Lightweight Process

System Security Plan (SSP) for

Amazon Web Services (AWS)



Beta FEC

Information System

FIPS 199 Low Impact

V 1.2

Month Day, Year

**Controlled Unclassified Information (CUI)**

System Security Plan

Prepared by

|  |  |  |
| --- | --- | --- |
| Identification of Organization that Prepared this Document | | |
| http://t1.gstatic.com/images?q=tbn:QU0RGXzmgr2vDM:http://www.jeffshupack.com/wp-content/uploads/2009/08/gsa-logo.jpg  <**insert logo**> | Organization Name | GSA OCISO and FEC Team, 18F |
| Street Address | 1800 F St, NW |
| Suite/Room/Building |  |
| City, State Zip | Washington, DC 20405 |

Executive Summary

This document details the System Security Plan (SSP) for the Beta FECsecurity controls. This System Security Plan was written in accordance with National Institute of Standards and Technology (NIST) *Special Publication (SP) 800-18, Revision 1, Guide for Developing Security Plans for Information Technology Systems*. Completion of this SSP, which describes how U.S. federal information will be safeguarded, is a requirement of the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, the Computer Security Act of 1987.

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Description** | **Version of System** | **Author** |
| 10/31/2016 | Initial Draft | 1.0 | Lindsay Young, Carlo Costino, Noah Manger |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

1. Information System Name/Title

2. Information System Categorization

2.1. Information Types

2.2. Security Objectives Categorization (FIPS 199)

2.3. E-Authentication Determination (E-Auth)

3. Information System Owner

4. Authorizing Official

5. Other Designated Contacts

6. Assignment of Security Responsibility

7. Information System Operational Status

8. Information System Type

8.1. System Type

8.2. Leveraged Provisional Authorizations

9. General System Description

9.1. System Function or Purpose

9.2. Information System Components and Boundaries

9.3. Types of Users

9.4. Network Architecture

10. System Environment

10.1.1. Hardware Inventory

10.1.2. Software Inventory

10.1.3. Network Inventory

10.1.4. Data Flow

10.1.5. Ports, Protocols and Services

11. System Interconnections

12. Applicable Laws and Regulations

12.1. Applicable Laws

12.2. Applicable Standards and Guidance

13. Minimum Security Controls

13.1. Account Management (AC-2)

13.2. Access Enforcement (AC-3)

13.3. Least Privilege (AC-6)

13.4. Audit Events (AU-2)

13.5. Audit Review, Analysis, and Reporting (AU-6)

13.6. Penetration Testing (CA-8)

13.7. Baseline Configuration (CM-2)

13.8. Configuration Change Control (CM-3)

13.9. Configuration Settings (CM-6)

13.10. Information System Component Inventory (CM-8)

13.11. User Identification and Authentication (IA-2)

13.12. Control Enhancement IA-2 (1)

13.13. Control Enhancement IA-2 (2)

13.14. Control Enhancement IA-2 (12)

13.15. Information Security Architecture (PL-8)

13.16. Vulnerability Scanning (RA-5)

13.17. Control Enhancement SA-22

13.18. Boundary Protection (SC-7)

13.19. Cryptographic protection (SC-13)

13.20. Control Enhancement SC-28 (1)

13.21. Flaw Remediation (SI-2)

13.22. Information system monitoring (SI-4)

13.23. Information Input validation (SI-10)

1. **Information System Name/Title**

This System Security Plan provides an overview of the security requirements for the Beta FEC 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 an asset 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 systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the Beta FEC information system.

The security safeguards implemented for the Beta FEC system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

**Table 1-1. Information System Name and Title**

|  |  |  |
| --- | --- | --- |
| Unique Identifier | Information System Name | Information System Abbreviation |
| FE9531BP17H0004 | Beta FEC | Beta FEC |

1. **Information System Categorization**

The overall information system sensitivity categorization is noted in the table that follows.

**Table 2-1. Security Categorization**

|  |  |
| --- | --- |
| Low | ☒ |
| Moderate | ☐ |
| High | ☐ |

* 1. **Information Types**

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

The following tables identify the information types that are input, stored, processed, and/or output from Beta FEC. The selection of the information types is based on guidance provided by OMB Federal Enterprise Architecture Program Management Office Business Reference Model 2.0, and FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems* which is based on NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

The tables also identify the security impact levels for confidentiality, integrity, and availability for each of the information types expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity, and availability) discussed in NIST SP 800-60 and FIPS Pub 199.

The potential impact is *low* if—

- The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

- A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is *moderate* if—

- The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

- A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is *high* if—

- The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

- A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.





**Note:** The information types found in NIST SP 800-60, Volumes I and II

Revision 1 are the same information types found in the Federal Enterprise Architecture (FEA) Consolidated Reference Model.



**Table 2-2. Sensitivity Categorization of Information Types**

|  |  |  |  |
| --- | --- | --- | --- |
| Information Type | Confidentiality | Integrity | Availability |
| Campaign Finance, How campaigns raise and spend money | Open data | Correct data on election spending is part of the FEC’s efforts to administer and enforce the Federal Election Campaign Act (FECA) | Important information about campaign finance would not be available. Disclosure of this information is also required by law. |
| Legal, regulatory and enforcement actions | Open data | Voluntary compliance to FECA is part of the FEC’s efforts of the administer and enforce FECA. People need to know laws, regulations and administrative actions to know how to be compliant. | Important information about campaign finance compliance would not be available. This would limit people’s ability to find out how to stay in compliance. Disclosure of this information is also required by law. |
| General information about the Federal Election Commission, its updates, press outreach and events. | Open data | FEC uses these resources to inform and educate the public about the FEC and its activities. | This might limit people's knowledge and access to FEC events, like hearings and other official duties. |

* 1. **Security Objectives Categorization (FIPS 199)**

Based on the information provided in Table 2-2, Information Types, for the Beta FEC default to the high-water mark for the noted Information Types as identified in the table below.

**Table 2-3. Security Impact Level**

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



**Note:** Please refer to *FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems.*



Through review and analysis it has been determined that the baseline security categorization for the Beta FEC system is listed in the table that follows.

**Table 2-4. Baseline Security Categorization**

|  |  |
| --- | --- |
| Beta FEC Security Categorization | Low |

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

* 1. **E-Authentication Determination (E-Auth)**

The information system e-Authentication Determination is described in the table that follows.

**Table 2-5. E-Authentication Questions**

|  |  |  |
| --- | --- | --- |
| Yes | No | E-Authentication Question |
| ☒ | ☐ | Does the system require authentication via the Internet? |
| ☒ | ☐ | Is data being transmitted over the Internet via browsers? |
| ☒ | ☐ | Do users connect to the system from over the Internet? |





**Note:** Please refer to *OMB Memo M-04-04 E-Authentication Guidance for*

*Federal Agencies* for more information on e-Authentication.



The summary E-Authentication Level is recorded in the table that follows.

**Table 2-6. E-Authentication Level Determination**

|  |  |
| --- | --- |
| E-Authentication Determination | |
| System Name | Beta FEC |
| System Owner | Lindsay Young |
| Assurance Level |  |
| Date Approved |  |

1. **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**

|  |  |
| --- | --- |
| Name | Lindsay Young |
| Title | Innovation Specialist |
| Company / Organization | GSA 18F |
| Address | 1800 F Street, Washington, DC |
| Phone Number | 202-222-5427 |
| Email Address | lindsayn.young@gsa.gov |

1. **Authorizing Official**

The Authorizing Official (AO) for this information system is defined below.

**Table 4-1. Authorizing Official Point of Contact**

|  |  |
| --- | --- |
| Name |  |
| Title | Noah Kunin |
| Company / Organization | GSA TTS |
| Address | 1800F Street, Washington, DC |
| Phone Number | 202-577-7167 |
| Email Address | noah.kunin@gsa.gov |

1. **Other Designated Contacts**

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

**Table 5-1. Information System Management Point of Contact**

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Company / Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

**Table 5-2. Information System Technical Point of Contact**

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Company / Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

1. **Assignment of Security Responsibility**

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

**Table 6-1. System ISSO (or Equivalent)**

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Company / Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

1. **Information System Operational Status**

The system is currently in the life-cycle phase noted in the table that follows.

**Table 7-1. System Status**

|  |  |  |
| --- | --- | --- |
| System Status | | |
| ☒ | Operational | The system is operating and in production. |
| ☐ | Under Development | The system is being designed, developed, or implemented |
| ☐ | Major Modification | The system is undergoing a major change, development, or transition. |
| ☐ | Other | Explain: |



1. **Information System Type**

The Beta FEC makes use of unique managed service provider architecture layer(s).

* 1. **System Type**

**Table 8-1. SSP System Type**

|  |  |
| --- | --- |
| Service Provider Architecture Layers | |
| ☒ | Major Application |
| ☐ | General Support System |



* 1. **Leveraged Provisional Authorizations**

The Beta FEC plans to leverage a pre-existing Provisional Authorization. Provisional Authorizations leveraged by this Beta FEC are noted in the table that follows.

**Table 8-2. Leveraged Authorizations**

|  |  |  |
| --- | --- | --- |
| Information System Name | Service Provider Owner | Date Granted |
| AWS FedRamp Agency ATO (issued by the HHS) | Amazon | May 13, 2013 |

1. **General System Description**

The Federal Election Commission (FEC) releases information to the public about money that's raised and spent in federal elections — that's elections for US president, Senate, and House of Representatives.

Are you interested in seeing how much money a candidate raised? Or spent? How much debt they took on? Who contributed to their campaign? The FEC is the authoritative source for that information.

betaFEC is a collaboration between 18F and the FEC. It aims to make campaign finance information more accessible (and understandable) to all users.

All FEC repositories:

* FEC: a general discussion forum. We compile feedback from betaFEC's feedback widget here, and this is the best place to submit general feedback.
* openFEC: betaFEC's API
* swagger-ui: forked repo that generates our interactive API documentation
* openFEC-web-app: the web app for exploring campaign finance data
* fec-style: shared styles and user interface components, including this project's glossary and feedback tools
* fec-cms: this project's content management system (CMS)
* fec-proxy: this is a lightweight app that coordinates the paths between the web app and CMS
  1. **System Function or Purpose** 

BetaFEC is the emerging full-scale replacement for the existing suite of content and applications hosted at fec.gov. As a product hosted at beta.fec.gov, it provides three distinct themes of value related to the Federal Election Commission’s mission:

1. **Disclose federal campaign finance data:** beta.fec.gov/data makes federal campaign finance data easier to find, use and understand. It provides users the ability to browse through the FEC’s open data sets as raw and processed data and explore trends and summaries through data visualizations. It allows users to explore and compare the financial details of candidates, PACs and political party committees in order make informed decisions and understand the flow of money in the political process.
2. **Assist candidates and campaign committees exercise voluntary compliance:** BetaFEC includes static content designed to make it easier for people and groups participating in federal elections understand what they need to do to be legally compliant in their activities, and to give them the information they need to be able to file and report their financial activity.
3. **Give legal professionals access to the information they need to make informed legal decisions:** BetaFEC makes it easier to search and browse through the FEC’s statutes, regulations, Advisory Opinions, enforcement matters and more in order to derive the most up-to-date interpretation of the law and make informed legal decisions.
   1. **Information System Components and Boundaries**

BetaFEC consists of the following components hosted on cloud.gov:

1. **The OpenFEC API:** This API exposes data stored in a Postgres database hosted on Amazon Web Services, which in turn is provided data pushed from the FEC’s databases via nightly updates. The API has a Redis instance, Celery worker, and an ElasticSearch instance. Static exports of data from the API can be triggered from the front-end application and these in turn are stored in an S3 bucket. The API uses a secrets service for credential management. It uses Mandrill for emailing error messages and New Relic for reporting errors. Users access the API via the api.data.gov umbrella.
2. **The OpenFEC web app:** This Flask app provides the front-end web site for accessing data provided by the API, which it access via api.data.gov. The app uses the secrets service for credential management. It uses Sentry and New Relic for error monitoring and reporting. Users may submit feedback via a form that posts issues to GitHub’s issues API. Users may also sign up to be usability test participants via an embedded form provided by Ethnio.
3. **The FEC CMS:** This is an instance of Wagtail CMS, which is based on Django. The CMS hosts written content, as well as a dynamic calendar populated by data from the API. It has its own Postgres database for storing content and its own secrets service for credential management. It uses New Relic for error reporting, Sentry for monitoring. And it also provides the option to submit comments to GitHub issues (via a form that submits to a route on the OpenFEC web app), and the ability to sign up for usability tests via an embedded Ethnio form.
4. **A proxy app:** The web app (2) and the CMS (3) are accessed via a proxy app.
5. **FEC eRegulations:** The FEC eRegulations instance has its own Postgres database and secrets service for credential management. It uses New Relic for reporting. The platform consists of:
   1. The regulations site
   2. The regulations core
   3. The regulations parser

All applications are deployed by TravisCI.

* 1. **Types of Users**

All users have their employee status categorized with a sensitivity level in accordance with PS-2. 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 the table that follows.



**Table 9-1. User Roles and Privileges**

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Internal or External | Sensitivity Level | Authorized Privileges and Functions Performed |
| Data Admins | internal |  | Maintain databases and website with connections to the AWS databases, cloud.gov and GitHub. |
| CMS Admins | internal |  | Content creators for the CMS web content |
| public | external | Not applicable | visit the website’s various pages and make calls to the API |



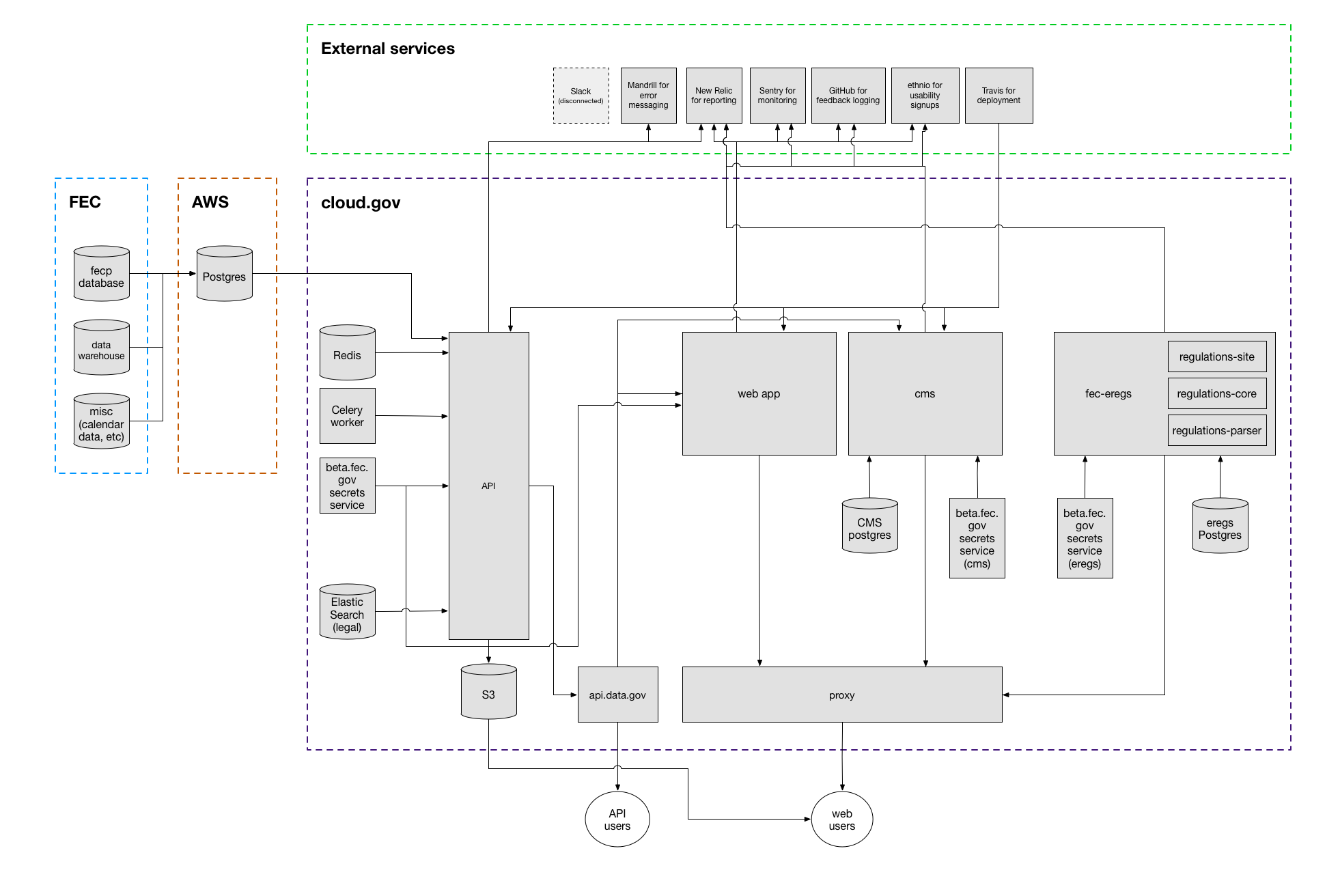
**Note:** User roles typically align with Active Directory, LDAP, Role-based Access Controls (RBAC), NIS and UNIX groups, and/or UNIX netgroups.



There are currently tens of internal users and thousands of external users. Within one year, it is anticipated that there will be tens of internal users and thousands of external users.

* 1. **Network Architecture** 

The following architectural diagram(s) provides a visual depiction of the major hardware components that constitute Beta FEC.



**Figure 10-1. Network Diagram**

1. **System Environment** 
   * 1. **Hardware Inventory**

The following table lists the principal server hardware components for Beta FEC.



**Table 10-1. Server Hardware Components**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Hostname | Make | Model and Firmware | Location | Components that Use this Device |
| None |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |



**Note:** A complete and detailed list of the system hardware and software

inventory is required per NIST SP 800-53, Rev 4 CM-8.



* + 1. **Software Inventory**

[See hostnames in attachment A]



**Table 10-2. Software Components**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Hostname | Function | Version | Patch Level | Virtual (Yes / No) |
|  | Development database instance used for active development of the betaFEC site | Amazon RDS PostgreSQL 9.5 | 9.5.4 | Yes |
|  | Development read replica database instance used for testing during development of the betaFEC site | Amazon RDS PostgreSQL 9.5 | 9.5.4 | Yes |
|  | Staging database instance used for testing features and work of an upcoming release of software of the betaFEC site | Amazon RDS PostgreSQL 9.5 | 9.5.4 | Yes |
|  | Production database instance used to power the live user-facing site of the betaFEC site | Amazon RDS PostgreSQL 9.5 | 9.5.4 | Yes |
|  | Production read replica database instance used to serve all read-only traffic in the production environment of the betaFEC site | Amazon RDS PostgreSQL 9.5 | 9.5.4 | Yes |
|  | Development Amazon S3 bucket for testing new feature development requiring file storage for data exports of the betaFEC site | cloud.gov s3 (basic) service |  | Yes |
|  | Staging Amazon S3 bucket for testing upcoming release functionality requiring file storage for data exports of the betaFEC site | cloud.gov s3 (basic) service |  | Yes |
|  | Production Amazon S3 bucket for storing export files generated by the live user facing betaFEC site | cloud.gov s3 (basic) service |  | Yes |
|  | Development Elasticsearch service for testing new feature development requiring search on the betaFEC site | cloud.gov elasticsearch-swarm-1.7.1 (1x) service | 1.7.1 | Yes |
|  | Secondary development Elasticsearch service for testing new feature development requiring search on the betaFEC site | cloud.gov elasticsearch-swarm-1.7.1 (3x) service | 1.7.1 | Yes |
|  | Staging Elasticsearch service for testing upcoming release functionality requiring search on the betaFEC site | cloud.gov elasticsearch-swarm-1.7.1 (1x) service | 1.7.1 | Yes |
|  | Secondary Staging Elasticsearch service for testing upcoming release functionality requiring search on the betaFEC site | cloud.gov elasticsearch-swarm-1.7.1 (1x) service | 1.7.1 | Yes |
|  | Production Elasticsearch service for providing search functionality to the live user facing betaFEC site | cloud.gov elasticsearch-swarm-1.7.1 (1x) service | 1.7.1 |  |
|  | Development database instance used for active development of our content management system for the betaFEC site | cloud.gov rds (shared-psql) service |  | Yes |
|  | Staging database instance used for testing upcoming release features of our content management system for the betaFEC site | cloud.gov rds (shared-psql) service |  | Yes |
|  | Production database instance used for managing content in the live user facing betaFEC site | cloud.gov rds (shared-psql) service |  | Yes |
|  | Development Amazon S3 bucket used during active development for storing static content assets on the betaFEC site | cloud.gov s3 (basic) service |  | Yes |
|  | Staging Amazon S3 bucket used during tests of upcoming releases for storing static content assets on the betaFEC site | cloud.gov s3 (basic) service |  | Yes |
|  | Production Amazon S3 bucket used for storing static content assets on the live user facing betaFEC site | cloud.gov s3 (basic) service |  | Yes |
|  | Development Redis instance used during active development to test functionality requiring asynchronous task queue management on the betaFEC site | cloud.gov redis28-swarm (standard) service | 2.8 | Yes |
|  | Staging Redis instance used during testing of upcoming releases for functionality requiring asynchronous task queue management on the betaFEC site | cloud.gov redis28-swarm (standard) service | 2.8 | Yes |
|  | Production Redis instance used for management of asynchronous task queue on the live user facing betaFEC site | cloud.gov redis28-swarm (standard) service | 2.8 | Yes |
|  | Development Elasticsearch service for testing new feature development requiring search on the betaFEC eregs site | cloud.gov elasticsearch-swarm-1.7.1 (1x) service | 1.7.1 | Yes |
|  | Staging Elasticsearch service for testing upcoming release functionality requiring search on the betaFEC erges site | cloud.gov elasticsearch-swarm-1.7.1 (1x) service | 1.7.1 | Yes |
|  | Production Elasticsearch service for providing search functionality to the live user facing betaFEC eregs site | cloud.gov elasticsearch-swarm-1.7.1 (1x) service | 1.7.1 | Yes |
|  | Development database instance used for active development of our content management system for the betaFEC eregs site | cloud.gov rds (shared-psql) service |  | Yes |
|  | Staging database instance used for testing upcoming release features of our content management system for the betaFEC ergegs site | cloud.gov rds (shared-psql) service |  | Yes |
|  | Production database instance used for managing content in the live user facing betaFEC eregs site | cloud.gov rds (shared-psq) service |  | Yes |
|  | Development Amazon RDS instance used for active development of FEC project planner app | cloud.gov aws-rds (shared-psql) service |  |  |
|  | Development Amazon S3 instanced used for storing static content/files in active development of FEC project planner app | cloud.gov s3 (basic) service |  | Yes |

* + 1. **Network Inventory**

The following table lists the principle network devices and components for **Beta FEC**.

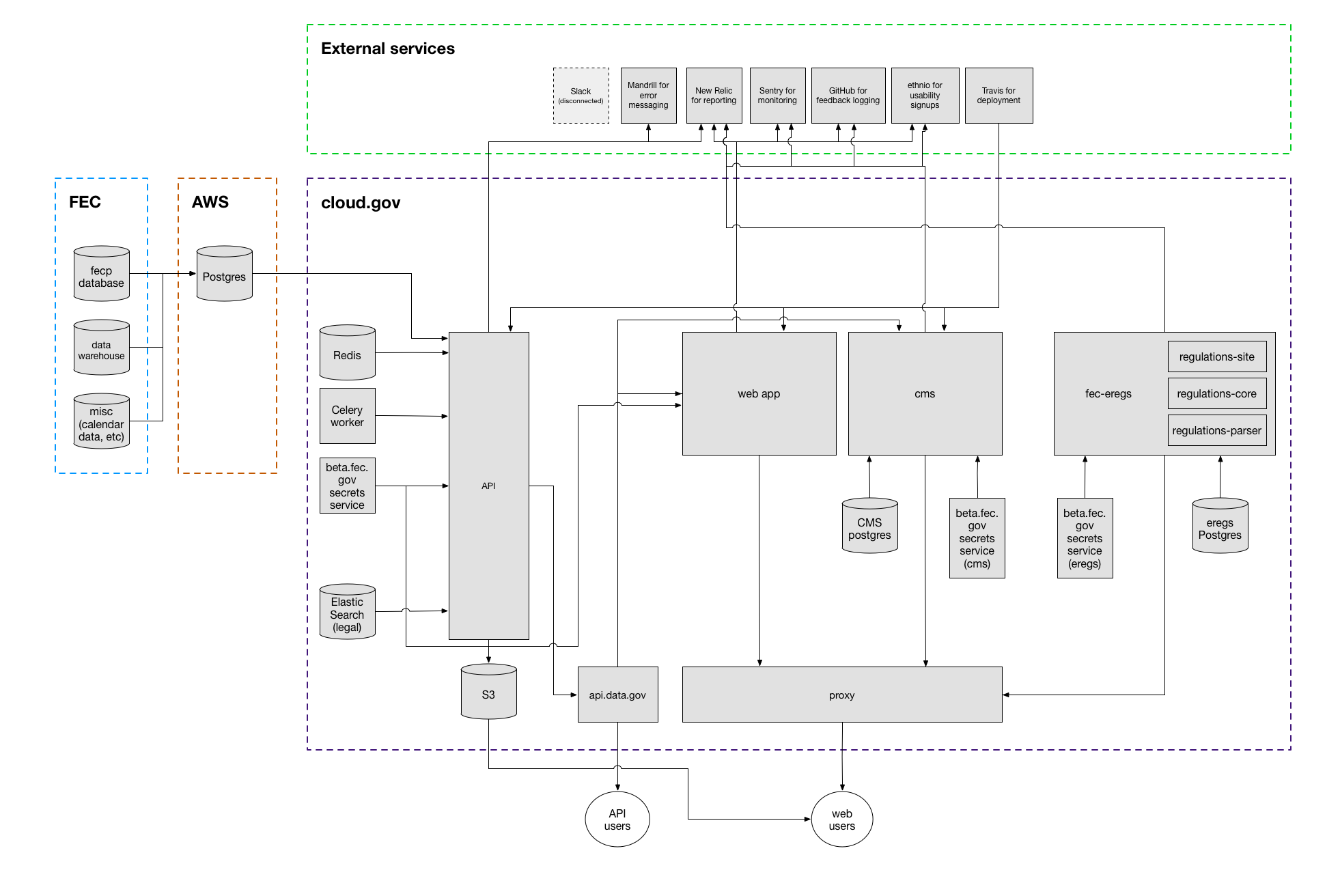


**Table 10-3. Network Components**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Hostname | Make | Model | IP Address | Function |
| (Leveraged AWS) |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Data Flow**





**Figure 10-2. Data Flow Diagram**

* + 1. **Ports, Protocols and Services**

The table below lists the Ports, Protocols, and Services enabled in this information system. TCP ports are indicated with a T and UDP ports are indicated with a U.



**Table 10-4. Ports, Protocols, and Services**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ports (T or U) | Protocols | Services | Purpose | Used By |
| 443 |  |  | internet | Web apps |
| 5432 | PostgreSQL uses a message-based protocol for communication between frontends and backends (clients and servers). The protocol is supported over TCP/IP and also over Unix-domain sockets. |  | Postgres | Postgres databases |
| 9300 | Elasticsearch transport protocol |  | Elasticsearch | Elasticsearch clusters |
|  |  |  |  |  |

1. **System Interconnections** 

[See CSP IP Address, External Organization Name and IP Address of System and Interface in Appendex B]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CSP IP Address and Interface | External Organization Name and IP Address of System | External Point of Contact and Phone Number | Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer etc.) | Data Direction (incoming, outgoing, or both) | Information Being Transmitted | Ports or Circuit # |
|  |  |  | N/A | Outgoing | Disclosure Data | 5432 |
|  |  |  | N/A | Outgoing | Disclosure Data | 5432 |
|  |  |  | N/A | Outgoing | Disclosure Data | 5432 |
|  |  |  |  |  |  |  |
|  |  |  | N/A | Outgoing | Disclosure Data | 5432 |
|  |  |  | N/A | Outgoing | Disclosure Data | 5432 |
|  |  |  | N/A | Outgoing | Disclosure Data | 5432 |
|  |  |  |  |  |  |  |
|  |  |  | N/A | Outgoing | Disclosure Data | 5432 |
|  |  |  | N/A | Outgoing | Disclosure Data | 5432 |
|  |  |  | N/A | Outgoing | Disclosure Data | 5432 |
|  |  |  |  |  |  |  |
|  |  |  | N/A | Outgoing | Disclosure Data | 5432 |
|  |  |  | N/A | Outgoing | Disclosure Data | 5432 |
|  |  |  | N/A | Outgoing | Disclosure Data | 5432 |

1. **Applicable Laws and Regulations**
   1. **Applicable Laws**

The following laws and regulations apply to the information system:

* Computer Fraud and Abuse Act [PL 99-474, 18 USC 1030]
* E-Authentication Guidance for Federal Agencies [OMB M-04-04]
* Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
* Freedom of Information Act As Amended in 2002 [PL 104-232, 5 USC 552]
* Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
* Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7]
* Internal Control Systems [OMB Circular A-123]
* Management of Federal Information Resources [OMB Circular A-130]
* Management’s Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
* Privacy Act of 1974 as amended [5 USC 552a]
* Protection of Sensitive Agency Information [OMB M-06-16]
* Records Management by Federal Agencies [44 USC 31]
* Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
* Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]
  1. **Applicable Standards and Guidance**

The following standards and guidance apply to the information system:

* CIO IT Security 14-68, LiteWeight Security Authorization Process
* A NIST Definition of Cloud Computing [NIST SP 800-145]
* Computer Security Incident Handling Guide [NIST SP 800—61, Revision 1]
* Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
* Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]
* Guide for Assessing the Security Controls in Federal Information Systems [NIST SP 800-53A]
* Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Revision 1]
* Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]
* Guide for Mapping Types of Information and Information Systems to Security Categories [NISP SP 800-60, Revision 1]
* Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]
* Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
* Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
* Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-1]
* Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 4]
* Risk Management Guide for Information Technology Systems [NIST SP 800-30]
* Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
* Security Requirements for Cryptographic Modules [FIPS Publication 140-2]
* Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
* Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]



**Note:** All NIST Computer Security Publications can be found at the following

URL: <http://csrc.nist.gov/publications/PubsSPs.html>



1. **Minimum Security Controls**
   1. **Account Management (AC-2)**

The organization:

1. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];

**AC-2a Parameter Requirement:** individual, group, system, application, guest/anonymous, and temporary

1. Assigns account managers for information system accounts;
2. Establishes conditions for group and role membership;
3. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
4. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;

**AC-2e Parameter Requirement:** GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO

1. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];

**AC-2f Parameter Requirement:** GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO

1. Monitors the use of information system accounts;
2. Notifies account managers:
   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual information system usage or need-to-know changes;
3. Authorizes access to the information system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the organization or associated missions/business functions;
4. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and

**AC-2j Parameter Requirement:** at least annually

1. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

|  |  |
| --- | --- |
| AC-2 | Control Summary Information |
| Implemented Parameter AC-2a:  Implemented Parameter AC-2e:  Implemented Parameter AC-2f:  Implemented Parameter AC-2j: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☒ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  Customers are responsible for all aspects of this control related to user account access to their compute instances, virtual networks, and block stores. Details of each aspect of EC2, VPC, and EBS are outlined below.  *EC2*  Virtual EC2 instances are completely controlled by the customer agency. Customers have full root access or administrative control over accounts, services, and applications. AWS does not have any access rights to customer instances and cannot log into the guest OS.  AWS recommends a base set of security best practices to include disabling password-only access to their servers, and utilizing some form of multi-factor authentication to gain access to their instances (or at a minimum certificate-based SSH Version 2 access).  Additionally, customers should employ a privilege escalation mechanism with logging on a per-user basis. For example, if the guest OS is Linux, after hardening their instance, they should utilize certificate-based SSHv2 to access the virtual instance, disable remote root login, use command-line logging, and use ‘sudo’ for privilege escalation.  Customers should generate their own key pairs in order to guarantee that they are unique, and not shared with other customers or with AWS.  *EBS*  Once a customer creates an Amazon EBS volume, the customer can attach it to an Amazon EC2 instance. Once attached, it will appear as a mounted device similar to any hard drive or other block device. At that point, the instance can interact with the volume just as it would with a local drive, formatting it with a file system or installing applications on it directly. The customer controls which EC2 instance an EBS volume may be attached to.  *VPC*  Through the AWS Management Console, Amazon Virtual Private Cloud (Amazon VPC) lets customers provision a private, isolated section of the Amazon Web Services (AWS) Cloud where customers can launch AWS resources in the customer-defined virtual network. Customers can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet. | |

|  |  |
| --- | --- |
| AC-2 What is the solution and how is it implemented? Discuss for both the AWS environment and Beta FEC. | |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |
| Part h |  |
| Part i |  |
| Part j |  |
| Part k |  |

* 1. **Access Enforcement (AC-3)**

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

|  |  |
| --- | --- |
| AC-3 | Control Enhancement Summary Information |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☒ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  Customers are responsible for establishing groups and permissions in the management console, thereby, ensuring that the process is performed in accordance with the customer’s access control policy and the authorizations granted to the system users are approved as required. | |

|  |
| --- |
| AC-3 What is the solution and how is it implemented? Discuss for Beta FEC. |
|  |

* 1. **Least Privilege (AC-6)**

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

|  |  |
| --- | --- |
| AC-6 | Control Enhancement Summary Information |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☒ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  Customers are responsible for employing the concept of least privilege, allowing only authorized accesses for their users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | |

|  |
| --- |
| AC-6 What is the solution and how is it implemented? Discuss for Beta FEC. |
|  |

* 1. **Audit Events (AU-2)**

The organization:

1. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];

**AU-2a Parameter Requirement:** Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.

1. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
2. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
3. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

**AU-2d Parameter Requirement:** Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. Settings to be audited continually for each identified event.

|  |  |
| --- | --- |
| AU-2 | Control Summary Information |
| Responsible Role: | |
| AU-2a Parameter:  AU-2d Parameter: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☒ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  Customers are responsible for establishing, implementing, reviewing configuring and updating auditable events on their storage resources and virtual machines, based on a risk assessment and mission/business needs. The collection and protection of these audits belongs to the customer as well. | |

|  |  |
| --- | --- |
| AU-2 What is the solution and how is it implemented? Discuss for both the AWS environment and Beta FEC. | |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

* 1. **Audit Review, Analysis, and Reporting (AU-6)**

The organization:

1. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*]; and

**AU-6a Parameter 1 Requirement:** At least weekly

**AU-6a Parameter 2 Requirement:** GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO

1. Reports findings to [*Assignment: organization-defined personnel or roles*].

**AU-6a Parameter 2 Requirement:** ISSO, ISSM, Helpdesk, and the GSA Office of the Chief Information Security Officer following the Incident Reporting Procedures in GSA IT Security Procedural Guide 01-02, Incident Response

|  |  |
| --- | --- |
| AU-6 | Control Summary Information |
| Responsible Role: | |
| Implemented Parameter AU-6a Parameter 1:  Implemented Parameter AU-6a Parameter 2:  Implemented Parameter AU-6b: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☒ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  Customers are responsible for:   1. Reviewing and analyzing information system audit records at least weekly for indications of inappropriate or unusual activity, and report’s findings to designated organizational officials; and 2. Adjusting the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. | |

|  |  |
| --- | --- |
| AU-6 What is the solution and how is it implemented? Discuss for both the AWS environment and Beta FEC. | |
| Part a |  |
| Part b |  |

* 1. **Penetration Testing (CA-8)**

The organization conducts penetration testing [*Assignment: organization-defined frequency*] on [*Assignment: organization-defined information systems or system components*].

**CA-8 Parameter 1 Requirement:** Annually

**CA-8 Parameter 2 Requirement:** Internet accessible components

|  |  |
| --- | --- |
| CA-8 | Control Enhancement Summary Information |
| Implemented Parameter CA-8 Parameter 1:  Implemented Parameter CA-8 Parameter 2: | |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☐ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  AWS operates under a model of shared responsibility between the customer and AWS. AWS provides AMIs for client VMs that, after instantiation, are fully the customer agency’s’ responsibility. These default images are not included in vulnerability scanning activities conducted by AWS. Additionally, AWS will not maintain administrator access to customer VMs.  Upon deployment of virtual machines, the customer assumes full administrator access and is responsible for performing additional application installation, configuration, patching, security hardening, operating system vulnerability scanning, web application vulnerability scanning, and database vulnerability scanning (as applicable) for assets with which they have implementation responsibility (above the hypervisor, within each instance) as necessary. Customer management of the security of their operating environment as well as conducting vulnerability scans and pen-tests shall be conducted in accordance with their own Risk Assessment, the AWS Acceptable Use Policy, and the AWS Vulnerability / Penetration Testing Request Form.  Customers that want to conduct vulnerability scans and pen-tests of their operating environment must first contact AWS for permission To do so, AWS uses a web form to collect the information necessary to review security audit requests. In order to begin the authorization process, please visit the following AWS site: <http://aws.amazon.com/security/penetration-testing/>  At the site, the customer selects the "AWS Vulnerability / Penetration Testing Request Form" link and completes the form as requested. This form also includes the AWS Terms and Policies with regard to testing. Once the form is completed and received by AWS, the authorization review process is conducted and normally takes 1-2 business days to complete. | |

|  |
| --- |
| CA-8 What is the solution and how is it implemented? Discuss for Beta FEC. |
|  |

* 1. **Baseline Configuration (CM-2)**

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

|  |  |
| --- | --- |
| CM-2 | Control Enhancement Summary Information |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☐ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  The customer is responsible for guest operating systems, deployed applications, and configuration control of select networking resources such as EC2 host firewalls, and VPC internal network configuration. The customer is not responsible for the underlying cloud infrastructure. For Virtual Machine, AWS provides a Linux Amazon Machine Image (AMIs) for the guest operating system. The installation will be the minimum installation of the operating system, with no configuration applied to the ISO image. AWS does not perform patch management, system hardening, and does not provide any application support within the image.  At customer instantiation of an AMI, the vendor makes no warranties as to the patch level or configuration settings. Customer responsibility includes updating any instance to a recent patch level and configuring to suit specific needs.  Upon deployment of AMIs, the customer assumes full administrator access and is responsible for performing additional configuration, patching, security hardening, vulnerability scanning and application installation, as necessary. AWS will not maintain administrator access to customer EC2 instances, EBS storage or VPCs. | |

|  |
| --- |
| CM-2 What is the solution and how is it implemented? Discuss for Beta FEC. |
|  |

* 1. **Configuration Change Control (CM-3)**

The organization:

1. Determines the types of changes to the information system that are configuration-controlled;
2. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
3. Documents configuration change decisions associated with the information system;
4. Implements approved configuration-controlled changes to the information system;
5. Retains records of configuration-controlled changes to the information system for [*Assignment: organization-defined time period*];

**CM-3e Parameter Requirement:** Retained for a period of not less than 1 year or in accordance with record retention policies and procedures; whichever is greater.

1. Audits and reviews activities associated with configuration-controlled changes to the information system; and
2. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board)*] that convenes [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].

**CM-3g Parameters 1-3 Requirement:** GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO**.** Systems shall establish a central means (bulletin, status page, etc) of communicating major changes/development affecting services.

|  |  |
| --- | --- |
| CM-3 | Control Summary Information |
| Responsible Role: | |
| Implemented Parameter CM3e:  Implemented Parameter CM3g Paramter 1:  Implemented Parameter CM3e Parameter 2:  Implemented Parameter CM3e Parameter 3: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☒ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  The customer is responsible for establishing a Configuration Change Control process for their information systems built on the AWS infrastructure. This includes controlling the configuration of the guest Operating System and any applications that are installed on the customer’s instances.  Additionally, the customer is responsible for testing, validating, analyzing changes to their information system built on the AWS infrastructure to determine potential security impacts, and documenting changes to the information system before implementing the changes on their operational systems built on the AWS infrastructure. This also includes the guest Operating System and any applications that are installed on the customer’s instances. | |

|  |  |
| --- | --- |
| CM-3 What is the solution and how is it implemented? Discuss for both the AWS environment and Beta FEC. | |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

* 1. **Configuration Settings (CM-6)**

The organization:

1. Establishes and documents configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;

**CM-6a Parameter Requirement:** GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines in hardening their systems, as deemed appropriate by the GSA Authorizing Official. Implemented checklists must be integrated with Security Content Automation Protocol (SCAP) content (if available and/or to the greatest extent possible.)

1. Implements the configuration settings;
2. Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and

**CM-6c Parameter Requirement 1:** All information system components

**CM-6c Parameter Requirement 2:** GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO.

1. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.



**Note:** Information on the USGCB checklists can be found at: [*http://usgcb.nist.gov/usgcb\_faq.html#usgcbfaq\_usgcbfdcc\*](http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc/)

Information on SCAP can be found at:

[*http://scap.nist.gov/*](http://scap.nist.gov/)



|  |  |
| --- | --- |
| CM-6 | Control Summary Information |
| Responsible Role: | |
| Implemented Parameter CM6a:  Implemented Parameter CM6c Parameter 1:  Implemented Parameter CM6c Parameter 2: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☐ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  The customer is responsible for establishing, documenting, implementing, monitoring and controlling changes to configuration on their information systems built on the AWS infrastructure. This includes identifying, documenting, and approving exceptions from the mandatory configuration settings for customer instances within their information system. The customer is also responsible for the security configurations of guest operating systems, deployed applications, and configuration control (through automated mechanisms where possible) of select networking resources such as EC2 host firewalls, and VPC internal network configuration.  AMIs contain standard releases from OS vendors such as Windows Server, RHEL, SUSE Linux and Ubuntu Linux. It is the customer’s responsibility to install the latest security patches after creating instances from these AMIs. The Amazon Linux AMI guest operating system is patched to a point in time, typically quarterly. However, customer responsibility includes updating any instance to a recent patch level and configuring to suit specific needs. AWS does not perform patch management, system hardening, and does not provide any application support within the image.  Upon deployment of AMIs, the customer assumes full administrator access and is responsible for performing additional configuration, patching, security hardening, vulnerability scanning and application installation, as necessary. AWS will not maintain administrator access to customer EC2 instances, EBS storage or VPCs. Customers are responsible for establishing, documenting, implementing, monitoring, and enforcing the configuration settings on their virtual machines.  Additionally the customer is responsible for incorporating a mechanism for the detection of unauthorized, security-relevant configuration changes into the customer’s incident response capability. The customer will also be responsible for controlling personnel/accounts that may change hardware/software and reviewing those privileges periodically. | |

|  |  |
| --- | --- |
| CM-6 What is the solution and how is it implemented? Discuss for Beta FEC. | |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

* 1. **Information System Component Inventory (CM-8)**

The organization:

1. Develops and documents an inventory of information system components that:
   1. Accurately reflects the current information system;
   2. Includes all components within the authorization boundary of the information system;
   3. Is at the level of granularity deemed necessary for tracking and reporting; and
   4. Includes *[Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and

**CM-8a4 Parameter Requirement:** GSA S/SO or Contractor recommended information deemed necessary to ensure property accountability that must be approved and accepted by the GSA AO. List may include hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address. See additional requirements and guidance.

1. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].

**CM-8b Parameter Requirement:** After every change.

|  |  |
| --- | --- |
| CM-8 | Control Summary Information |
| Responsible Role: | |
| Implemented Parameter CM-8a4:  Implemented Parameter CM-8b: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☐ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  The customer is responsible for developing, documenting, and maintaining an inventory of customer instances. | |

|  |  |
| --- | --- |
| CM-8 What is the solution and how is it implemented? Discuss for Beta FEC. | |
| Part a |  |
| Part b |  |

* 1. **User Identification and Authentication (IA-2)**

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

|  |  |
| --- | --- |
| IA-2 | Control Summary Information |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☒ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  *EC2*  Virtual EC2 instances are completely controlled by the customer agency. Customers have full root access or administrative control over accounts, services, and applications. AWS does not have any access rights to customer instances and cannot log into the guest OS.  AWS recommends a base set of security best practices to include disabling password-only access to their servers, and utilizing multi-factor authentication to gain access to their instances (or at a minimum certificate-based SSH Version 2 access).  Additionally, customers should employ a privilege escalation mechanism with logging on a per-user basis. For example, if the guest OS is Linux, after hardening their instance, they should utilize certificate-based SSHv2 to access the virtual instance, disable remote root login, use command-line logging, and use ‘sudo’ for privilege escalation.  Customers should generate their own key pairs in order to guarantee that they are unique, and not shared with other customers or with AWS.  *EBS*  Once a customer creates an Amazon EBS volume, the customer can attach it to an Amazon EC2 instance. Once attached, it will appear as a mounted device similar to any hard drive or other block device. At that point, the instance can interact with the volume just as it would with a local drive, formatting it with a file system or installing applications on it directly. The customer controls the EC2 instance an EBS volume may be attached to.  *VPC*  Through the AWS Management Console, Amazon Virtual Private Cloud (Amazon VPC) lets customers provision a private, isolated section of the Amazon Web Services (AWS) Cloud where customers can launch AWS resources in the customer-defined virtual network. Customers can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet. | |

|  |
| --- |
| IA-2 What is the solution and how is it implemented? Discuss for both the AWS environment and Beta FEC. |
|  |

* 1. **Control Enhancement IA-2 (1)**

IA-2 (1) The information system implements multifactor authentication for network access to privileged accounts.

|  |  |
| --- | --- |
| IA-2 (1) | Control Enhancement Summary Information |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☒ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  AWS Multi-Factor Authentication (AWS MFA) provides an extra level of security that customer agencies apply to their AWS environment. Customer agencies can enable AWS MFA for their account and for individual users they have created under their account. With AWS MFA enabled a user that signs into the FedCloud Console will be prompted for their username and password, as well as for an authentication code from their MFA device. Taken together, these multiple factors provide increased security for customer agencies’ AWS account settings and resources.  Virtual EC2 instances are completely controlled by the customer agency. Customers have full root access or administrative control over accounts, services, and applications. AWS does not have any access rights to customer instances and cannot log into the guest OS.  AWS recommends a base set of security best practices to include disabling password-only access to their servers, and utilizing multi-factor authentication to gain access to their instances (or at a minimum certificate-based SSH Version 2 access) | |

|  |
| --- |
| IA-2 (1) What is the solution and how is it implemented? Discuss for both the AWS environment and Beta FEC. |
|  |

* 1. **Control Enhancement IA-2 (2)**

IA-2 (2) The information system implements multifactor authentication for network access to non-privileged accounts.

|  |  |
| --- | --- |
| IA-2 (2) | Control Enhancement Summary Information |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☒ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  AWS Multi-Factor Authentication (AWS MFA) provides an extra level of security that customer agencies apply to their AWS environment. Customer agencies can enable AWS MFA for their account and for individual users they have created under their account. With AWS MFA enabled a user that signs into the FedCloud Console will be prompted for their username and password, as well as for an authentication code from their MFA device. Taken together, these multiple factors provide increased security for customer agencies’ AWS account settings and resources.  Virtual EC2 instances are completely controlled by the customer agency. Customers have full root access or administrative control over accounts, services, and applications. AWS does not have any access rights to customer instances and cannot log into the guest OS.  AWS recommends a base set of security best practices to include disabling password-only access to their servers, and utilizing multi-factor authentication to gain access to their instances (or at a minimum certificate-based SSH Version 2 access) | |

|  |
| --- |
| IA-2 (2) What is the solution and how is it implemented? Discuss for both the AWS environment and Beta FEC. |
|  |

* 1. **Control Enhancement IA-2 (12)**

IA-2 (12) The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

|  |  |
| --- | --- |
| IA-2 (12) | Control Enhancement Summary Information |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☐ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:** None. | |

|  |
| --- |
| IA-2 (12) What is the solution and how is it implemented? Discuss for Beta FEC. |
|  |

* 1. **Information Security Architecture (PL-8)**

The organization:

1. Develops an information security architecture for the information system that:
2. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
3. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
4. Describes any information security assumptions about, and dependencies on, external services;
5. Reviews and updates the information security architecture [*Assignment: organization-defined frequency*] to reflect updates in the enterprise architecture; and

**PL-8b Parameter Requirement:** At least annually.

1. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

|  |  |
| --- | --- |
| PL-8 | Control Enhancement Summary Information |
| Responsible Role: | |
| Implemented Parameter PL-8b: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☒ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:** None. | |

|  |  |
| --- | --- |
| PL-8 What is the solution and how is it implemented? Discuss for both the AWS environment and Beta FEC. | |
| Part a |  |
| Part b |  |
| Part c |  |

* 1. **Vulnerability Scanning (RA-5)**

The organization:

1. Scans for vulnerabilities in the information system and hosted applications *[Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process]* and when new vulnerabilities potentially affecting the system/applications are identified and reported;

**RA-5a Parameter Requirements:** Monthly Operating System (OS) and web application scanning; quarterly Database scanning (as applicable); and, OS and Web application scanning with every code release.

1. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
   1. Enumerating platforms, software flaws, and improper configurations;
   2. Formatting checklists and test procedures; and
   3. Measuring vulnerability impact;
2. Analyzes vulnerability scan reports and results from security control assessments;
3. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and

**RA-5d Parameter Requirements:** High-risk vulnerabilities mitigated within thirty days; moderate risk vulnerabilities mitigated within ninety days.

1. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

**RA-5e Parameter Requirements:** ISSO, ISSM, System Program Manager, and submits quarterly as part of the POA&M to the GSA OCISO (unless scanned by GSA enterprise vulnerability scanning solution).

|  |  |
| --- | --- |
| RA-5 | Control Summary Information |
| Responsible Role: | |
| Implemented Parameter 5a:  Implemented Parameter 5d:  Implemented Parameter 5e: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☐ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  AWS operates under a model of shared responsibility between the customer and AWS. AWS provides AMIs for client VMs that, after instantiation, are fully the customer agency’s’ responsibility. These default images are not included in vulnerability scanning activities conducted by AWS. Additionally, AWS will not maintain administrator access to customer VMs.  Upon deployment of virtual machines, the customer assumes full administrator access and is responsible for performing additional application installation, configuration, patching, security hardening, operating system vulnerability scanning, web application vulnerability scanning, and database vulnerability scanning (as applicable) for assets with which they have implementation responsibility (above the hypervisor, within each instance) as necessary. Customer management of the security of their operating environment as well as conducting vulnerability scans and pen-tests shall be conducted in accordance with their own Risk Assessment, the AWS Acceptable Use Policy, and the AWS Vulnerability / Penetration Testing Request Form.  Customers that want to conduct vulnerability scans and pen-tests of their operating environment must first contact AWS for permission To do so, AWS uses a web form to collect the information necessary to review security audit requests. In order to begin the authorization process, please visit the following AWS site: http://aws.amazon.com/security/penetration-testing/  At the site, the customer selects the "AWS Vulnerability / Penetration Testing Request Form" link and completes the form as requested. This form also includes the AWS Terms and Policies with regard to testing. Once the form is completed and received by AWS, the authorization review process is conducted and normally takes 1-2 business days to complete. | |

|  |  |
| --- | --- |
| RA-5 What is the solution and how is it implemented? Discuss for Beta FEC. | |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |

* 1. **Control Enhancement SA-22**

The organization:

1. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and
2. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

|  |  |
| --- | --- |
| SA-22 | Control Enhancement Summary Information |
| Responsible Role: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☒ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:** None. | |

|  |
| --- |
| SA-22 What is the solution and how is it implemented? Discuss for Beta FEC. |
|  |

* 1. **Boundary Protection (SC-7)**

The information system:

1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
2. Implements subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and

**SC-7b Parameter Requirements:** physically and/or logically.

1. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

|  |  |
| --- | --- |
| SC-7 | Control Summary Information |
| Responsible Role: | |
| Implemented Paramter: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☒ GSA AWS Environment  ☐ Application | |
| **AWS Customer Responsibility Requirement:**  Customer agencies are responsible for maintaining host-based firewall on compute instances in order to protect against malicious communications at the external boundary of the system. In addition, where the customer agencies have established key internal boundaries within the system, the customer agency is responsible for the setup and configuration of their VPC in order to enforce communications rules between internal networks. | |

|  |  |
| --- | --- |
| SC-7 What is the solution and how is it implemented? Discuss for the AWS environment. | |
| Part a |  |
| Part b |  |
| Part c |  |

* 1. **Cryptographic protection (SC-13)**

The information system implements [*Assignment: organization-defined cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

**SC-13 Parameter Requirements:** FIPS 140-2 validated encryption modules shall be implemented for digital media stored outside of controlled areas; e-mail; for data on portable storages devices; web sites (internal and public) with logon functions (must also implement TLS); and all sensitive information such as Personally Identifiable Information (as deemed by the data owner) transmitted outside the GSA firewall.

|  |  |
| --- | --- |
| SC-13 | Control Enhancement Summary Information |
| Responsible Role: | |
| Implemented Parameter: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☐ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  Customers are responsible for configuring their web browsers, mobile devices, etc., to enable communications through encryption. In addition, customers are responsible for implementing the Transmission Integrity, Transmission Confidentiality, Use of Cryptography, and Session Authenticity controls for the applications that customers establish within their Virtual Machine environments. | |

|  |
| --- |
| SC-13 What is the solution and how is it implemented? Discuss for Beta FEC. |
|  |

* 1. **Control Enhancement SC-28 (1)**

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] on [*Assignment: organization-defined information system components*].

**SC-28 (1) Parameter Requirement 1:** Personally Identifiable Information and all sensitive information (as deemed by the data owner).

**SC-28 (1) Parameter Requirement 2:** Stored data (e.g., database).

|  |  |
| --- | --- |
| SC-28 (1) | Control Enhancement Summary Information |
| Responsible Role: | |
| Implemented Parameter: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☐ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  Customers have complete control over their compute instances, virtual networks, and block stores in EC2, VPC, and EBS, respectively. Customers should configure their compute instances and block stores to protect the confidentiality and integrity of their information at rest. | |

|  |
| --- |
| SC-28 (1) What is the solution and how is it implemented? Discuss for Beta FEC. |
|  |

* 1. **Flaw Remediation (SI-2)**

The organization:

1. Identifies, reports, and corrects information system flaws;
2. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and

**SI-2 Parameter Requirement:** Monthly patching during scheduled maintenance windows following change control processes (including testing) with the ability to push emergency patches on demand from either the direction of the CISO or the AO. In terms of vulnerability remediation, High-risk vulnerabilities shall be mitigated within thirty days; moderate risk vulnerabilities mitigated within ninety days.

1. Incorporates flaw remediation into the organizational configuration management process.

|  |  |
| --- | --- |
| SI-2 | Control Summary Information |
| Responsible Role: | |
| Implemented Parameter SI2c: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☐ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  Customers are responsible for performing operating system vulnerability scanning, web application, and database scanning (as applicable) for assets for which they have implementation responsibility (above the hypervisor). AWS provides Amazon Machine Images (AMIs) for client Virtual Machines (VMs) that after instantiation are fully the customer agencies responsibility. Upon deployment of virtual machines, the customer assumes full administrator access and is responsible for performing additional configuration, patching, security hardening, vulnerability scanning and application installation, as necessary.  AWS will not maintain administrator access to customer VMs. These default images are not included in vulnerability scanning activities conduct by AWS or its Approved Scanning Vendor (ASV). | |

|  |  |
| --- | --- |
| SI-2 What is the solution and how is it implemented? Discuss for Beta FEC. | |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |

* 1. **Information system monitoring (SI-4)**

The organization:

1. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and

**SI-4a Parameter Requirement:** GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO.

* 1. Unauthorized local, network, and remote connections;

1. Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];

**SI-4b Parameter Requirement:** GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO.

1. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
2. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
3. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
4. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
5. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

**SI-4g Parameter Requirement 1:** GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO.

**SI-4g Parameter Requirement 2:** GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO.

**SI-4g Parameter Requirement 2:** GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO.

|  |  |
| --- | --- |
| SI-4 | Control Summary Information |
| Responsible Role: | |
| Implemented Parameter SI-4a:  Implemented Parameter SI-4b:  Implemented Parameter SI-4g Parameter 1:  Implemented Parameter SI-4g Parameter 2:  Implemented Parameter SI-4g Parameter 3: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☒ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  Customers are responsible for monitoring alerts and identifying unauthorized use of information systems. In addition, customers are responsible for implementing the Information System Monitoring Tools and Techniques control for the applications that tenants establish within their Virtual Machine environments. | |

|  |  |
| --- | --- |
| SI-4 What is the solution and how is it implemented? Discuss for both the AWS environment and Beta FEC. | |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |

* 1. **Information Input validation (SI-10)**

The information system checks the validity of [Assignment: organization-defined information inputs].

**SI-10 Parameter Requirement:** Inputs shall be validated for correct syntax and semantics (e.g., character set, length, numerical range, and acceptable values) to ensure they match specified definitions for format and content. Input validation protections will be tested through monthly operating system and web application vulnerability scanning as defined in control RA-5.

|  |  |
| --- | --- |
| SI-10 | Control Summary Information |
| Responsible Role: | |
| Implemented Parameter: | |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| Control Applicability (check all that apply):  ☐ GSA AWS Environment  ☒ Application | |
| **AWS Customer Responsibility Requirement:**  Customers using the AWS virtual machine (EBS) offering should develop a policy identifying acceptable data types to be stored. The customer is also responsible for defining field types, creating input validation rules for specific objects, as well as configuring any input restrictions and conducting any validity checks required on the information they place into the storage environment. In addition, the customer is responsible for ensuring only authorized individuals are designated as administrators within the management portal. | |

|  |
| --- |
| SI-10 What is the solution and how is it implemented? Discuss for Beta FEC. |
|  |