readme.io/docs/getting-started>.

Here are any links if provided:

{{REV5TABLE|D-1}}

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Digital Identity Worksheet

**Mapping FedRAMP Levels to NIST SP 800-63 Levels**

Digital identity is the process of establishing confidence in user identities electronically presented to an information system. Authentication focuses on the identity proofing process, the authenticator management process, and the assertion protocol used in a federated environment to communicate authentication and attribute information, if applicable.

Table E.1, below, “Mapping FedRAMP Levels to NIST SP 800-63 Levels”, maps the FedRAMP impact levels (Low/LI-SaaS, Moderate, and High) to [NIST SP 800-63 Digital Identity Guidelines](https://pages.nist.gov/800-63-3/) levels:

* Identity Assurance Level (IAL) - Refers to the identity proofing process
* Authenticator Assurance Level (AAL) - Refers to the authentication process
* Federation Assurance Level (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 E.1 Mapping FedRAMP Levels to NIST SP 800-63 Levels

| FedRAMP Impact Level | 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; authenticators and verifiers use FIPS 140-validated cryptography; authenticator must be hardware-based | FAL3: The assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it. For very high value or very high-risk situations, the subscriber (user) must provide proof of possession of a secure, cryptographic key, and a HW based device to provide verifier impersonation resistance. The device may fulfill both requirements. |
| **Moderate** | IAL2: In-person or remote, potentially involving a “trusted referee” | AAL2: Multi-factor required; authenticators and verifiers use FIPS 140-validated cryptography | FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it |
| **Low and  FedRAMP LI-SaaS** | IAL1: Self-asserted | AAL1: Single-factor or multi-factor; verifiers use FIPS 140-validated cryptography | FAL1: Assertion is digitally signed by the identity provider |

**Digital Identity Level Selection**

The {{SSP|SECURITYPLAN.CSPORGNAME}} has identified that they support the digital identity level that has been selected for the {{SSP|SECURITYPLAN.SYSTEMNAME}}. The selected digital identity level indicated is supported for federal agency consumers of the CSO. Implementation details of the digital identity mechanisms are provided in Appendix A under control IA-2.

Table E.2 Digital Identity Level

| Digital Identity Level | Maximum Impact Profile | Selection |
| --- | --- | --- |
| Level 1: AAL1, IAL1, FAL1 | Low/LI-SaaS | {{CHECKBOX|IDENTITYASSURANCELEVEL|1}} |
| Level 2: AAL2, IAL2, FAL2 | Moderate | {{CHECKBOX|IDENTITYASSURANCELEVEL|2}} |
| Level 3: AAL3, IAL3, FAL3 | High | {{CHECKBOX|IDENTITYASSURANCELEVEL|3}} |

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Rules of Behavior (RoB)

The {{SSP|SECURITYPLAN.SYSTEMNAME}} rules of behavior are included in Appendix F, attached separately.

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Information System Contingency Plan (ISCP)

The {{SSP|SECURITYPLAN.SYSTEMNAME}} information system contingency plan is included in Appendix G, attached separately.

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Configuration Management Plan (CMP)

The {{SSP|SECURITYPLAN.SYSTEMNAME}} configuration management plan is included as Appendix H, attached separately.

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Incident Response Plan (IRP)

The {{SSP|SECURITYPLAN.SYSTEMNAME}} incident response plan is included as Appendix I, attached separately.

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Control Implementation Summary (CIS) and Customer Responsibilities Matrix (CRM) Workbook

The {{SSP|SECURITYPLAN.SYSTEMNAME}} CIS and CRM workbook is included as Appendix J, attached separately.

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Federal Information Processing Standard (FIPS) 199 Categorization

The FIPS 199 Categorization (Security Categorization) report is a key component of the security authorization package developed for submission to FedRAMP authorizing officials. The FIPS 199 Categorization report below includes the determination of the security impact level for the {{SSP|SECURITYPLAN.SYSTEMNAME}} cloud environment.

Note: This report is initially completed by the CSP in anticipation of what the actual federal data that might be stored, processed, and transmitted. Each agency must do this FIPS 199 analysis for their own data flows to ensure compatibility with the overall criticality level.

The {{SSP|SECURITYPLAN.SYSTEMNAME}} system has been determined to have a security categorization of {{SSP|SECURITYPLAN.OVERALLCATEGORIZATION}}, as determined in Table K.1.

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 199 is the High watermark for the impact level of all the applicable information types.

Table K.1 uses the NIST SP 800-60 (current revision) 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 K.1 {{SSP|SECURITYPLAN.SYSTEMNAME}} Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1

{{REV5TABLE|K-1}}

1. {{SSP|SECURITYPLAN.SYSTEMNAME}}-Specific Laws and Regulations

Table L.1 {{SSP|SECURITYPLAN.SYSTEMNAME}}-specific Laws and Regulations

{{REV5TABLE|L-1}}

Table L. {{SSP|SECURITYPLAN.SYSTEMNAME}}-specific Standards and Guidance

{{REV5TABLE|L-2}}

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Integrated Inventory Workbook (IIW)

The {{SSP|SECURITYPLAN.SYSTEMNAME}} integrated inventory workbook is included in Appendix M, attached separately.

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Continuous Monitoring Plan

The {{SSP|SECURITYPLAN.SYSTEMNAME}} continuous monitoring plan is included in Appendix N, attached separately.

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} POA&M

The {{SSP|SECURITYPLAN.SYSTEMNAME}} plan of action and milestones (POA&M) is included in Appendix O, attached separately.

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Supply Chain Risk Management Plan (SCRMP)

The {{SSP|SECURITYPLAN.SYSTEMNAME}} supply chain risk management plan (SCRM) is included in Appendix P, attached separately.

1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Cryptographic Modules Table

The {{SSP|SECURITYPLAN.SYSTEMNAME}} cryptographic modules table is included as Appendix Q, attached separately.

{{REV5TABLE|APPQDIT}}

{{REV5TABLE|APPQDAR}}

{{REV5TABLE|APPQOTH}}