# FISMA Low Impact

## Contents

* [1. Information System Name](#Xe571fa566fc783417b04b6263275643482d7f51)
* [2. Information System Categorization](#X83f798301692f6aa72c318d5e2ba410452831e5)
  + [2.1. Information Types](#Xb46cc86f6c6dd544c742670cbad64e5ba5cfb82)
  + [2.2. Security Objectives Categorization (FIPS 199)](#X99ab91dfb788fff556f5ecfe615a7ede4c63fa6)
* [3. Information System Owner](#X7d2819236c9a842457b4e8ac62b2bb927c29287)
* [4. Independent Assessor](#Xb8408773cbe3e55387e10e8392c5179b4aa9be1)
* [5. Authorizing Official](#X7f900ff511ad12d5b0c7626b536dbd1b16160b1)
* [6. Other Designated Contacts](#X8dc2563ff258846d407c3abafd26e7acc9aeb4f)
* [7. Assignment of Security Responsibility](#X2d0e82b080034124caa1cb3a68cd70143ffe31b)
* [8. Information System Operational Status](#X8900fced630672b15dd816566d69d59f558f4ac)
* [9. Information System Type](#Xc164f973d61cf1b6e95a2e92c50c046e8bc3ee0)
  + [9.1. Cloud Service Models](#Xc16d6b8a97c791bf0572cd9feaa547c302bb9bb)
  + [9.2. Cloud Deployment Models](#X64274166fd8acc9bab9613ffbe717d3d746a38d)
  + [9.3. Leveraged Authorizations](#Xef14e6dfd204a9ee176b5d0859b4eb622c42504)
* [10. General System Description](#X0e105ade24275f8c510c75bbb3cd938d3b352f3)
  + [10.1. System Function or Purpose](#X32bda3b7f01785333ff4f52a235fcde2b2b4104)
  + [10.2. Information System Components and Boundaries](#Xf053c08e68c9f39226fcd945a257d8aee584323)
  + [10.3. Types of Users](#Xc5070976e6069fed53a76385758663cb3e83272)
  + [10.4. Network Architecture](#Xd92d89a24aca4811611e15847f42f2b140df8fc)
* [11. System Environment](#X5a74c06febec4adcbcd5fbf9f4ab9357b95104f)
  + [11.1. Hardware Inventory](#Xaa1d4e8f5a41cd3d5772c0eae942e964a3d8f70)
  + [11.2. Software Inventory](#X59e68934d73ffa413b7b046801fd295ad6c4f31)
  + [11.3. Network Inventory](#X82a9b597f670948f479cb1ce7744cc171a276b1)
  + [11.4. Data Flow](#X259a01749e963f0727c622ad0e4f893b576335f)
  + [11.5. Ports, Protocols, and Services](#Xfdec493ac354cc396fe7766622d9b809bbf2cae)
* [12. System Interconnections](#X155541915b7e23a28a2526b560942dffaff5eda)

## 1. Information System Name

This FISMA Low Impact Framework provide an overview of the security requirements for the *Project Full Name* (*Project*) 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 (IT) systems is essential to ensure the required risk impact level of confidentiality, integrity, and availability of the data transmitted, processed, or stored by the *Project* system is in place and operating as intended.

The security safeguards implemented for the *Project* system meet the policy and control requirements set forth in this FISMA Low Impact Framework. All systems are subject to monitoring, consistent with applicable laws, regulations, agency policies, procedures, and practices.

Table 1‑1. **Information System Identifier, Name, and Abbreviation**

| **Unique Identifier** | **Information System Name** | **Information System Abbreviation** |
| --- | --- | --- |
| None | Project Full Name | Project |

## 2. Information System Categorization

The overall *Project* sensitivity categorization is recorded in Table 2.1, Security Categorization, which follows. The completed FedRAMP FIPS 199 document is included in this document as Attachment 3 – FedRAMP FIPS Security Categorization.

Table 2‑1. **System Security Categorization**

|  |  |
| --- | --- |
| **System Sensitivity Level:** | Low Impact |

### 2.1. Information Types

This section describes how the information types used by *Project* are categorized for confidentiality, integrity, and availability of sensitivity levels.

The following tables identify the information types that are input, stored, processed, and/or output from *Project*. The selection of the information types is based on guidance provided by the Office of Management and Budget (OMB) Federal Enterprise Architecture (EA) Program Management Office (PMO) Business Reference Model 2.0, National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, and NIST Special Publication 800-60 (NIST SP 800-60), Guide for Mapping Types of Information and Information Systems to Security Categories.

FIPS 199[1] allows for a full range of information types. In order to meet specific, niche needs of systems, Agencies can specify the types of information being placed in the cloud environment. For FISMA Low Impact, Agencies can specify the type(s) of information that will reside in FISMA Low Impact applications/systems.

To be considered a FISMA Low Impact cloud application/service, the answer to all of the following questions must be “yes:”

1. Does the service operate in a cloud environment?
2. Is the cloud service fully operational?
3. Is the cloud service a Software as a Service (SaaS), as defined by NIST SP 800-145, The NIST Definition of Cloud Computing?
4. Does the cloud service contain no personally identifiable information (PII), except as needed to provide a login capability (username, password and email address)?
5. Is the cloud service low-security-impact, as defined by FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems?
6. Is the cloud service hosted within a FedRAMP-authorized Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), or is the CSP providing the underlying cloud infrastructure?

Table 2‑2. **Sensitivity Categorization of Information Types for the *Project* System**

| **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** | **Statement for Impact Adjustment Justification** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Training Materials | Low | Low | Low | Low | Low | Low | Training materials is not classified, or FOUO. Users only have access to the training if the instructor grants access to the Training content. All students are vetted prior to coming to the training class and are granted access control to all training material within his/her course |
| Profile Information | Low | Low | Low | Low | Low | Low | Users have the option of sharing his/her profile information. Information is considered business rolodex information and doesn’t contain financial information or highly sensitive information. User account information is encrypted with 256 bit encryption using FIPS 140-2 compliant security requirements and requires multi-factor authentication and privileged user access to access user accounts. |

### 2.2. Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2.2, Sensitivity Categorization of Information Types for the *Project* default to the high-water mark for the Information Types as identified in Table 2.3, Security Impact Level, below.

If the security impact level for confidentiality, integrity, and availability for any of the identified data types is moderate or high, the information system is not a FISMA Low Impact system. The Cloud Service Provider (CSP) must meet the standard FedRAMP Low, Moderate, or High impact baseline security requirements, as applicable, and complete the requirement documentation.

Table 2‑4. **Security Impact Level**

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

Through careful review and analysis, the baseline security categorization for the *Project* system has been determined and is listed in Table 2.5, Baseline Security Configuration, which follows.

Table 2‑5. **Baseline Security Configuration**

|  |  |
| --- | --- |
| *Project* Security Categorization | Low |

Using this categorization, in conjunction with the risk assessment and any unique security requirements, the security controls for this system have been established as detailed in this FISMA Low Impact Framework.

## 3. Information System Owner

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

Table 3‑1. **Information System Owner**

| **Information System Owner Information** |  |
| --- | --- |
| **Name** | John Manager |
| **Title** | Program Manager, System Owner |
| **Company / Organization** | Client Full Name |
| **Address** | None |
| **Phone Number** | 555.555.1234 |
| **Email Address** | john.manager@example.com |

## 4. Independent Assessor

The following individual is identified as the Independent Assessor for this system.

Table 4‑1. **Independent Assessor**

| **Independent Assessor Information** |  |
| --- | --- |
| **Name** | Jane Assessor |
| **Title** | System Assessor |
| **Company / Organization** | Client Full Name |
| **Address** | None |
| **Phone Number** | 555.555.2345 |
| **Email Address** | jane.assessor@example.com |

## 5. Authorizing Official

The Authorizing Official (AO) or Designated Approving Authority (DAA) for the Project Full Name is the None.\*

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

Table 6‑1. **Information System AO Management Point of Contact**

| **Information System AO Management Point of Contact** |  |
| --- | --- |
| **Name** | Jan Poc |
| **Title** | Authorizing Official |
| **Company / Organization** | Client Full Name |
| **Address** | None |
| **Phone Number** | 555.555.3456 |
| **Email Address** | jan.poc@example.com |

## 7. Assignment of Security Responsibility

The Project Full Name Information System Security Officer (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

Table 7‑1. **Internal ISSO (or Equivalent) Point of Contact**

| **Internal ISSO (or Equivalent) Point of Contact** |  |
| --- | --- |
| **Name** | AWS East/West |
| **Title** | Information Systems Security Officer (ISSO) |
| **Company / Organization** | Amazon Web Services |
| **Address** | None |
| **Phone Number** | 555.555.5678 |
| **Email Address** | staff@amazon.com |

Table 7‑2. **AO ISSO Point of Contact**

| **AO ISSO Point of Contact** |  |
| --- | --- |
| **Name** | Jim Issopoc |
| **Title** | Information Systems Security Manager (ISSM) |
| **Company / Organization** | Client Full Name |
| **Address** | None |
| **Phone Number** | 555.555.6789 |
| **Email Address** | jim.issopoc@example.com |

## 8. Information System Operational Status

The system is currently in the life-cycle phase shown in Table 8.1, System Status, which follows. Only operational systems can be granted an Authority to Operate (ATO).

Table 8‑1. **System Status**

| **System Status** |  |
| --- | --- |
| Major Modification | The system is undergoing a major change, development, or transition. |

## 9. Information System Type

The *Project* makes use of unique managed service provider architecture layer(s).

### 9.1. Cloud Service Models

Information systems, particularly those based on cloud architecture models, are made up of different service layers. Below are some questions that can help system owners determine if their system is a cloud followed by specific questions to help system owners determine the type of cloud.

Table 9‑1. **Determining a Cloud System**

| **Question (Yes/No)** | **Conclusion** |
| --- | --- |
| Does the system use virtual machines (VM)? | 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 customer to build anything other than servers? | A no response means that the system is an Infrastructure as a Service (IaaS). A yes response means that the system is either a Platform as a Service (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 Application Programming Interfaces (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 *Project* defined in this FISMA Low Impact Framework are indicated in Table 9.2, Service Layers Represented in this FISMA Low Impact Framework, which follows.

Table 9‑2. **Service Layers Represented in this FISMA Low Impact Framework**

| **Service Provider Architecture Layers** |  |
| --- | --- |
| Software as a Service (SaaS) | Major Application |

### 9.2. Cloud Deployment Models

Information systems are made up of different deployment models. The deployment models of the *Project* that are defined in this FISMA Low Impact Framework, and that are not leveraged by any other FedRAMP Authorizations, are indicated in Table 9.3, Cloud Deployment Model Represented in this FISMA Low Impact Framework, which follows.

Table 9‑3. **Cloud Deployment Model Represented in this FISMA Low Impact Framework**

| **Service Provider Cloud Deployment Model** |  |
| --- | --- |
| Public | Cloud services and infrastructure supporting multiple organizations and agency clients. |

### 9.3. Leveraged Authorizations

The *Project* leverages a pre-existing FedRAMP Authorized IaaS and/or PaaS. FedRAMP Authorizations leveraged by this *Project* are listed in Table 9.4, Leveraged Authorizations, which follows.

Table 9‑4. **Leveraged Authorizations**

| **Leveraged Information System Name** | **Leveraged Service Provider Owner** | **Date Granted** |
| --- | --- | --- |
|  |  |  |

## 10. General System Description

This section includes a general description of the *Project* system.

### 10.1. System Function or Purpose

The Project uses Open Source Software and is a web based social business tool built on top of a Content Management System (CMS).

### 10.2. Information System Components and Boundaries

The accreditation boundary includes applications and guest operating systems that reside on the AWS Infrastructure-as-a-Service (IaaS).

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 10.1, Authorization Boundary Diagram, below.

Figure 10‑1. **Authorization Boundary Diagram** Network Diagram

### 10.3. 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 10.1, Personnel Roles and Privileges, which follows.

Table 10‑1. **Personnel Roles and Privileges**

| **Role** | **Internal or External** | **Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)** | **Sensitivity Level** | **Authorized Privileges** | **Functions Performed** |
| --- | --- | --- | --- | --- | --- |
| AWS Dashboard Administrator | Internal | P | Moderate | AWS Dashboard access | Add/remove virtual hardware, manage backup and restore server |
| UNIX System Administrator | Internal | P | Moderate | Full administrative access (root) | Add/remove system users, install and configure software, OS updates, patches and hotfixes |
| Site Administrator | Internal | P | Limited | Full Application Access | Application configuration, external user permissions, and content management |
| Manager | Internal | P | N/A | Extended Application Access | Limited user permissions and content management. |
| Editor | Internal | NP | N/A | General Users | Create, edit and delete content. |
| Authenticated User | Internal | NP | N/A | General Users | View published content and post comments. |

The Project uses groups for access to most content. \* **Unauthenticated Users** – *Unauthenticated users* have limited access to content on the Project. They can only access content that is marked as *Public* and can request membership to *Organizations* and *Groups*.

* **Authenticated Users** – Users need to be request access, or be added to *Groups*.
* **Group Manager** – *Group Managers* is responsible for managing the content and members for a group.
* **Group Members** – *Group Members* can access public content as well as content specific to their groups.

### 10.4. Network Architecture

Assessors should be able to easily map hardware, software, and network inventories back to this diagram.

The logical network topology is shown in Figure 10.2, Network Diagram, mapping the data flow between components.

Figure 10.2, Network Diagram(s), provides a visual depiction of the system network components that constitute the *Project* system.

Figure 10‑2. **Network Diagram** Network Diagram

## 11. System Environment

The FedRAMP Inventory Workbook is included in this document in ATTACHMENT 2 – FedRAMP Inventory Workbook.

### 11.1. Hardware Inventory

Use the FedRAMP Inventory Workbook to list the principal hardware components for *Project*.

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

### 11.2. Software Inventory

Use the FedRAMP Inventory Workbook to list the principal software components for *Project*.

### 11.3. Network Inventory

Use the FedRAMP Inventory Workbook to list the principal network devices and components for *Project*.

### 11.4. Data Flow

The data flow in and out of the system boundaries is represented in Figure 11.1, Data Flow Diagram, below.

Figure 11‑1. **Data Flow Diagram**

### 11.5. Ports, Protocols, and Services

Table 11.1, Ports, Protocols, and Services, lists the ports, protocols, and services enabled for the *Project*.

Table 11‑1. **Ports, Protocols, and Services**

| **Ports (TCP/UDP)** | **Protocols** | **Services** | **Purpose** | **Used By** |
| --- | --- | --- | --- | --- |
| 22 | TCP | SSH Bastion | SSH acces to server | System Administrator |
| 53 | TCP/UDP | AWS DNS | DNS service within AWS | None |
| 123 | UDP | AWS NTP | Network time protocol | None |
| 443 | TCP | AWS ELB | Load balancing | None |
| 3306 | TCP | Amazon RDS | Database | None |
| 5044 | TCP/UDP | SSH/rsync audit records | Elasticsearch (from all instances in VPC) | None |
| 8983 | TCP | Solr | Solr search | None |
| 443 | TCP | CMS | CMS update | CMS |
| 443 | TCP | ClamAV | ClamAV definitions updates | ClamAV |
| 443 | TCP | BrowseCap | Determine browser capabilities | CMS |
| 443 | TCP | GitLab | Used to pull in code changes via git pull | CMS |
| 443 | TCP | GitLab docker registry | Used to pull in docker images | Audit |
| 443 | TCP | OpsGenie | AWS CloudWatch pings OpsGenie | all instances |
| 443 | TCP | yum | RHEL (AWS mirrors) - Repo Lists | all instances |
| 443 | TCP | LetsEncrypt | SSL certificates | all instances |
| 25 | TCP | AWS SES | AWS Simple Email Service (from all) | None |
| 636 | TCP | OCSP | Online Certificate Status Protocol | CMS |
| 143 | TCP/UDP | IMAP | Spam report management | CMS |
| 993 | TCP/UDP | IMAPS | Spam report management | CMS |
| 443 | TCP | pip | Python package management | Python |

## 12. System Interconnections

There are no System Interconnections.