SSP ATTACHMENT 3 –

FedRAMP Electronic Authentication (E-Authentication) Plan 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 |
| --- | --- | --- | --- |
| 9/19/2013 | Sections 3, 4, Table 3-1 Revised text, table, and instructions  | 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 Information (CUI), removed front matter section How This Document is Organized, added Section 1 Introduction and Purpose | 2.0 | FedRAMP PMO |
| 3/6/2017 | Document renamed from "Electronic Authentication (E-Authentication) Template" to "SSP ATTACHMENT 3 - FedRAMP Electronic Authentication (E-Authentication) Plan Template" | 2.1 | FedRAMP PMO |
| 6/6/2017 | Updated logo | 2.1 | FedRAMP PMO |

Revision History

Complete 15.3 Attachment 3 - E-Authentication 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](#_Toc454692742)

[2 Information System Name/Title 1](#_Toc454692743)

[3 E-Authentication Level Definitions 1](#_Toc454692744)

[4 Review Maximum Potential Impact Levels 1](#_Toc454692745)

[5 E-Authentication Level Selection 2](#_Toc454692746)

[6 Acronyms and Definitions 3](#_Toc454692747)

List of Tables

[Table 2‑1 Information System Name and Title 1](#_Toc443965649)

[Table 4‑1 Potential Impacts for Assurance Levels 2](#_Toc443965650)

[Table 5‑1 E-Authentication Level 2](#_Toc443965651)

# Introduction and Purpose

This document provides guidance on electronic authentication (E-Authentication, which is the process of establishing confidence in user identities electronically presented to an information system. Authentication focuses on confirming a person’s identity, based on the reliability of his or her credential. Office of Management and Budget (OMB) Memorandum M-04-04, E-Authentication Guidance for Federal Agencies requires federal information system owners determine the system’s electronic authentication (E-Authentication) requirements to minimize the potential impact of authentication errors and misuse of credentials.

OMB Memorandum M-04-04 can be found at the following URL: [OMB M-04-04.pdf](http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf)

# Information System Name/Title

This E-Authentication Plan provides an overview of the security requirements for the Information System Name (Information System Abbreviation) in accordance with OMB Memo M-04-04.

Table 2‑1 Information System Name and Title

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

# E-Authentication Level Definitions

The OMB memo defines four authentication levels to categorize a federal information system’s E-Authentication posture. The OMB Memo defines the four E-Authentication levels as:

* Level 1: Little or no confidence in the asserted identity’s validity
* Level 2: Some confidence in the asserted identity’s validity
* Level 3: High confidence in the asserted identity’s validity
* Level 4: Very high confidence in the asserted identity’s validity

Selecting the appropriate E-Authentication level for a system enables the system owner to determine the right system authentication technology solution for the selected E-Authentication level. Guidance on selecting the system authentication technology solution is available in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Revision 2, Electronic Authentication Guideline.

NIST SP 800-63, Revision 2 can be found at the following URL: [SP 800-63-2](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf)

# Review Maximum Potential Impact Levels

CSP Name has assessed the potential risk from E-Authentication errors, or E-Authentication 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 4‑1 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 4‑1 Potential Impacts for Assurance Levels

|  | Assurance Level Impact Profile |
| --- | --- |
| Potential Impact Categories  | 1 | 2 | 3 | 4 |
| Inconvenience, distress or damage to standing or reputation | Low | Mod | Mod | High |
| Financial loss or agency liability | Low | Mod | Mod | High |
| Harm to agency programs or public interests | N/A | Low | Mod | High |
| Unauthorized release of sensitive information | N/A | Low | Mod | High |
| Personal Safety | N/A | N/A | Low | Mod, High |
| Civil or criminal violations | N/A | Low | Mod | High |

# E-Authentication Level Selection

Instruction: Select the lowest level that will cover all potential impact identified from Table 4‑1 Potential Impacts for Assurance Levels.

Delete this instruction from your final version of this document.

The CSP Name has identified that they support the E-Authentication Level that has been selected for the Information System Name as noted in Table 5‑1 E-Authentication Level. The selected E-Authentication Level indicated is supported for federal agency consumers of the cloud service offering. Implementation details of the E-Authentication mechanisms are provided in the System Security Plan under control IA-2

Table 5‑1 E-Authentication Level

| E-Authentication Level | Maximum Impact Profile | Selection |
| --- | --- | --- |
| Level 1: no identity proofing requirement | Low |[ ]
| Level 2: single factor remote authentication | Low |[ ]
| Level 3: multi-factor remote authentication | Moderate |[ ]
| Level 4: multi-factor remote authentication; hard crypto tokens | High |[ ]

# Acronyms and Definitions

| Acronym | Definition |
| --- | --- |
| CSP | Cloud Service Provider |
| E-Authentication | Electronic Authentication |
| FedRAMP | Federal Risk and Authorization Management Program |
| NIST | National Institute of Standards and Technology |
| NIST-SP | NIST Special Publication |
| OMB | Office of Management and Budget |