SSP ATTACHMENT 10 – FedRAMP Federal Information Processing Standard (FIPS) 199 Categorization Template

CSP Name

<Information System Name>

Version #.#

Version Date

Controlled Unclassified Information

Prepared by

| Organization Name that prepared this document |
| --- |
|  | Street Address | Click here to enter text. |
| Suite/Room/Building | Click here to enter text. |
| City, State, ZIP | Click here to enter text. |

Prepared for

| Organization Name for whom this document was prepared |
| --- |
|  | Street Address | Click here to enter text. |
| Suite/Room/Building | Click here to enter text. |
| City, State, ZIP | Click here to enter text. |

Instruction: Delete this Record of Changes for Template table and this instruction from your final version of this document.

Record of Changes for Template

| Date | Description | Version  | Author |
| --- | --- | --- | --- |
| 5/2/2012 | Original publication | 1.0 | FedRAMP PMO |
| 5/18/2016 | Reformatted to FedRAMP Document Standard, added repeated text schema, and content fields to tables, revised cover page, changed document designation to Confidential Unclassified Confidential Information (CUI), added instruction to complete 15.10 Attachment 10 - Revision History in the System Security Plan, minor revisions to Section 2, added instruction to Appendix A to see SSP Attachment 12 for FedRAMP Laws and Regulations, Standards and Guidance. | 2.0 | FedRAMP PMO |
| 3/9/2017 | Document renamed from "FedRAMP Federal Information Processing Standard (FIPS) 199 Categorization Template" to "SSP ATTACHMENT 10 - FedRAMP Federal Information Processing Standard (FIPS) 199 Categorization Template"  | 2.1 | FedRAMP PMO |
| 6/6/2017 | Updated logo | 2.1 | FedRAMP PMO |

Revision History

Complete 15.10 Attachment 10 – FIPS 199 Revision History in the System Security Plan. Detail specific changes in the table below.

| Date | Version | Page(s) | Description | Author |
| --- | --- | --- | --- | --- |
| Click here to enter a date. | Click  | Click  | Click here to enter text. | Click  |
| Click here to enter a date. | Click  | Click  | Click here to enter text. | Click  |

How to contact us

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

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

Table of Contents

[1 Introduction and Purpose 1](#_Toc454695890)

[1.1 Scope 1](#_Toc454695891)

[1.2 System Description 1](#_Toc454695892)

[2 Methodology 1](#_Toc454695893)

[3 Acronyms and Definitions 4](#_Toc454695894)

[4 Applicable Laws, Regulations, and Directives 4](#_Toc454695895)

[4.1 Applicable Laws and Regulations 4](#_Toc454695896)

[4.2 Applicable Standards and Guidance 4](#_Toc454695897)

List of Tables

[Table 2‑1 CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1 3](#_Toc454695899)

# Introduction and Purpose

This document is intended to be used by service providers who are applying for an Authorization through the U.S. federal government FedRAMP program.

The Federal Information Processing Standard 199 (FIPS 199) Categorization (Security Categorization) report is a key document in the security authorization package developed for submission to the Federal Risk and Authorization Management Program (FedRAMP) authorizing officials. The FIPS199 Categorization report includes the determination of the security impact level for the cloud environment that may host any or all of the service models (Information as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The ultimate goal of the security categorization is for the cloud service provider (CSP) to be able to select and implement the FedRAMP security controls applicable to its environment.

The purpose of the FIPS199 Categorization report is for the CSP to assess and complete the categorization of their cloud environment, to provide the categorization to the System Owner/Certifier and the FedRAMP Joint Authorization Board (JAB) and in helping them to make a determination of the CSP’s ability to host systems at that level. The completed security categorization report will aid the CSP in selection and implementation of FedRAMP security controls at the determined categorization level.

## Scope

The scope of the FIPS199 Categorization report includes the assessment of the information type categories as defined in the NIST Special Publication 800-60 Volume II Revision 1 Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.

## System Description

The <Information System Name> system has been determined to have a security categorization of *Choose level*.

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

# Methodology

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

Impact levels are determined for each information type based on the security objectives (confidentiality, integrity, availability). The confidentiality, integrity, and availability impact levels define the security sensitivity category of each information type. The FIPS PUB 199 is the high watermark for the impact level of all the applicable information types.

The FIPS PUB 199 analysis represents the information type and sensitivity levels of the CSP’s cloud service offering (and is not intended to include sensitivity levels of agency data). Customer agencies will be expected to perform a separate FIPS 199 Categorization report analysis for their own data hosted on the CSP’s cloud environment. The analysis must be added as an appendix to the SSP and drive the results for the Categorization section.

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

The Table 2‑1 CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1below uses the NIST SP 800-60 V2 R1 Volume II Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories to identify information types with the security impacts.

Table ‑ CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1

| Information Type | NIST SP 800-60 V2 R1 Recommended Confidentiality Impact Level | NIST SP 800-60 V2 R1 Recommended Integrity Impact Level | NIST SP 800-60 V2 R1 Recommended Availability Impact Level | CSP Selected Confidentiality Impact Level | CSP Selected Integrity Impact Level | CSP Selected Availability Impact Level | Statementfor Impact Adjustment Justification |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |

# Acronyms and Definitions

|  |  |
| --- | --- |
| Acronyms | Definition |
| **ATO** | Authorization to Operate |
| **AO** | Authorizing Official |
| **CSP** | Cloud Service Provider |
| **FedRAMP** | Federal Risk and Authorization Management Program |
| **FIPS PUB 199** | Federal Information Processing Standard Publication |
| **FISMA** | Federal Information Security Management Act |
| **IaaS** | Infrastructure as a Service (Model) |
| **JAB** | FedRAMP Joint Authorization Board  |
| **NIST** | National Institute of Standards and Technology |
| **OMB** | Office of Management and Budget |
| **PaaS** | Platform as a Service (Model) |
| **R1** | Revision 1 |
| **SaaS** | Software as a Service (Model) |
| **SP** | Special Publication |
| **SSP** | System Security Plan |
| **V2** | Version 2 |

# Applicable Laws, Regulations, and Directives

Instruction: Refer to Section 12 of the System Security Plan for system specific laws, regulations, standards, and guidance.
Delete this instruction from your final version of this document.

## Applicable Laws and Regulations

The FedRAMP Laws and Regulations may be found on: [www.fedramp.gov](http://www.fedramp.gov) Templates.

## Applicable Standards and Guidance

The FedRAMP Standards and Guidance may be found on: [www.fedramp.gov](http://www.fedramp.gov) Templates, FedRAMP Laws and Regulations.