

Digital Identity Risk Assessment (DIRA) for [System Name]

**UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT**

**Office of the Chief Information Officer**

**Version [Version #]
[Date as (Month DD, YYYY)]**

**[Explanation of Version Numbering**

Initial drafts of documents not previously issued are numbered .01 through .*nn.* Initial document sign-off by the document owners results in version 1.0. Future sign-offs will always yield whole version numbers (version 2.0, 3.0, etc.). Any significant process changes prompt a change of version number. For example, if a new sub-process is added after initial sign-off, this would result in Draft Version 1.01. Once this change is signed off by the document owner, the document becomes Version 2.0.]

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Publication Date** | **Description of Change** | **Author** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Document Approval**

[Document approvers vary depending on the nature of and reason for the document. Please ensure that your document includes all necessary approvers and only those]

Information System Security Officer (ISSO):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Name) (Signature) (Date)

System Owner (SO):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Name) (Signature) (Date)

IA Division:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Name) (Signature) (Date)

Table of Contents

[1 Introduction 1](#_Toc53058070)

[1.1 Purpose 1](#_Toc53058071)

[1.2 System Information 1](#_Toc53058072)

[2 Is DIRA Required? 2](#_Toc53058073)

[3 Is System Federated? 2](#_Toc53058074)

[4 Determine Impact Level 3](#_Toc53058075)

[5 Determine Identity Assurance Level (IAL) 5](#_Toc53058076)

[6 Determine Authenticator Assurance Level (AAL) 6](#_Toc53058077)

[7 Determine Federation Assurance Level (FAL) 7](#_Toc53058078)

[Appendix A. DIRA Process Flowcharts 9](#_Toc53058079)

[A.1 Flowchart - High Level Process 9](#_Toc53058080)

[A.2 Flowchart - Is a DIRA Required? Is System Federated? 10](#_Toc53058081)

[A.3 Flowchart - IAL 11](#_Toc53058082)

[A.4 Flowchart - AAL 13](#_Toc53058083)

[A.5 Flowchart - FAL 15](#_Toc53058084)

[Appendix B. References and Acronyms 17](#_Toc53058085)

[B.1 Authorities, Policies, Processes, Websites, and Other References 17](#_Toc53058086)

[B.2 Acronyms and Abbreviations 17](#_Toc53058087)

Tables

[Table 1. Information System Name 1](#_Toc53058088)

[Table 2. Potential Impact Level 3](#_Toc53058089)

**[Instructions to the Author**

For purposes of completing sections and paragraphs in this document, text providing instructions for use of this template is given in blue type within brackets ([ ]). When the document is completed, all instructional material in blue type—including this section of instructions—should be deleted. Your final document should include only material pertinent to its subject.]

[USAID has provided this template to complete the Digital Identity Risk Assessment (DIRA).]

# Introduction

Per National Institute of Standards and Technology (NIST) Special Publication (SP) [800-63-3, Digital Identity Guidelines](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf), Federal agencies must perform Digital Identity Risk Assessments (DIRA); select individual assurance levels (xALs) for identity proofing, authentication, and federation (if applicable); determine which processes and technologies they will employ to meet each assurance level; and document these decisions in a “Digital Identity Acceptance Statement.” This USAID DIRA document fulfills this requirement for the identified system.

## Purpose

This document - the USAID DIRA - helps System Owners (SOs) and Information System Security Officers (ISSOs) to determine and record the following information so that they can meet the DIRA requirements in NIST SP 800-63-3:

*For all systems:*

* Determine whether a DIRA is required for the system

*For systems for which a DIRA is required:*

* Determine if the system is federated
* Determine the system’s identity, authenticator, and (if applicable) federator assurance level
* Complete the required Digital Identity Acceptance Statement

[This template provides a framework for USAID SOs and ISSOs to collect, approve, and disseminate the required DIRA information for their system.]

## System Information

Table 1 shows the full name of the information system, the abbreviation used for the system (if applicable), and the system’s unique identifier (found in CSAM).

Table 1. Information System Name

| Information System Name | Abbreviation | Unique Identifier |
| --- | --- | --- |
|  |  |  |

# Is DIRA Required?

The following question must be answered to determine if a DIRA is required.

[Additional guidance on the DIRA process is provided in the [Digital Identity Risk Assessment Playbook](https://drive.google.com/file/d/1RLsJI0cWOT2Od0p8ASwtmp5GY_F900cH/view?usp=sharing). Please note that this link is to a version posted by the IA team in a USAID Google Drive folder. To ensure you are using the latest version, please visit the [Identity Credential and Access Management Subcommittee (ICAMSC) Max.gov, ICAMSC Guidance Documents](https://community.max.gov/display/Egov/ICAMSC%2BGuidance%2BDocuments) page.]

**Does the system support non-Agency personnel?**

[ ]  **Yes**. A Digital Identity Risk Assessment *is required*.
*Instructions:* Check the **Yes** box and proceed to the next section. Complete the document as directed. When finished, obtain Management Bureau/Office of the Chief Information Officer/Information Assurance Division/Compliance and Risk Management (M/CIO/IA/CRM) approval, and retain a signed copy of the document in the Cyber Security Assessment and Management (CSAM) tool.

[ ]  **No**. A Digital Identity Risk Assessment is *not* required.  **Note: Even when no DIRA is required, Agency workforce members (employees and contractors) must still be authenticated by a valid PIV card, PIV-I card, or an approved alternative IAL 3/AAL 3 credential.**
*Instructions:* Check the **No** box, obtain M/CIO/IA/CRM approval for this document, and retain a signed copy of the DIRA in the CSAM tool.

# Is System Federated?

The following question must be answered to determine which sections of the document are required.

[Additional guidance on the DIRA process is provided in the [Digital Identity Risk Assessment Playbook](https://drive.google.com/file/d/1RLsJI0cWOT2Od0p8ASwtmp5GY_F900cH/view?usp=sharing).]

**Is the system federated[[1]](#footnote-1)?**

[ ]  **No**. An assessment must be performed to determine the following:

* Identity Assurance Level (IAL) (Section 5)
* Authenticator Assurance Level (AAL) (Section 6)

[ ]  **Yes**. An assessment must be performed to determine the following:

* Identity Assurance Level (IAL) (Section 5)
* Authenticator Assurance Level (AAL) (Section 6)
* Federation Assurance Level (FAL) (Section 7)

# Determine Impact Level

[Additional guidance on the DIRA process is provided in the [Digital Identity Risk Assessment Playbook](https://drive.google.com/file/d/1RLsJI0cWOT2Od0p8ASwtmp5GY_F900cH/view?usp=sharing).]

Based on NIST SP 800-63-3, the agency must assess the risk of identity proofing and authentication errors to determine the required assurance level for each transaction. This risk must be assessed in the context of six impact categories (shown below) specific to digital identity.

*Note:* Risk should be considered from the perspective of the organization and to the user, since one may not be negatively impacted while the other could significantly harmed.

[Select the checkbox for the maximum impact level for each category in the table below. Use this information to update the remaining sections in this template where indicated.]

Table 2. Potential Impact Level

| Category | Impact Level | Select Potential Impact Level |
| --- | --- | --- |
| Low | Moderate | High |
| **Inconvenience, distress or damage to standing or reputation** | At worst, limited, short-term inconvenience, distress or embarrassment to any party. | At worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party. | Severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals). | [ ]  Low[ ]  Moderate[x]  High |
| **Financial Loss** | At worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability. | At worst, a serious unrecoverable financial loss to any party, or a serious agency liability. | Severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability. | [ ]  Low[ ]  Moderate[ ]  High  |
| **Harm to agency programs or public interests** | At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests. | At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests. | A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests. | [ ]  Low[ ]  Moderate[ ]  High |
| **Unauthorized release of sensitive information** | At worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199. | At worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199. | A release of personal, U.S. government sensitive or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199. | [ ]  Low[ ]  Moderate[ ]  High |
| **Personal Safety** | At worst, minor injury not requiring medical treatment. | At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment | A risk of serious injury or death. | [ ]  Low[ ]  Moderate[ ]  High |
| **Civil or criminal violations** | At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts. | At worst, a risk of civil or criminal violations that may be subject to enforcement efforts. | A risk of civil or criminal violations that are of special importance to enforcement programs. | [ ]  Low[ ]  Moderate[ ]  High |

# Determine Identity Assurance Level (IAL)

This section is mandatory for all systems that require a DIRA.

[Additional guidance on the DIRA process is provided in the [Digital Identity Risk Assessment Playbook](https://drive.google.com/file/d/1RLsJI0cWOT2Od0p8ASwtmp5GY_F900cH/view?usp=sharing).]

Please answer the following questions to determine the appropriate IAL:

1. **To provide the service, do you need any personal information[[2]](#footnote-2)?**

[ ]  **No**. Your system is **IAL-1**.

[ ]  **Yes**. Proceed to question 2.

1. **To complete the transaction do you need the information to be validated?**

[ ]  **No**. Your system is **IAL-1**.

[ ]  **Yes** or **I don’t know**. Proceed to question 3.

1. **What are the risks (to the organization or the subject) of providing the digital service? In Section 4, Table 2, did you assess at high for any of the above categories?**

[ ]  **No**. Proceed to question 4.

[ ]  **Yes**. Your system is **IAL-3**.

1. **Did you assess moderate for personal safety?**

[ ]  **No**. Proceed to question 5.

[ ]  **Yes**. Your system is **IAL-3**.

1. **Did you assess moderate for any of the remaining categories?**

[ ]  **No**. Proceed to question 6.

[ ]  **Yes**. Your system is **IAL-2**.

1. **Did you assess low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?**

[ ]  **No**. Your system is **IAL-1**.

[ ]  **Yes**. Your system is **IAL-2**.

|  |
| --- |
| **IAL Level:**  Per the guidelines in this section, **[system name]** is **[enter IAL level here].** |

# Determine Authenticator Assurance Level (AAL)

This section is mandatory for all systems that require a DIRA.

[Additional guidance on the DIRA process is provided in the [Digital Identity Risk Assessment Playbook](https://drive.google.com/file/d/1RLsJI0cWOT2Od0p8ASwtmp5GY_F900cH/view?usp=sharing).]

Please answer the following questions to determine the appropriate AAL:

1. **What are the risks (to the organization or the subject) of providing the service? Refer to
Table** **2. Did you assess at high for any of the categories?**

[ ]  **No**. Proceed to question 2.

[ ]  **Yes**. Your system is **AAL-3**.

1. **Did you assess moderate for personal safety?**

[ ]  **No**. Proceed to question 3.

[ ]  **Yes**. Your system is **AAL-3**.

1. **Did you assess moderate for any of the remaining categories?**

[ ]  **No**. Proceed to question 4.

[ ]  **Yes**. Your system is **AAL-2**.

1. **Did you assess low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?**

[ ]  **No**. Proceed to question 5.

[ ]  **Yes**. Your system is **AAL-2**.

1. **Are you making personal data accessible?**

[ ]  **No**. Your system is **AAL-1**.

[ ]  **Yes**. Your system is **AAL-2**.

|  |
| --- |
| **AAL Level:**  Per the guidelines in this section, **[system name]** is **[enter AAL level here].** |

# Determine Federation Assurance Level (FAL)

This section is required only for federated systems.

[Additional guidance on the DIRA process is provided in the [Digital Identity Risk Assessment Playbook](https://drive.google.com/file/d/1RLsJI0cWOT2Od0p8ASwtmp5GY_F900cH/view?usp=sharing).]

Please answer the following questions to determine the appropriate FAL:

1. **Are you federating?**

[ ]  **No**. No FAL assessment is required.

☐ **Yes**. Proceed to question 2.

1. **What are the risks (to the organization or the subject) of providing the digital service? Refer to Table 2. Did you assess at high for any of the categories?**

[ ]  **No**. Proceed to question 3.

[ ]  **Yes**. Your system is **FAL-3**.

1. **Did you assess moderate for personal safety?**

[ ]  **No**. Proceed to question 4.

[ ]  **Yes**. Your system is **FAL-3**.

1. **Did you assess moderate for any of the remaining categories?**

[ ]  **No**. Proceed to question 5.

[ ]  **Yes**. Your system is **FAL-2**.

1. **Did you assess low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?**

[ ]  **No**. Proceed to question 6.

[ ]  **Yes**. Your system is **FAL-2**.

1. **Will personal data be in the system?**

[ ]  **No**. Proceed to question 7.

[ ]  **Yes**. Your system is **FAL-2**.

1. **Are you using font channel?**

[ ]  **No**. Your system is **FAL-1**.

[ ]  **Yes**. Your system is **FAL-2**.

|  |
| --- |
| **FAL Level** (if applicable)**:**  Per the guidelines in this section, **[system name]** is **[enter FAL level here].** |

1. DIRA Process Flowcharts

[Additional guidance on the DIRA process is provided in the [Digital Identity Risk Assessment Playbook](https://drive.google.com/file/d/1RLsJI0cWOT2Od0p8ASwtmp5GY_F900cH/view?usp=sharing).]

## A.1 Flowchart - High Level Process



## A.2 Flowchart - Is a DIRA Required? Is System Federated?



## A.3 Flowchart - IAL



(IAL flowchart, step 3, continues on next page)

(IAL flowchart, step 3, continued from previous page)



## A.4 Flowchart - AAL



(AAL flowchart, step 1, continues on next page)

(AAL flowchart, step 1, continued from previous page)



## A.5 Flowchart - FAL



(FAL flowchart, step 2, continues on next page)

(FAL flowchart, step 2, continued from previous page)



1. References and Acronyms

## B.1 Authorities, Policies, Processes, Websites, and Other References

Refer to the [Reference List for IA Documentation](https://docs.google.com/spreadsheets/d/1zSgTaeOIucJgAp8CVrQwAKBI9AphVcgwVbRAjZH9xpY/edit?usp=sharing) for links to work cited in this document.

[If a reference is missing from the Reference List, follow the instructions at the top of the list to submit the reference for inclusion.]

## B.2 Acronyms and Abbreviations

Refer to the [IA Acronym List](https://docs.google.com/document/d/14cGh9Dyni7sYgtNhgjWX_iaXB04oAZPJOF37-zNVuYU/edit?usp=sharing) for definitions of acronyms and abbreviations used in this document.

[If an acronym is missing from the IA Acronym List, follow the instructions at the top of the list to submit the acronym for inclusion.]

1. Per NIST SP 800-63-3, Digital Identity Guidelines, *federation* is defined as “a process that allows the conveyance of identity and authentication information across a set of networked systems. [↑](#footnote-ref-1)
2. Per NIST 800-63-3, *personal information* is synonymous with *personally identifiable information (PII)*. According to ADS Chapter 508, PII is “information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.” This can be any directly linked information (such as full name, home address, social security number (SSN), driver’s license, or passport information), or linkable information ( like date of birth (DOB), physical characteristics, etc.). [↑](#footnote-ref-2)