FedRAMP System Security Plan (SSP)

|  |
| --- |
|  |

18F / GSA

cloud.gov

Version 1.38

Version May 9, 2018

Controlled Unclassified Information

System Security Plan

Prepared by

| Identification of Organization that Prepared this Document | | |
| --- | --- | --- |
|  | Organization Name | 18F |
| Street Address | 1800 F Street, NW |
| Suite/Room/Building | 4400 |
| City, State Zip | Washington, DC, 20405 |

Prepared for

| Identification of Cloud Service Provider | | |
| --- | --- | --- |
|  | Organization Name | 18F |
| Street Address | 1800 F Street, NW |
| Suite/Room/Building | 4400 |
| City, State Zip | Washington, DC, 20405 |

Record of Changes

| Date | Description |
| --- | --- |
| 1/21/2013 | Original publication |
| 6/6/2014 | Major revision for SP800-53 Revision 4. Includes new template and formatting changes. |
| 3/6/2017 | Document renamed from "FedRAMP System Security Plan (SSP) Moderate Baseline Master Template to "FedRAMP System Security Plan (SSP) Moderate Baseline Template” |
| 6/20/2016 | Reformatted to FedRAMP Document Standard, added repeated text schema and content fields to tables that were not Control Tables.  Revised cover page, changed document designation to Confidential Unclassified Information (CUI),  Removed front matter section How This Document is Organized, Instructions re-written,  Corrected section numbering to match SSP v1.0,  Revised Section 9 Table 9-1 Personnel Roles and Privileges, Removed Section 10 inventory tables (see Attachment 13 FedRAMP Inventory Workbook).  Global verbiage change, Authorizing Official (AO) changed to JAB/AO; e-Authentication, e-authentication and E-authentication changed to E-Authentication.  Added attachments 10 FIPS 199, 11 Separation of Duties Matrix, 12 FedRAMP Laws and Regulations, 13 FedRAMP Inventory Workbook.  Changes to the following controls: AC-02 (05), AC-05, AC-17 (09), AU-03 (01), AU-05, AU-06, CA-02 (03), CA-7, CM-02 (01), IA-02 (11), MP-03, PL-08, SA-09 (01), SC-15, SI-04 (04) |
| 10/21/2016 | Removed tables in Sec 15.12 FedRAMP Laws and Regulations  Removed revision history tables in all of Sec 15  Removed Acronyms - see FedRAMP Master Acronyms and Glossary resource document  Added PTA to Sec 15.4 PTA and PIA  Added E-Authentication to Sec 15.3  Added FIPs to Sec 15.10 FIPS 199  Changed Inventory instruction and guidance Sec 10 and Attachment 13  Removed chapter numbers from Attachments  Removed 3 questions from Sec 2.3 E-Authentication Determination |
| 6/6/2017 | Updated logo |

Revision History

| Date | Description | Version of SSP | Author |
| --- | --- | --- | --- |
| 7/5/2016 | Updated cloud.gov FedRAMP SSP. | 1.0 | Valiant / 18F |
| 7/29/2016 | Updated descriptions, diagrams, and attachments. | 1.1 | Valiant / 18F |
| 8/31/2016 | Updated descriptions. | 1.2 | 18F |
| 9/30/2016 | Updated all content, removed all Valiant content, removed CUI designation. | 1.3 | 18F |
| 10/12/2016 | Significant modifications to control narratives in CA, CP, MA, MP, PS, RA, SA, SI control families.  Minor wording edits for clarity on AC-1, IA-1. | 1.4 | 18F |
| 10/18/2016 | Removed duplicative version number in cover sheet.  Updates to CA, CP, MA, MP, PS, RA, SA, SI linked procedures.  Minor correction to old Valiant information in CA-2. | 1.5 | 18F |
| 10/20/2016 | Major revisions to AU, CM, IR.  Minor revision to various AC controls. | 1.6 | 18F |
| 10/20/16 | Major revisions to AT. | 1.7 | 18F |
| 10/22/16 | Minor revision of PL controls.  Supplied missing IR-9 (4). | 1.8 | 18F |
| 10/22/16 | Major revisions to SC. | 1.9 | 18F |
| 10/24/16 | Assorted small fixes for clarity and consistency. | 1.10 | 18F |
| 10/25/16 | Significant clarifications and updates to the SA controls. | 1.11 | 18F |
| 10/25/16 | Updated PL-2 to accommodate the fact that the SSP might also be maintained as a Google Doc. | 1.12 | 18F |
| 11/7/16 | Updated section AC based on JAB TR comments. | 1.13 | 18F |
| 11/10/16 | Updated AC and IA based on JAB TR comments. | 1.14 | 18F |
| 11/14/16 | Updated parts of AC, IA, and sections 1-11, based on JAB TR comments.  Fixed problems with section numbering in section 10. | 1.15 | 18F |
| 11/15/16 | Updated additional parts of IA and section 9 based on JAB TR comments. | 1.16 | 18F |
| 11/17/16 | Updated AU, CA, CM, CP, and MA items based on JAB TR comments. | 1.17 | 18F |
| 11/18/16 | Updated AU. | 1.18 | 18F |
| 11/18/16 | Updated AU, CA, CM, CP, MA, RA, PS. | 1.19 | 18F |
| 11/21/16 | Updated AU-8, AU-8 (1), CM-2 (2), CP-6 (3), RA-3, other minor edits. | 1.20 | 18F |
| 11/23/16 | Updated IR, SA, SC, RA-2, 10.1.2.2., ports table, AC-3, other minor edits. | 1.21 | 18F |
| 11/25/16 | Added link to additional hardening information in SC-39. | 1.22 | 18F |
| 11/28/16 | Updated SC, SI. | 1.23 | 18F |
| 11/29/16 | Updated SI, IR, IA-2 (11), AU-5; updated some links throughout SSP. | 1.24 | 18F |
| 11/30/16 | Updated AU-9. | 1.25 | 18F |
| 12/2/16 | Updated AC-2 (5), AC-11, AC-11 (1), AC-12. | 1.26 | 18F |
| 12/7/16 | Updated AC-14, CA-3 (3), IA-2 (11); fixed some formatting. | 1.27 | 18F |
| 12/8/16 | Updated CP-4 (1), CP-9 (1), CP-10 (2), RA-3, RA-5, RA-5 (1), SI-2 (2), SI-3, SI-4, SI-7, SI-7 (1). | 1.28 | 18F |
| 12/9/16 | Updated RA-5, SI-2 (2). | 1.29 | 18F |
| 12/12/16 | Updated IA-3. | 1.30 | 18F |
| 12/13/16 | Updated 9.1. | 1.31 | 18F |
| 12/16/16 | Updated 9.2.1, CA-3 (3).  Update some mentions of “CloudWatch” to more specifically indicate “CloudWatch Logs”.  Minor update to CA-7 with new document location.  Minor formatting fixes. | 1.32 | 18F |
| 12/20/16 | Minor formatting fixes. | 1.33 | 18F |
| 2/15/18 | Integrated approved Significant Change Requests.  Updated points of contact.  Updated many details. Controls with more than superficial changes: AC-2 (3), AC-2 (5), AC-2 (9), AC-2 (10), AC-7, AC-10, AC-11, AC-11 (1), AC-12, AC-14, AC-22, CM-8 (5), CM-11, CP-3, CP-4, CP-4 (1), IA-2 (1), IA-2 (11), IA-2 (12), IA-4, IA-4 (4), IA-5, IA-5 (4), IA-5 (11), IA-8 (1), IA-8 (2), IA-8 (3), IA-8 (4), RA-5, SA-2, SA-3, SA-4 (9), SA-11 (1), SC-7 (7), SC-7 (8),SC-10, SC-12, SC-23, SI-10.  Updated FIPS 199 categorization in section 2.2. | 1.34 | 18F |
| 2/27/18 | Updated details in AC-10, SC-10, and SI-2 (2) for precision. | 1.35 | 18F |
| 3/30/18 | Updated figure numbering in sections 9 and 10.  Corrected AC-14 parameter.  Generalized mentions of brand names for GitHub issues and 1Password.  Updated AU-6 (3) implementation status.  Added GitHub information to CP-9.  Updated SI-2 (3) and RA-5. | 1.36 | 18F |
| 4/10/18 | Moved content to latest FedRAMP SSP template.  Updated figure numbering again to use Word cross-reference capability.  Updated -1 control narratives.  Updated PE control narratives to match MA/MP.  Updated SA-4, SA-4 (1), SA-4 (2), SA-5, SA-9 (1), SA-9 (5), SA-10 to rely less on cross-references to other controls and documents.  Minor grammatical fixes and broken link updates.  Updated attachments list and integrated attachments as listed. | 1.37 | 18F |
| 5/9/18 | Updated deployment model from “Public” to “Government Only Community” to more accurately reflect the system. | 1.38 | 18F |

How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact [*info@FedRAMP.gov*](mailto:info@fedramp.gov)

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

Table of Contents

[1 Information System Name/Title 1](#_Toc513650193)

[2 Information System Categorization 1](#_Toc513650194)

[2.1 Information Types 1](#_Toc513650195)

[2.2 Security Objectives Categorization (FIPS 199) 2](#_Toc513650196)

[2.3 E-Authentication Determination 3](#_Toc513650197)

[3 Information System Owner 3](#_Toc513650198)

[4 Authorizing Official 4](#_Toc513650199)

[5 Other Designated Contacts 4](#_Toc513650200)

[6 Assignment of Security Responsibility 4](#_Toc513650201)

[7 Information System Operational Status 5](#_Toc513650202)

[8 Information System Type 5](#_Toc513650203)

[8.1 Cloud Service Models 5](#_Toc513650204)

[8.2 Cloud Deployment Models 6](#_Toc513650205)

[8.3 Leveraged Authorizations 7](#_Toc513650206)

[9 General System Description 7](#_Toc513650207)

[9.1 System Function or Purpose 7](#_Toc513650208)

[9.2 Information System Components and Boundaries 8](#_Toc513650209)

[AWS Components and Boundaries 8](#_Toc513650210)

[cloud.gov Components and Boundaries 9](#_Toc513650211)

[9.3 Types of Users 10](#_Toc513650212)

[9.4 Network Architecture 17](#_Toc513650213)

[9.5 System Component Architecture 17](#_Toc513650214)

[9.6 Customer Separation 18](#_Toc513650215)

[9.7 Application Isolation 19](#_Toc513650216)

[10 System Environment And Inventory 20](#_Toc513650217)

[Basic structure of cloud.gov within AWS GovCloud 20](#_Toc513650218)

[Structure of customer application containers 20](#_Toc513650219)

[10.1 cloud.gov Virtual Private Cloud Environment 21](#_Toc513650220)

[Production Public Subnets 21](#_Toc513650221)

[Production Private Subnets 21](#_Toc513650222)

[cloud.gov Tooling VPC 21](#_Toc513650223)

[Tooling Public Subnets 22](#_Toc513650224)

[Tooling Private Subnets 22](#_Toc513650225)

[cloud.gov Development VPC 23](#_Toc513650226)

[10.2 cloud.gov Logical System Environment 23](#_Toc513650227)

[Organizations 23](#_Toc513650228)

[Spaces 24](#_Toc513650229)

[Buildpacks 24](#_Toc513650230)

[Secrets 27](#_Toc513650231)

[Services 27](#_Toc513650232)

[10.3 cloud.gov Security Domain Stack 27](#_Toc513650233)

[Identification and Authentication Control 27](#_Toc513650234)

[AWS 27](#_Toc513650235)

[cloud.gov 27](#_Toc513650236)

[ACLs, Software Defined Firewalls, and Security Groups 29](#_Toc513650237)

[AWS 29](#_Toc513650238)

[cloud.gov 29](#_Toc513650239)

[Audit Logging, Monitoring, and Intrusion Detection 29](#_Toc513650240)

[AWS 29](#_Toc513650241)

[cloud.gov 29](#_Toc513650242)

[Vulnerability Scanning and Penetration Testing 30](#_Toc513650243)

[Cloud Network Inventory and Asset Management 31](#_Toc513650244)

[Static and Dynamic Code Analysis 31](#_Toc513650245)

[Incident Response Resolution and Communication 31](#_Toc513650246)

[Configuration Management and Version Control 31](#_Toc513650247)

[10.4 Hardware Inventory 31](#_Toc513650248)

[10.5 Software Inventory 31](#_Toc513650249)

[10.6 Network Inventory 31](#_Toc513650250)

[10.7 Data Flow 32](#_Toc513650251)

[Firewall Rules 32](#_Toc513650252)

[10.8 Ports, Protocols and Services 32](#_Toc513650253)

[11 System Interconnections 35](#_Toc513650254)

[12 Laws, Regulations, Standards and Guidance 36](#_Toc513650255)

[12.1 Applicable Laws and Regulations 36](#_Toc513650256)

[12.2 Applicable Standards and Guidance 36](#_Toc513650257)

[13 Minimum Security Controls 36](#_Toc513650258)

[13.1 Access Control (AC) 44](#_Toc513650259)

[AC-1 Access Control Policy and Procedures Requirements (L) (M) 44](#_Toc513650260)

[AC-2 Account Management (L) (M) 45](#_Toc513650261)

[AC-2 (1) Control Enhancement (M) (H) 48](#_Toc513650262)

[AC-2 (2) Control Enhancement (M) 49](#_Toc513650263)

[AC-2 (3) Control Enhancement (M) 50](#_Toc513650264)

[AC-2 (4) Control Enhancement (M) 51](#_Toc513650265)

[AC-2 (5) Control Enhancement (M) 52](#_Toc513650266)

[AC-2 (7) Control Enhancement (M) 52](#_Toc513650267)

[AC-2 (9) Control Enhancement (M) 53](#_Toc513650268)

[AC-2 (10) Control Enhancement (M) (H) 54](#_Toc513650269)

[AC-2 (12) Control Enhancement (M) 55](#_Toc513650270)

[AC-3 Access Enforcement (L) (M) (H) 56](#_Toc513650271)

[AC-4 Information Flow Enforcement (M) (H) 57](#_Toc513650272)

[AC-4 (21) Control Enhancement (M) (H) 58](#_Toc513650273)

[AC-5 Separation of Duties (M) (H) 59](#_Toc513650274)

[AC-6 Least Privilege (M) (H) 60](#_Toc513650275)

[AC-6 (1) Control Enhancement (M) 61](#_Toc513650276)

[AC-6 (2) Control Enhancement (M) (H) 62](#_Toc513650277)

[AC 6 (5) Control Enhancement (M) (H) 63](#_Toc513650278)

[AC-6 (9) Control Enhancement (M) (H) 63](#_Toc513650279)

[AC-6 (10) Control Enhancement (M) (H) 64](#_Toc513650280)

[AC-7 Unsuccessful Login Attempts (L) (M) 65](#_Toc513650281)

[AC-8 System Use Notification (L) (M) (H) 66](#_Toc513650282)

[AC-10 Concurrent Session Control (M) (H) 69](#_Toc513650283)

[AC-11 Session Lock (M) (H) 70](#_Toc513650284)

[AC-11 (1) Control Enhancement (M) (H) 71](#_Toc513650285)

[AC-12 Session Termination (M) (H) 71](#_Toc513650286)

[AC-14 Permitted Actions without Identification or Authentication (L) (M) (H) 72](#_Toc513650287)

[AC-17 Remote Access (L) (M) (H) 73](#_Toc513650288)

[AC-17 (1) Control Enhancement (M) (H) 74](#_Toc513650289)

[AC-17 (2) Control Enhancement (M) (H) 74](#_Toc513650290)

[AC-17 (3) Control Enhancement (M) (H) 75](#_Toc513650291)

[AC-17 (4) Control Enhancement (M) (H) 76](#_Toc513650292)

[AC-17 (9) Control Enhancement (M) (H) 76](#_Toc513650293)

[AC-18 Wireless Access Restrictions (L) (M) (H) 77](#_Toc513650294)

[AC-18 (1) Control Enhancement (M) (H) 78](#_Toc513650295)

[AC-19 Access Control for Portable and Mobile Systems (L) (M) (H) 78](#_Toc513650296)

[AC-19 (5) Control Enhancement (M) (H) 79](#_Toc513650297)

[AC-20 Use of External Information Systems (L) (M) (H) 80](#_Toc513650298)

[AC-20 (1) Control Enhancement (M) (H) 81](#_Toc513650299)

[AC-20 (2) Control Enhancement (M) (H) 82](#_Toc513650300)

[AC-21 Information Sharing (M) (H) 82](#_Toc513650301)

[AC-22 Publicly Accessible Content (L) (M) (H) 83](#_Toc513650302)

[13.2 Awareness and Training (AT) 86](#_Toc513650303)

[AT-1 Security Awareness and Training Policy and Procedures (L) (M) 86](#_Toc513650304)

[AT-2 Security Awareness (L) (M) (H) 87](#_Toc513650305)

[AT-2 (2) Control Enhancement (M) (H) 88](#_Toc513650306)

[AT-3 Role-Based Security Training (L) (M) (H) 89](#_Toc513650307)

[AT-4 Security Training Records (L) (M) 90](#_Toc513650308)

[13.3 Audit and Accountability (AU) 91](#_Toc513650309)

[AU-1 Audit and Accountability Policy and Procedures (L) (M) 91](#_Toc513650310)

[AU-2 Audit Events (L) (M) (H) 93](#_Toc513650311)

[AU-2 (3) Control Enhancement (M) (H) 95](#_Toc513650312)

[AU-3 Content of Audit Records (L) (M) (H) 96](#_Toc513650313)

[AU-3 (1) Control Enhancement (M) 97](#_Toc513650314)

[AU-4 Audit Storage Capacity (L) (M) (H) 98](#_Toc513650315)

[AU-5 Response to Audit Processing Failures (L) (M) (H) 99](#_Toc513650316)

[AU-6 Audit Review, Analysis, and Reporting (L) (M) (H) 100](#_Toc513650317)

[AU-6 (1) Control Enhancement (M) (H) 103](#_Toc513650318)

[AU-6 (3) Control Enhancement (M) (H) 104](#_Toc513650319)

[AU-7 Audit Reduction and Report Generation (M) (H) 104](#_Toc513650320)

[AU-7 (1) Control Enhancement (M) (H) 105](#_Toc513650321)

[AU-8 Time Stamps (L) (M) (H) 106](#_Toc513650322)

[AU-8 (1) Control Enhancement (M) (H) 107](#_Toc513650323)

[AU-9 Protection of Audit Information (L) (M) (H) 109](#_Toc513650324)

[AU-9 (2) Control Enhancement (M) (H) 110](#_Toc513650325)

[AU-9 (4) Control Enhancement (M) (H) 111](#_Toc513650326)

[AU-11 Audit Record Retention (M) 111](#_Toc513650327)

[AU-12 Audit Generation (L) (M) (H) 112](#_Toc513650328)

[13.4 Security Assessment and Authorization (CA) 114](#_Toc513650329)

[CA-1 Certification, Authorization, Security Assessment Policy and Procedures (L) (M) 114](#_Toc513650330)

[CA-2 Security Assessments (L) (M) (H) 115](#_Toc513650331)

[CA-2 (1) Control Enhancement (L) (M) (H) 116](#_Toc513650332)

[CA-2 (2) Control Enhancement (M) (H) 117](#_Toc513650333)

[CA-2 (3) Control Enhancement (M) (H) 118](#_Toc513650334)

[CA-3 System Interconnections (L) (M) (H) 119](#_Toc513650335)

[CA-3 (3) Control Enhancement (M) (H) 120](#_Toc513650336)

[CA-3 (5) Control Enhancement (M) 122](#_Toc513650337)

[CA-5 Plan of Action and Milestones (L) (M) (H) 122](#_Toc513650338)

[CA-6 Security Authorization (L) (M) (H) 123](#_Toc513650339)

[CA-7 Continuous Monitoring (L) (M) (H) 124](#_Toc513650340)

[CA-7 (1) Control Enhancement (M) (H) 127](#_Toc513650341)

[CA-8 Penetration Testing (M) (H) 127](#_Toc513650342)

[CA-8 (1) Control Enhancement (M) (H) 128](#_Toc513650343)

[CA-9 Internal System Connections (L) (M) (H) 129](#_Toc513650344)

[13.5 Configuration Management (CM) 130](#_Toc513650345)

[CM-1 Configuration Management Policies and Procedures (L) (M) 130](#_Toc513650346)

[CM-2 Baseline Configuration (L) (M) (H) 131](#_Toc513650347)

[CM-2 (1) Control Enhancement (M) 132](#_Toc513650348)

[CM-2 (2) Control Enhancement (M) (H) 133](#_Toc513650349)

[CM-2 (3) Control Enhancement (M) 134](#_Toc513650350)

[CM-2 (7) Control Enhancement (M) (H) 135](#_Toc513650351)

[CM-3 Configuration Change Control (M) (H) 136](#_Toc513650352)

[CM-4 Security Impact Analysis (L) (M) (H) 139](#_Toc513650353)

[CM-5 Access Restrictions for Change (M) (H) 139](#_Toc513650354)

[CM-5 (1) Control Enhancement (M) (H) 140](#_Toc513650355)

[CM-5 (3) Control Enhancement (M) (H) 141](#_Toc513650356)

[CM-5 (5) Control Enhancement (M) (H) 142](#_Toc513650357)

[CM-6 Configuration Settings (L) (M) (H) 143](#_Toc513650358)

[CM-6 (1) Control Enhancement (M) (H) 145](#_Toc513650359)

[CM-7 Least Functionality (L) (M) (H) 146](#_Toc513650360)

[CM-7 (1) Control Enhancement (M) (H) 147](#_Toc513650361)

[CM-7 (2) Control Enhancement (M) (H) 148](#_Toc513650362)

[CM-7 (5) Control Enhancement (M) 149](#_Toc513650363)

[CM-8 Information System Component Inventory (L) (M) (H) 150](#_Toc513650364)

[CM-8 (1) Control Enhancement (M) (H) 152](#_Toc513650365)

[CM-8 (3) Control Enhancement (M) (H) 153](#_Toc513650366)

[CM-8 (5) Control Enhancement (M) (H) 154](#_Toc513650367)

[CM-9 Configuration Management Plan (M) (H) 155](#_Toc513650368)

[CM-10 Software Usage Restrictions (L) (M) (H) 156](#_Toc513650369)

[CM-10 (1) Control Enhancement (M) (H) 157](#_Toc513650370)

[CM-11 User-Installed Software (M) (H) 158](#_Toc513650371)

[13.6 Contingency Planning (CP) 159](#_Toc513650372)

[CP-1 Contingency Planning Policy and Procedures (L) (M) 159](#_Toc513650373)

[CP-2 Contingency Plan (L) (M) (H) 160](#_Toc513650374)

[CP-2 (1) Control Enhancement (M) (H) 162](#_Toc513650375)

[CP-2 (2) Control Enhancement (M) (H) 163](#_Toc513650376)

[CP-2 (3) Control Enhancement (M) (H) 164](#_Toc513650377)

[CP-2 (8) Control Enhancement (M) (H) 164](#_Toc513650378)

[CP-3 Contingency Training (L) (M) (H) 165](#_Toc513650379)

[CP-4 Contingency Plan Testing (H) 166](#_Toc513650380)

[CP-4 (1) Control Enhancement (M) (H) 167](#_Toc513650381)

[CP-6 Alternate Storage Site (M) (H) 167](#_Toc513650382)

[CP-6 (1) Control Enhancement (M) (H) 168](#_Toc513650383)

[CP-6 (3) Control Enhancement (M) (H) 169](#_Toc513650384)

[CP-7 Alternate Processing Site (M) (H) 170](#_Toc513650385)

[CP-7 (1) Control Enhancement (M) (H) 171](#_Toc513650386)

[CP-7 (2) Control Enhancement (M) (H) 172](#_Toc513650387)

[CP-7 (3) Control Enhancement (M) (H) 172](#_Toc513650388)

[CP-8 Telecommunications Services (M) (H) 173](#_Toc513650389)

[CP-8 (1) Control Enhancement (M) (H) 174](#_Toc513650390)

[CP-8 (2) Control Enhancement (M) (H) 174](#_Toc513650391)

[CP-9 Information System Backup (L) (M) (H) 175](#_Toc513650392)

[CP-9 (1) Control Enhancement (M) 176](#_Toc513650393)

[CP-9 (3) Control Enhancement (M) (H) 177](#_Toc513650394)

[CP-10 Information System Recovery and Reconstitution (L) (M) (H) 178](#_Toc513650395)

[CP-10 (2) Control Enhancement (M) (H) 178](#_Toc513650396)

[13.7 Identification and Authentication (IA) 179](#_Toc513650397)

[IA-1 Identification and Authentication Policy and Procedures (L) (M) 179](#_Toc513650398)

[IA-2 User Identification and Authentication (L) (M) (H) 180](#_Toc513650399)

[IA-2 (1) Control Enhancement (L) (M) (H) 181](#_Toc513650400)

[IA-2 (2) Control Enhancement (M) (H) 182](#_Toc513650401)

[IA-2 (3) Control Enhancement (M) (H) 183](#_Toc513650402)

[IA-2 (5) Control Enhancement (M) (H) 183](#_Toc513650403)

[IA-2 (8) Control Enhancement (M) (H) 184](#_Toc513650404)

[IA-2 (11) Control Enhancement (M) (H) 185](#_Toc513650405)

[IA-2 (12) Control Enhancement (L) (M) (H) 186](#_Toc513650406)

[IA-3 Device Identification and Authentication (M) (H) 187](#_Toc513650407)

[IA-4 Identifier Management (L) (M) 188](#_Toc513650408)

[IA-4 (4) Control Enhancement (M) (H) 190](#_Toc513650409)

[IA-5 Authenticator Management (L) (M) 190](#_Toc513650410)

[IA-5 (1) Control Enhancement (L) (M) 195](#_Toc513650411)

[IA-5 (2) Control Enhancement (M) (H) 197](#_Toc513650412)

[IA-5 (3) Control Enhancement (M) (H) 198](#_Toc513650413)

[IA-5 (4) Control Enhancement (M) 199](#_Toc513650414)

[IA-5 (6) Control Enhancement (M) (H) 200](#_Toc513650415)

[IA-5 (7) Control Enhancement (M) (H) 200](#_Toc513650416)

[IA-5 (11) Control Enhancement (L) (M) (H) 201](#_Toc513650417)

[IA-6 Authenticator Feedback (L) (M) (H) 202](#_Toc513650418)

[IA-7 Cryptographic Module Authentication (L) (M) (H) 202](#_Toc513650419)

[IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H) 203](#_Toc513650420)

[IA-8 (1) Control Enhancement (L) (M) (H) 204](#_Toc513650421)

[IA-8 (2) Control Enhancement (L) (M) (H) 205](#_Toc513650422)

[IA-8 (3) Control Enhancement (L) (M) (H) 205](#_Toc513650423)

[IA-8 (4) Control Enhancement (L) (M) (H) 206](#_Toc513650424)

[13.8 Incident Response (IR) 207](#_Toc513650425)

[IR-1 Incident Response Policy and Procedures (L) (M) 207](#_Toc513650426)

[IR-2 Incident Response Training (L) (M) 208](#_Toc513650427)

[IR-3 Incident Response Testing (M) 209](#_Toc513650428)

[IR-3 (2) Control Enhancement (M) (H) 210](#_Toc513650429)

[IR-4 Incident Handling (L) (M) (H) 211](#_Toc513650430)

[IR-4 (1) Control Enhancement (M) (H) 212](#_Toc513650431)

[IR-5 Incident Monitoring (L) (M) (H) 213](#_Toc513650432)

[IR-6 Incident Reporting (L) (M) (H) 214](#_Toc513650433)

[IR-6 (1) Control Enhancement (M) (H) 215](#_Toc513650434)

[IR-7 Incident Response Assistance (L) (M) (H) 216](#_Toc513650435)

[IR-7 (1) Control Enhancement (M) (H) 216](#_Toc513650436)

[IR-7 (2) Control Enhancement (M) (H) 217](#_Toc513650437)

[IR-8 Incident Response Plan (L) (M) (H) 218](#_Toc513650438)

[IR-9 Information Spillage Response (M) (H) 220](#_Toc513650439)

[IR-9 (1) Control Enhancement (M) (H) 223](#_Toc513650440)

[IR-9 (2) Control Enhancement (M) 224](#_Toc513650441)

[IR-9 (3) Control Enhancement (M) (H) 224](#_Toc513650442)

[IR-9 (4) Control Enhancement (M) (H) 225](#_Toc513650443)

[13.9 Maintenance (MA) 226](#_Toc513650444)

[MA-1 System Maintenance Policy and Procedures (L) (M) 226](#_Toc513650445)

[MA-2 Controlled Maintenance (L) (M) (H) 227](#_Toc513650446)

[MA-3 Maintenance Tools (M) (H) 228](#_Toc513650447)

[MA-3 (1) Control Enhancement (M) (H) 229](#_Toc513650448)

[MA-3 (2) Control Enhancement (M) (H) 229](#_Toc513650449)

[MA-3 (3) Control Enhancement (M) (H) 230](#_Toc513650450)

[MA-4 Remote Maintenance (L) (M) (H) 231](#_Toc513650451)

[MA-4 (2) Control Enhancement (M) (H) 232](#_Toc513650452)

[MA-5 Maintenance Personnel (L) (M) (H) 232](#_Toc513650453)

[MA-5 (1) Control Enhancement (L) (M) 233](#_Toc513650454)

[MA-6 Timely Maintenance (M) (H) 234](#_Toc513650455)

[13.10 Media Protection (MP) 235](#_Toc513650456)

[MP-1 Media Protection Policy and Procedures (L) (M) 235](#_Toc513650457)

[MP-2 Media Access (L) (M) 236](#_Toc513650458)

[MP-3 Media Labeling (M) (H) 237](#_Toc513650459)

[MP-4 Media Storage (M) (H) 237](#_Toc513650460)

[MP-5 Media Transport (M) (H) 238](#_Toc513650461)

[MP-5 (4) Control Enhancement (M) (H) 239](#_Toc513650462)

[MP-6 Media Sanitization and Disposal (L) (M) 240](#_Toc513650463)

[MP-6 (2) Control Enhancement (M) 241](#_Toc513650464)

[MP-7 Media Use (L) (M) (H) 241](#_Toc513650465)

[MP-7 (1) Control Enhancement (M) (H) 242](#_Toc513650466)

[13.11 Physical and Environmental Protection (PE) 243](#_Toc513650467)

[PE-1 Physical and Environmental Protection Policy and Procedures (L) (M) 243](#_Toc513650468)

[PE-2 Physical Access Authorizations (L) (M) 244](#_Toc513650469)

[PE-3 Physical Access Control (L) (M) (H) 245](#_Toc513650470)

[PE-4 Access Control for Transmission Medium (M) (H) 246](#_Toc513650471)

[PE-5 Access Control for Output Devices (M) (H) 247](#_Toc513650472)

[PE-6 Monitoring Physical Access (L) (M) (H) 248](#_Toc513650473)

[PE-6 (1) Control Enhancement (M) (H) 248](#_Toc513650474)

[PE-8 Visitor Access Records (L) (M) (H) 249](#_Toc513650475)

[PE-9 Power Equipment and Cabling (M) (H) 250](#_Toc513650476)

[PE-10 Emergency Shutoff (M) (H) 250](#_Toc513650477)

[PE-11 Emergency Power (M) (H) 251](#_Toc513650478)

[PE-12 Emergency Lighting (L) (M) (H) 252](#_Toc513650479)

[PE-13 Fire Protection (L) (M) (H) 252](#_Toc513650480)

[PE-13 (2) Control Enhancement (M) (H) 253](#_Toc513650481)

[PE-13 (3) Control Enhancement (M) (H) 254](#_Toc513650482)

[PE-14 Temperature and Humidity Controls (L) (M) (H) 254](#_Toc513650483)

[PE-14 (2) Control Enhancement (M) (H) 255](#_Toc513650484)

[PE-15 Water Damage Protection (L) (M) (H) 256](#_Toc513650485)

[PE-16 Delivery and Removal (L) (M) (H) 256](#_Toc513650486)

[PE-17 Alternate Work Site (M) (H) 257](#_Toc513650487)

[13.12 Planning (PL) 258](#_Toc513650488)

[PL-1 Security Planning Policy and Procedures (L) (M) 258](#_Toc513650489)

[PL-2 System Security Plan (L) (M) (H) 259](#_Toc513650490)

[PL-2 (3) Control Enhancement (M) (H) 261](#_Toc513650491)

[PL-4 Rules of Behavior (L) (M) 262](#_Toc513650492)

[PL-4 (1) Control Enhancement (M) (H) 263](#_Toc513650493)

[PL-8 Information Security Architecture (M) (H) 264](#_Toc513650494)

[13.13 Personnel Security (PS) 267](#_Toc513650495)

[PS-1 Personnel Security Policy and Procedures (L) (M) 267](#_Toc513650496)

[PS-2 Position Categorization (L) (M) 268](#_Toc513650497)

[PS-3 Personnel Screening (L) (M) (H) 269](#_Toc513650498)

[PS-3 (3) Control Enhancement (M) (H) 270](#_Toc513650499)

[PS-4 Personnel Termination (L) (M) 270](#_Toc513650500)

[PS-5 Personnel Transfer (L) (M) 272](#_Toc513650501)

[PS-6 Access Agreements (L) (M) 273](#_Toc513650502)

[PS-7 Third-Party Personnel Security (L) (M) 274](#_Toc513650503)

[PS-8 Personnel Sanctions (L) (M) 275](#_Toc513650504)

[13.14 Risk Assessment (RA) 276](#_Toc513650505)

[RA-1 Risk Assessment Policy and Procedures (L) (M) 276](#_Toc513650506)

[RA-2 Security Categorization (L) (M) (H) 278](#_Toc513650507)

[RA-3 Risk Assessment (L) (M) 279](#_Toc513650508)

[RA-5 Vulnerability Scanning (L) (M) (H) 281](#_Toc513650509)

[RA-5 (1) Control Enhancement (M) (H) 284](#_Toc513650510)

[RA-5 (2) Control Enhancement (M) (H) 285](#_Toc513650511)

[RA-5 (3) Control Enhancement (M) (H) 286](#_Toc513650512)

[RA-5 (5) Control Enhancement (M) (H) 286](#_Toc513650513)

[RA-5 (6) Control Enhancement (M) (H) 287](#_Toc513650514)

[RA-5 (8) Control Enhancement (L) (M) (H) 288](#_Toc513650515)

[13.15 System and Services Acquisition (SA) 289](#_Toc513650516)

[SA-1 System and Services Acquisition Policy and Procedures (L) (M) 289](#_Toc513650517)

[SA-2 Allocation of Resources (L) (M) (H) 290](#_Toc513650518)

[SA-3 System Development Life Cycle (L) (M) (H) 291](#_Toc513650519)

[SA-4 Acquisitions Process (L) (M) (H) 292](#_Toc513650520)

[SA-4 (1) Control Enhancement (M) (H) 294](#_Toc513650521)

[SA-4 (2) Control Enhancement (L) (M) 294](#_Toc513650522)

[SA-4 (8) Control Enhancement (M) (H) 295](#_Toc513650523)

[SA-4 (9) Control Enhancement (M) (H) 296](#_Toc513650524)

[SA-4 (10) Control Enhancement (M) (H) 296](#_Toc513650525)

[SA-5 Information System Documentation (L) (M) 297](#_Toc513650526)

[SA-8 Security Engineering Principles (M) (H) 298](#_Toc513650527)

[SA-9 External Information System Services (L) (M) (H) 299](#_Toc513650528)

[SA-9 (1) Control Enhancement (M) (H) 300](#_Toc513650529)

[SA-9 (2) Control Enhancement (M) (H) 301](#_Toc513650530)

[SA-9 (4) Control Enhancement (M) (H) 302](#_Toc513650531)

[SA-9 (5) Control Enhancement (M) (H) 302](#_Toc513650532)

[SA-10 Developer Configuration Management (M) (H) 303](#_Toc513650533)

[SA-10 (1) Control Enhancement (M) (H) 304](#_Toc513650534)

[SA-11 Developer Security Testing and Evaluation (M) (H) 305](#_Toc513650535)

[SA-11 (1) Control Enhancement (M) (H) 306](#_Toc513650536)

[SA-11 (2) Control Enhancement (M) (H) 307](#_Toc513650537)

[SA-11 (8) Control Enhancement (M) (H) 307](#_Toc513650538)

[13.16 System and Communications Protection (SC) 308](#_Toc513650539)

[SC-1 System and Communications Protection Policy and Procedures (L) (M) 308](#_Toc513650540)

[SC-2 Application Partitioning (M) (H) 309](#_Toc513650541)

[SC-4 Information in Shared Resources (M) (H) 310](#_Toc513650542)

[SC-5 Denial of Service Protection (L) (M) (H) 311](#_Toc513650543)

[SC-6 Resource Availability (M) (H) 312](#_Toc513650544)

[SC-7 Boundary Protection (L) (M) (H) 313](#_Toc513650545)

[SC-7 (3) Control Enhancement (M) (H) 315](#_Toc513650546)

[SC-7 (4) Control Enhancement (M) 316](#_Toc513650547)

[SC-7 (5) Control Enhancement (M) (H) 317](#_Toc513650548)

[SC-7 (7) Control Enhancement (M) (H) 318](#_Toc513650549)

[SC-7 (8) Control Enhancement (M) (H) 318](#_Toc513650550)

[SC-7 (12) Control Enhancement (M) 319](#_Toc513650551)

[SC-7 (13) Control Enhancement (M) 320](#_Toc513650552)

[SC-7 (18) Control Enhancement (M) (H) 321](#_Toc513650553)

[SC-8 Transmission confidentiality and Integrity (M) (H) 322](#_Toc513650554)

[SC-8 (1) Control Enhancement (M) (H) 323](#_Toc513650555)

[SC-10 Network Disconnect (M) 323](#_Toc513650556)

[SC-12 Cryptographic Key Establishment & Management (L) (M) (H) 324](#_Toc513650557)

[SC-12 (2) Control Enhancement (M) (H) 325](#_Toc513650558)

[SC-12 (3) Control Enhancement (M) (H) 326](#_Toc513650559)

[SC-13 Use of Cryptography (L) (M) (H) 327](#_Toc513650560)

[SC-15 Collaborative Computing Devices (M) (H) 328](#_Toc513650561)

[SC-17 Public Key Infrastructure Certificates (M) (H) 329](#_Toc513650562)

[SC-18 Mobile Code (M) (H) 330](#_Toc513650563)

[SC-19 Voice Over Internet Protocol (M) (H) 331](#_Toc513650564)

[SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H) 332](#_Toc513650565)

[SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H) 333](#_Toc513650566)

[SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H) 334](#_Toc513650567)

[SC-23 Session Authenticity (M) (H) 335](#_Toc513650568)

[SC-28 Protection of Information at Rest (M) (H) 335](#_Toc513650569)

[SC-28 (1) Control Enhancement (M) 336](#_Toc513650570)

[SC-39 Process Isolation (L) (M) (H) 337](#_Toc513650571)

[13.17 System and Information Integrity (SI) 338](#_Toc513650572)

[SI-1 System and Information Integrity Policy and Procedures (L) (M) 338](#_Toc513650573)

[SI-2 Flaw Remediation (L) (M) (H) 339](#_Toc513650574)

[SI-2 (2) Control Enhancement (M) (H) 341](#_Toc513650575)

[SI-2 (3) Control Enhancement (M) (H) 342](#_Toc513650576)

[SI-3 Malicious Code Protection (L) (M) 343](#_Toc513650577)

[SI-3 (1) Control Enhancement (M) (H) 345](#_Toc513650578)

[SI-3 (2) Control Enhancement (M) (H) 346](#_Toc513650579)

[SI-3 (7) Control Enhancement (M) (H) 347](#_Toc513650580)

[SI-4 Information System Monitoring (L) (M) (H) 347](#_Toc513650581)

[SI-4 (1) Control Enhancement (M) (H) 349](#_Toc513650582)

[SI-4 (2) Control Enhancement (M) (H) 350](#_Toc513650583)

[SI-4 (4) Control Enhancement (M) (H) 351](#_Toc513650584)

[SI-4 (5) Control Enhancement (M) (H) 351](#_Toc513650585)

[SI-4 (14) Control Enhancement (M) (H) 352](#_Toc513650586)

[SI-4 (16) Control Enhancement (M) (H) 353](#_Toc513650587)

[SI-4 (23) Control Enhancement (M) (H) 354](#_Toc513650588)

[SI-5 Security Alerts & Advisories (L) (M) (H) 354](#_Toc513650589)

[SI-6 Security Functionality Verification (M) (H) 355](#_Toc513650590)

[SI-7 Software & Information Integrity (M) (H) 357](#_Toc513650591)

[SI-7 (1) Control Enhancement (M) (H) 358](#_Toc513650592)

[SI-7 (7) Control Enhancement (M) (H) 359](#_Toc513650593)

[SI-8 Spam Protection (M) (H) 360](#_Toc513650594)

[SI-8 (1) Control Enhancement (M) (H) 360](#_Toc513650595)

[SI-8 (2) Control Enhancement (M) (H) 361](#_Toc513650596)

[SI-10 Information Input Validation (M) (H) 362](#_Toc513650597)

[SI-11 Error Handling (M) (H) 363](#_Toc513650598)

[SI-12 Information Output Handling and Retention (L) (M) (H) 364](#_Toc513650599)

[SI-16 Memory Protection (M) (H) 365](#_Toc513650600)

[14 Acronyms 367](#_Toc513650601)

[15 Attachments 368](#_Toc513650602)

[ATTACHMENT 1 - Information Security Policies and Procedures 369](#_Toc513650603)

[ATTACHMENT 2 - User Guide 370](#_Toc513650604)

[ATTACHMENT 3 – e-Authentication Worksheet 371](#_Toc513650605)

[Introduction and Purpose 371](#_Toc513650606)

[Information System Name/Title 371](#_Toc513650607)

[E-Authentication Level Definitions 371](#_Toc513650608)

[Review Maximum Potential Impact Levels 371](#_Toc513650609)

[E-Authentication Level Selection 372](#_Toc513650610)

[ATTACHMENT 4 – PTA / PIA 373](#_Toc513650611)

[Privacy Overview and Point of Contact (POC) 373](#_Toc513650612)

[Applicable Laws and Regulations 373](#_Toc513650613)

[Applicable Standards and Guidance 373](#_Toc513650614)

[Personally Identifiable Information (PII) 374](#_Toc513650615)

[Privacy Threshold Analysis 374](#_Toc513650616)

[Qualifying Questions 374](#_Toc513650617)

[Designation 375](#_Toc513650618)

[ATTACHMENT 5 - Rules of Behavior 376](#_Toc513650619)

[ATTACHMENT 6 – Information System Contingency Plan 377](#_Toc513650620)

[ATTACHMENT 7 - Configuration Management Plan 378](#_Toc513650621)

[ATTACHMENT 8 - Incident Response Plan 379](#_Toc513650622)

[ATTACHMENT 9 - CIS Report and Worksheet 380](#_Toc513650623)

[ATTACHMENT 10 - FIPS 199 381](#_Toc513650624)

[Introduction and Purpose 381](#_Toc513650625)

[Scope 381](#_Toc513650626)

[System Description 381](#_Toc513650627)

[Methodology 381](#_Toc513650628)

[ATTACHMENT 11 – Services Table 383](#_Toc513650629)

[ATTACHMENT 12 – FedRAMP Laws and Regulations 384](#_Toc513650630)

[ATTACHMENT 13 – FedRAMP Inventory Workbook 385](#_Toc513650631)

List of Tables

[Table 1‑1 Information System Name and Title 1](#_Toc513650632)

[Table 2‑1 Security Categorization 1](#_Toc513650633)

[Table 2‑2 Sensitivity Categorization of Information Types 2](#_Toc513650634)

[Table 2‑3 Security Impact Level 3](#_Toc513650635)

[Table 2‑4 Baseline Security Configuration 3](#_Toc513650636)

[Table 3‑1 Information System Owner 3](#_Toc513650637)

[Table 5‑1 Information System Management Point of Contact 4](#_Toc513650638)

[Table 5‑2 Information System Technical Point of Contact 4](#_Toc513650639)

[Table 6‑1 CSP Name Internal ISSO (or Equivalent) Point of Contact 5](#_Toc513650640)

[Table 6‑2 AO ISSO Point of Contact 5](#_Toc513650641)

[Table 7‑1 System Status 5](#_Toc513650642)

[Table 8‑1 Service Layers Represented in this SSP 6](#_Toc513650643)

[Table 8‑2 Cloud Deployment Model Represented in this SSP 6](#_Toc513650644)

[Table 8‑3 Leveraged Authorizations 7](#_Toc513650645)

[Table 9‑1 Personnel Roles and Privileges 11](#_Toc513650646)

[Table 10‑1 Ports, Protocols and Services 33](#_Toc513650647)

[Table 12‑1 cloud.gov Laws and Regulations 36](#_Toc513650648)

[Table 12‑2 cloud.gov Standards and Guidance 36](#_Toc513650649)

[Table 13‑1 Summary of Required Security Controls 36](#_Toc513650650)

[Table 13‑2 Control Origination and Definitions 43](#_Toc513650651)

[Table 13‑3 CA-3 Authorized Connections 119](#_Toc513650652)

[Table 15‑1. Attachment File Naming Convention 368](#_Toc513650653)

List of Figures

[Figure 9‑1 Network Diagram 17](#_Toc511161962)

[Figure 9‑2 System Component Architecture Diagram 18](#_Toc511161963)

[Figure 9‑3 cloud.gov Customer Internal and External Separation 19](#_Toc511161964)

[Figure 10‑1 Customer Data Flow Diagram 32](#_Toc511161965)

[Figure 10‑2 Jumpbox Data Flow Diagram 32](#_Toc511161966)

[Figure 10‑3 Monitoring and Alerting Data Flow Diagram 32](#_Toc511161967)

[Figure 10‑4 Software Deployment Data Flow Diagram 32](#_Toc511161968)

System Security Plan Approvals

Cloud Service Provider Signatures

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| Name | Shashank Khandelwal | | Date | <Select Date> |
| Title | Director of cloud.gov | | | |
| Cloud Service Provider | | 18F / GSA | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | Britta Gustafson | | Date | <Select Date> |
| Title | Deputy Director of cloud.gov | | | |
| Cloud Service Provider | | 18F / GSA | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | Bret Mogilefsky | | Date | <Select Date> |
| Title | Program Manager | | | |
| Cloud Service Provider | | 18F / GSA | | |
|  | |  | | |

# Information System Name/Title

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

The security safeguards implemented for the cloud.gov 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 ‑ Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| F1607067912 | cloud.gov | cloud.gov |

# Information System Categorization

The overall information system sensitivity categorization is recorded in Table 2‑1 Security Categorization that follows. Directions for attaching the FIPS 199 document may be found in the following section: ATTACHMENT 10 - FIPS 199.

Table ‑ Security Categorization

|  |  |
| --- | --- |
| System Sensitivity Level: | Moderate (M) |

## 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 cloud.gov. The selection of the information types is based on guidance provided by Office of Management and Budget (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 Special Publication (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.

Example:

| Information Type  (Use only information types from NIST SP 800-60, Volumes I and II as amended) | NIST 800-60 identifier for Associated Information Type | Confidentiality | Integrity | Availability |
| --- | --- | --- | --- | --- |
| System Development | C.3.5.1 | Low | Moderate | Low |

Table ‑ Sensitivity Categorization of Information Types

| Information Type  (Use only information types from NIST SP 800-60, Volumes I and II  as amended) | NIST 800-60 identifier for Associated Information Type | Confidentiality | Integrity | Availability |
| --- | --- | --- | --- | --- |
| System Development | C.3.5.1 | Moderate (M) | Moderate (M) | Moderate (M) |
| Lifecycle/Change | C.3.5.2 | Moderate (M) | Moderate (M) | Moderate (M) |
| System Maintenance | C.3.5.3 | Moderate (M) | Moderate (M) | Moderate (M) |
| IT Infrastructure | C.3.5.4 | Moderate (M) | Moderate (M) | Moderate (M) |

## Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2‑2 Sensitivity Categorization of Information Types, for the cloud.gov, default to the high-water mark for the Information Types as identified in Table 2‑3 Security Impact Level below.

Table ‑ Security Impact Level

| Security Objective | Low, Moderate or High |
| --- | --- |
| Confidentiality | Moderate (M) |
| Integrity | Moderate (M) |
| Availability | Moderate (M) |

Through review and analysis it has been determined that the baseline security categorization for the cloud.gov system is listed in the Table 2‑4 Baseline Security Configuration that follows.

Table ‑ Baseline Security Configuration

|  |  |
| --- | --- |
| cloud.gov Security Categorization | Moderate (M) |

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.

## E-Authentication Determination

The e-Authentication information may be found in section: Section 15 Attachments E-Authentication Level Selection.

Note: Refer to OMB Memo M-04-04 E-Authentication Guidance for Federal Agencies for more information on e-Authentication.

The e-authentication level is Level 3: High confidence in the asserted identity’s validity

Additional e-Authentication information can be found in Section 15 Attachments E-Authentication Level Selection.

# Information System Owner

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

Table ‑ Information System Owner

| Information System Owner Information | |
| --- | --- |
| Name | Shashank Khandelwal |
| Title | Director of cloud.gov |
| Company / Organization | 18F / GSA |
| Address | 1800 F Street NW, Washington, DC, 20405 |
| Phone Number | 319-621-4915 |
| Email Address | shashank.khandelwal@gsa.gov |

# Authorizing Official

The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the JAB P-ATO: FedRAMP, JAB, as comprised of member representatives from the General Services Administration (GSA), Department of Defense (DoD) and Department of Homeland Security (DHS).

# Other Designated Contacts

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

Table ‑ Information System Management Point of Contact

| Information System Management Point of Contact | |
| --- | --- |
| Name | Shashank Khandelwal |
| Title | Director of cloud.gov |
| Company / Organization | 18F / GSA |
| Address | 1800 F Street NW, Washington, DC, 20405 |
| Phone Number | 319-621-4915 |
| Email Address | shashank.khandelwal@gsa.gov |

Table ‑ Information System Technical Point of Contact

| Information System Technical Point of Contact | |
| --- | --- |
| Name | Bret Mogilefsky |
| Title | Program Manager |
| Company / Organization | 18F / GSA |
| Address | 1800 F Street NW, Washington, DC, 20405 |
| Phone Number | 510-610-1956 |
| Email Address | bret.mogilefsky@gsa.gov |

# 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 ‑ CSP Name Internal ISSO (or Equivalent) Point of Contact

| CSP Name Internal ISSO (or Equivalent) Point of Contact | |
| --- | --- |
| Name | Britta Gustafson |
| Title | Deputy Director of cloud.gov |
| Company / Organization | 18F / GSA |
| Address | 1800 F Street NW, Washington, DC, 20405 |
| Phone Number | 415-920-3653 |
| Email Address | britta.gustafson@gsa.gov |

Table ‑ AO ISSO Point of Contact

|  |  |
| --- | --- |
| AO ISSO Point of Contact | |
| Name | FedRAMP ISSO |
| Title | FedRAMP ISSO |
| Organization | FedRAMP |
| Address | 1800 F Street NW, Washington, DC, 20405 |
| Phone Number | <555-555-5555> |
| Email Address | info@fedramp.gov |

# Information System Operational Status

The system is currently in the life-cycle phase shown in Table 7‑1 System Status that follows. (Only operational systems can be granted an ATO).

Table ‑ 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: |

# Information System Type

The cloud.gov makes use of unique managed service provider architecture layer(s).

## Cloud Service Models

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

|  |  |
| --- | --- |
| Question (Yes/No) | Conclusion |
| Does the system use virtual machines? | 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 consumer to build anything other than servers? | A no response means that the system is an IaaS. A yes response means that the system is either a PaaS or an 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 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 an SaaS. A no response means that the system is either a PaaS or an IaaS. |

The layers of the cloud.gov defined in this SSP are indicated in Table 8‑1 Service Layers Represented in this SSP that follows.

Table ‑ Service Layers Represented in this SSP

| Service Provider Architecture Layers | | |
| --- | --- | --- |
|  | Software as a Service (SaaS) | Major Application |
|  | Platform as a Service (PaaS) | Major Application |
|  | Infrastructure as a Service (IaaS) | General Support System |
|  | Other | Explain: |

Note: Refer to NIST SP 800-145 for information on cloud computing architecture models.

## Cloud Deployment Models

Information systems are made up of different deployment models. The deployment models of the cloud.gov that are defined in this SSP and are not leveraged by any other FedRAMP Authorizations, are indicated in Table 8‑2 Cloud Deployment Model Represented in this SSP that follows.

Table ‑ Cloud Deployment Model Represented in this SSP

| Service Provider Cloud Deployment Model | | |
| --- | --- | --- |
|  | Public | Cloud services and infrastructure supporting multiple organizations and agency clients |
|  | Private | Cloud services and infrastructure dedicated to a specific organization/agency and no other clients |
|  | Government Only Community | Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations |
|  | Hybrid | Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data)  AWS GovCloud |

## Leveraged Authorizations

cloud.gov plans to leverages a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by this cloud.gov are listed in Table 8‑3 Leveraged Authorizations that follows.

Table ‑ Leveraged Authorizations

| Leveraged Information System Name | Leveraged Service Provider Owner | Date Granted |
| --- | --- | --- |
| AWS GovCloud (High Baseline) | Amazon Web Services | 6/21/2016 |

# General System Description

This section includes a general description of the cloud.gov.

## System Function or Purpose

18F is a digital services office within the General Services Administration (GSA), an independent agency of the US government. 18F is within the Technology Transformation Services (TTS) within GSA. 18F built **cloud.gov** to help teams responsible for delivering federal digital services to operate those services efficiently and at-scale in a cloud-hosted environment while easing the burden of complying with federal requirements.

cloud.gov is a platform as a service (PaaS), and provides a suite of developer frameworks, application services, and usable management interface tools, which enable teams to develop and deploy applications without directly managing the underlying infrastructure.

cloud.gov is customized for government teams and designed to handle technical, legal, regulatory, and policy requirements common to federal government systems. It addresses security and scalability concerns without requiring many cloud operations experts for system management. By using cloud.gov, teams can skip repetitive foundational work and instead focus on developing and delivering quality applications (and updates to applications) to support their agency’s mission.

The platform runs on top of the AWS GovCloud infrastructure. cloud.gov serves as the middle layer; customers then run their own custom application code on top of cloud.gov.

cloud.gov is a completely open source project, based on 18F’s customized implementation and deployment of open source components. The majority of these components are collectively called **Cloud Foundry**. Cloud Foundry was originally developed by VMware and Pivotal Software. Governance and core development of Cloud Foundry components has since been turned over to the Cloud Foundry Foundation, a not-for-profit 501(c)6 with many commercial members, and an active community of contributors. Documentation for the core Cloud Foundry components is available publicly and will be referenced throughout this document for further information.

## Information System Components and Boundaries

The initial boundaries and components of the system are provided by a public cloud infrastructure as a service (IaaS) provider. The IaaS provider for cloud.gov is Amazon Web Services (AWS). cloud.gov is deployed in AWS GovCloud.

### AWS Components and Boundaries

AWS software components include:

* **Identity and Access Management (IAM)** – access control for services and resources
  + **Multi-Factor Authentication (MFA)** – additional validation of users who want to use IAM roles
* **Virtual Private Clouds (VPCs)** – secure and segmented virtual networks
  + **Elastic Network Interfaces (ENI)** – virtual network interfaces to VPCs
  + **Elastic Load Balancing (ELB**) – public-facing network endpoints that distribute traffic to specified VPCs
* **Elastic Compute Cloud (EC2**) – virtual machines (VMs)
* **Elastic Block Store (EBS**) – persistent block-level storage volumes
* **Relational Database Service (RDS)** – AWS operated databases
* **Simple Storage Service (S3)** – secure and durable object-based storage
* **CloudTrail** – logs all API calls to AWS systems, whether made through the graphical interface of the AWS Management Console, AWS software development kits (SDKs), command line tools, or even higher-level AWS services, such as AWS Config)
* **CloudWatch** – system-wide visibility into resources utilization, performance, and operational health
* **CloudWatch Logs** – agent-based collector of logs for EC2 instances; sends only encrypted data to AWS Kinesis in the AWS US West (Oregon) region for queue management (see <http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/govcloud-cw.html> )
* **Route 53** – highly scalable and automated Domain Name Service (DNS)
* **AWS Config** – resource inventory and full configuration history of other AWS components
* **Trusted Advisor** – AWS Management Console dashboard monitoring cost optimization, performance, fault tolerance, and security.

All underlying physical components and boundaries are managed by AWS. The security documentation for these systems is leveraged through the AWS GovCloud High FedRAMP provisional authority to operate (P-ATO) package ( <https://marketplace.fedramp.gov/index.html#/product/aws-govcloud-high?sort=productName&productNameSearch=aws> ). Similarly, all physical aspects of cloud.gov are outside of our authorization boundary and scope.

While the majority of the AWS software components above are within the AWS GovCloud P-ATO, the following are not:

* AWS Config
* Trusted Advisor
* Route 53

We determined that AWS Config and Trusted Advisor provide important “security support related functions”. The information contained in each service is information AWS already possesses, as a result of AWS being responsible for the underlying infrastructure services.

Activating these services simply makes this same information available to the AWS customer (in this case, 18F/GSA) as well. Given the importance of the data (including a history of AWS configuration state over time), the risk in the government not having access to the same data AWS has far outweighs the risk in activating the services.

Relatedly, managing DNS using AWS tooling significantly reduces the complexity of our operations. By using Route 53, we can fully automate our DNS setup, completely eliminating the risk posed by mistaken or accidental manual changes to the DNS configuration. Combined with the above services tracking the logs and configuration changes to DNS, we have achieved an extremely high level of continuous monitoring across all of our critical dependencies. Additional risk compensation in using Route 53 can be found below in control SC-20.

Accordingly, these AWS components are outside the current authorization boundary and scope for this FedRAMP Joint Authorization Board (JAB) review.

cloud.gov Components and Boundaries

cloud.gov components include a self-service application execution engine, an automation engine for application deployment, lifecycle management tools, scriptable command line interface (CLI), and integrated development tools to ease deployment processes. The platform includes buildpacks for programming language support, and service brokers to provide services such as caching and databases.

Using AWS components, cloud.gov has been built using four VPC environments, two of which are within the authorization boundary:

* **cloud.gov Production VPC** (*inside* the authorization boundary) – Contains both public and private platform components, including: the production EC2 instances supporting the Cloud Foundry deployment; customer applications; and certain enabling services (Application Logs, Databases, and Monitoring).
* **cloud.gov Tooling VPC** (*inside* the authorization boundary) – Contains enabling components which control and deploy the environment, including continuous integration, continuous deployment, configuration management, security scanning, and monitoring. The systems in this VPC deploy all other AWS environments via standard AWS API endpoints. The Tooling VPC has network ingress, egress, protocol and subnet firewall rules which prohibit other VPCs from communicating to restricted components.
* **cloud.gov Staging and Development VPCs** (*outside* the authorization boundary) – Isolated environment to vet components which we have not yet certified for production. Components and source code are tested for reliability, security, access control, and performance prior to being approved for production. The Staging and Development VPCs are prohibited from communication with the Production VPC (by default on AWS, VPCs do not have any network connections to each other; see SC-7 for details on how separation is enforced via AWS-layer controls). All deployments to the Production VPC are made directly – we do not pass any data through the Staging or Development VPC into the Production VPC.

cloud.gov uses **BOSH**, an open source tool for release engineering, deployment, lifecycle management, and monitoring of distributed systems. BOSH is responsible for the orchestration and management of the cloud.gov deployment in AWS. BOSH instruments AWS via a Cloud Provider Interface (CPI) in order to create EC2 virtual machines and EBS storage volumes, then customizing them to perform various roles in the overall system. BOSH’s interaction with AWS is restricted by secret AWS IAM keys only contained within BOSH itself. Cloud Operations staff never directly see or manipulate these keys; instead they invoke authenticated operations via BOSH’s own CLI.

cloud.gov customers use API endpoints to deploy their applications. Each application is always deployed into a specific **Organization** and a specific **Space**. These boundaries are *logical* boundaries, enforced via software. They are not reflected in AWS system architecture diagrams. These logical boundaries serve as the framework to support role-based access control in a multi-tenant platform. See *Table 9‑1 Personnel Roles and Privileges*for a full listing of roles and permissions, and see *10.2 cloud.gov Logical System Environment* for additional information.

The authorization boundary diagram represented within *Figure 9‑1 Network Diagram* depicts the core components which make up the system in its entirety. The diagram specifically depicts components that are within the authorization boundary and those that are outside of the boundary.

Other support services outside the cloud.gov authorization boundary include **PagerDuty**, **New** **Relic, StatusPage, Slack, GitHub,** and **Code Climate**. PagerDuty and Slack are communication tools used by 18F developers, security, and support staff. New Relic, GitHub, and Code Climate are developer tools that support the cloud.gov system. **StatusPage** ( <https://cloudgov.statuspage.io/> ) helps us communicate with our customers about the health of cloud.gov components, and it keeps them updated in the case of an outage or incident.

For a detailed and explicit definition of the system authorization boundary diagram, see *Figure 9‑1 Network Diagram*.

## Types of Users

All GSA users have their employee status categorized with a sensitivity level in accordance with the PS-2 control. Employees (or contractors) of GSA are considered Internal Users. All other users are considered External Users. No guest, anonymous, or temporary user accounts are allowed in any environment within 18F’s AWS account or in cloud.gov.

Because cloud.gov’s customers are often themselves government staff or government contractors, subject to the Office of Personnel Management’s (OPM) guidance on determining the sensitivity of federal positions, some roles require customer agencies to make the final determination. Customer agencies determine the sensitivity and impact of the applications deployed on cloud.gov, and they also decide whether application owners, auditors, managers, and developers are independent or not. These factors are critical to making an OPM FIN 10-06 determination.

Roles that are the responsibility of customer agencies to categorize in their application level system security plans:

* Application System Owner
* Org Manager
* Org Auditor
* Space Manager
* Space Developer
* Space Auditor

All user privileges (after authentication) are described in *Table 9‑1 Personnel Roles and Privileges* that follows.

The system includes GSA users with internal (team) roles, GSA users with external (customer) roles, and users at other agencies with external (customer) roles.

Table ‑ Personnel Roles and Privileges

| Role | Internal or External | Privileged (P), Non-Privileged (NP), or No Logical Access (NLA) | Sensitivity Level | Authorized Privileges | Functions Performed |
| --- | --- | --- | --- | --- | --- |
| External End Users | External | NP | Not Applicable | None | * None |
| Application System Owner | External | NP | Customer Responsibility | Responsible for customer application | * Assigned by cloud.gov customers (example: a federal agency). This role assigns personnel to the External cloud.gov roles listed here. |
| Org Manager | External | NP | Customer Responsibility | Org administrator | * Add and manage users * View users and edit org roles * View the org quota * Create, view, edit, and delete spaces * Invite and manage users in spaces * View the status, number of instances, service bindings, and resource use of each application in every space in the org * Add domains |
| Org Auditor | External | NP | Customer Responsibility | View-only access to org | * View users and org roles * View the org quota |
| Space Manager | External | NP | Customer Responsibility | Space administrator | * Add and manage users in the space * View the status, number of instances, service bindings, and resource use of each application in the space |
| Space Developer | External | NP | Customer Responsibility | Run and configure applications | * Deploy an application * Start or stop an application * Rename an application * Delete an application * Create, view, edit, and delete services in a space * Bind or unbind a service to an application * Rename a space * View the status, number of instances, service bindings, and resource use of each application in the space * Change the number of instances, memory allocation, and disk limit of each application in the space * Associate an internal or external URL with an application |
| Space Auditor | External | NP | Customer Responsibility | View-only access to space | * View the status, number of instances, service bindings, and resource use of each application in the space |
| cloud.gov development and design team | Internal (Technical) | NP | Non-Sensitive / High Risk (Public Trust) | Contribute to product design and engineering | * User access to ci.fr.cloud.gov (continuous deployment system) and grafana.fr.cloud.gov (system-level events and logging) * Read access to Cloud Foundry information about orgs, spaces, users, etc. * User access to modify cloud.gov GitHub repositories controlling content of deployments * This group includes (i.e. is a superset of) Cloud Operations. |
| Cloud Operations | Internal (Technical) | P | Non-Sensitive / High Risk (Public Trust) | System administration and development | * Administrative control of cloud.gov AWS accounts * Administrative control of ci.fr.cloud.gov (continuous deployment system) and grafana.fr.cloud.gov (system-level events and logging) * Administrative control of cloud.gov GitHub repositories * Administrative control of deployments * User access to ephemeral jumpboxes for temporary SSH into AWS EC2 instances |
| System Owner | Internal (Technical) | P | Non-Sensitive / High Risk (Public Trust) | Responsible for cloud.gov | * Ownership of AWS account with full administrative rights to grant access * Ownership of cloud.gov with full administrative rights to grant access * Ownership of overall 18F GitHub organization with full administrative rights to grant access * Grants technical access to personnel * Assigns Cloud Operations roles |
| Program Managers | Internal (Business) | P | Non-Sensitive / Low Risk (Public Trust) | Coordinates team | * Approves personnel assigned to internal (technical) roles including Cloud Operations |
| 18F Supervisors | Internal (Business) | NLA | Non-Sensitive / Low Risk (Public Trust) | Managers for team members | * Assigns personnel to internal (technical) roles other than the System Owner role |
| 18F Talent | Internal (Business) | NLA | Non-Sensitive / Moderate Risk (Public Trust) | 18F-specific support for GSA HR | * Initiates the 18F off-boarding checklist |
| 18F Products and Platforms Director | Internal (Business) | NLA | Non-Sensitive / Low Risk (Public Trust) | Oversight for cloud.gov program | * Assigns the System Owner role * Has ultimate fiduciary and personnel authority and accountability for cloud.gov * Is assigned by the head of the Technology Transformation Services |
| 18F Infrastructure Staff | Internal (Technical) | NP | Non-Sensitive / Moderate Risk (Public Trust) | 18F infrastructure support team | * Final tier of support backing all staff and contracts in Cloud Operations * Write access to DNS * Global read-only access |
| 3PAO | Internal (Technical) | NLA | Non-Sensitive / Low Risk (Public Trust) | Auditor | * Contracted by, and ultimately accountable to the System Owner * Global read-only access during audits or reviews |
| GSA Office of Human Resources Management | Internal (Business) | NLA | Non-Sensitive / Moderate Risk (Public Trust) | Personnel management | * Initiate GSA enterprise level on-boarding, including but not limited to overseeing the issuance of all GSA personal identity verification (PIV) cards |
| GSA Office of General Counsel (OGC) | Internal (Business) | NLA | Non-Sensitive / Low Risk (Public Trust) | Legal | * Advises all GSA teams on the correct application of laws and regulations |
| GSA Information Security (i.e. teams inside of the GSA Office of the Chief Information Security Officer. Includes but is not limited to Information Systems Security Manager (ISSM)s (ISSM) and Information Systems Security Officer (ISSO)s (ISSO).) | Internal (Technical) | NLA | From Non-Sensitive / Low Risk (Public Trust) to Non-Critical Sensitive | Oversight for security | * Access to CloudTrail logs * Access to security scanning tools * Global read-only access |
| GSA SecureAuth Admins | Internal (Technical) | NLA | Non-Sensitive / Moderate Risk (Public Trust | Single sign-on management | * Responsible for any manual resets to GSA SecureAuth passwords, if the password is lost or compromised |

## Network Architecture

*Figure 9‑1 Network Diagram* provides a visual depiction of the system network components that constitute **cloud.gov**. This diagram includes internal and external users (at left); all user connections to user-facing components are over HTTPS.

Figure ‑ Network Diagram

*This diagram is available as an SSP attachment and at* [*https://diagrams.fr.cloud.gov/10-1-network.html*](https://diagrams.fr.cloud.gov/10-1-network.html)

## System Component Architecture

*Figure 9‑2 System Component Architecture Diagram* describes key components above the AWS layer. Each component is labeled with its function in the overall system. Additional information about these components is available at <https://docs.cloudfoundry.org/concepts/architecture/>.

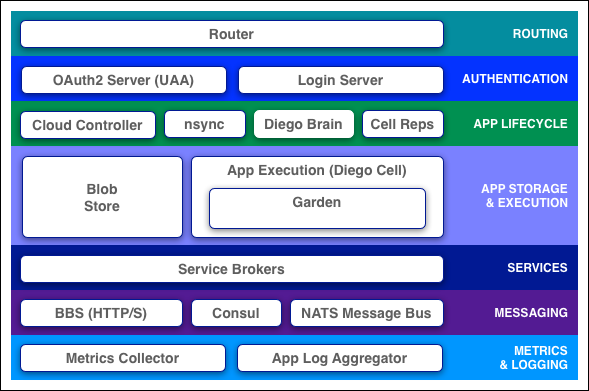


Figure ‑ System Component Architecture Diagram

## Customer Separation

*Figure 9‑3 cloud.gov Customer Internal and External Separation* describes the logical divisions of cloud.gov. Customers are assigned a role within and bound to these divisions. Customer users are initially created with access to nothing. Per *Table 9‑1 Personnel Roles and Privileges*, roles are then assigned based on business need, and grant read-only, read-write, and administrative capabilities accordingly for specific Organizations or Spaces. Customers manage their own application deployments within Spaces.

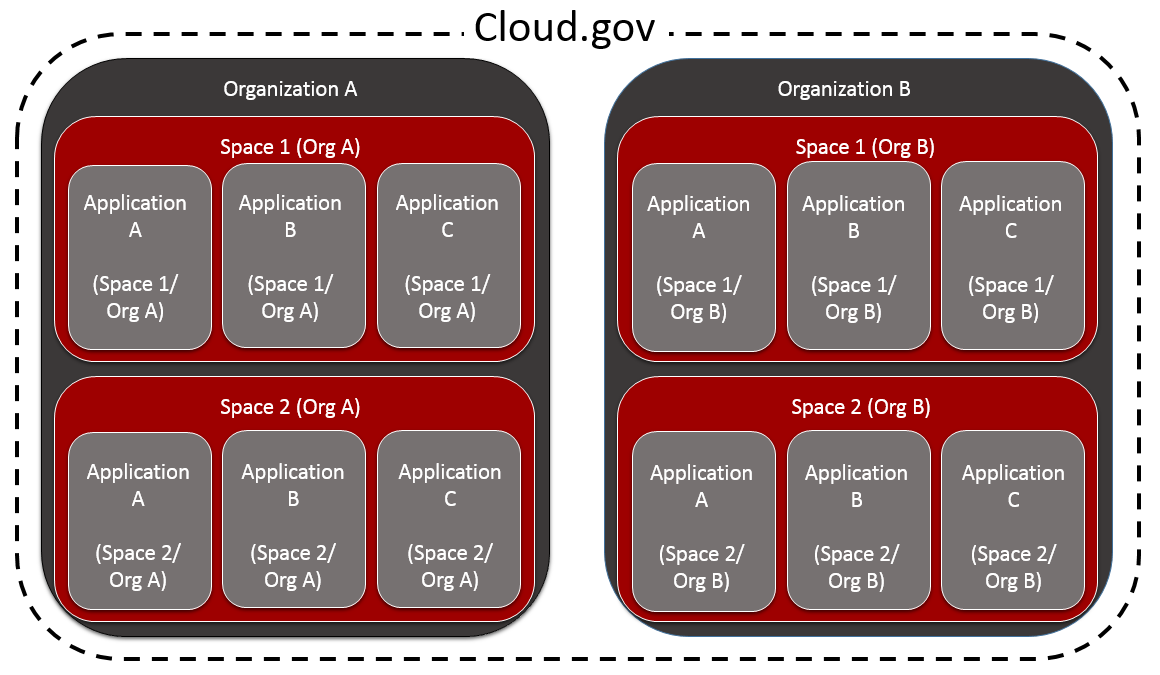


Figure ‑ cloud.gov Customer Internal and External Separation

## Application Isolation

Customer application code is executed in isolated environments using Linux kernel *namespace isolation* and *control groups*. Setting both simultaneously before deploying customer applications and their attendant processes is what is generally called a *container.* All known container systems (Garden, Docker, rkt, etc.) currently use this methodology to provide their containerization.

* **Namespace isolation** – Linux namespaces isolate a process or group of processes. Linux namespaces currently use six types of isolation:  
  + **Mount (mnt)** – sets the hierarchy of the filesystem. While a process within the context of the host OS will see the filesystem rooted at the true /, a process in a container can be made to see the filesystem root at any other location. The process will see an artificial /, and has no ability to see the filesystem beyond.
  + **Process ID (pid)** – sets limits on the processes themselves. A process in a container cannot see the processes running outside its *pid* namespace.
  + **Network (net)** –isolatesan entire network stack for the use of the container, separate from the container’s host OS.
  + **UTS** – creates isolated hostnames and allows for a different hostname for each container
  + **User ID (user)** – isolatesbothuser IDs and group IDs.
* **Control groups (cgroups)** – control and limit the allocation of system resources including CPU, memory, and network bandwidth. Ensures that containers do not impact system availability by using resources beyond a set allotment.

cloud.gov uses the **Garden** runtime for its containers. Garden, is similar to Docker in that it provides higher-level abstractions for manipulating these native Linux kernel capabilities. Garden manipulates the namespaces and cgroups to run a specific set of customer application processes in isolation. As a result, Garden restricts process visibility to only the subset of the host filesystem, network, and process space relevant to the customer application.

# System Environment And Inventory

The following describes cloud.gov as deployed in production.

### Basic structure of cloud.gov within AWS GovCloud

cloud.gov is implemented as hardened EC2 clusters in the Production VPC.

cloud.gov’s binary data store is hosted on AWS S3, and the backend databases are provided by the AWS Relational Database Service (RDS). These are hosted in two geographically-separated locations, otherwise known as AWS Availability Zones.

### Structure of customer application containers

When an application is deployed to our API endpoint, cloud.gov creates an image based on the supplied configuration files, and it stores the image internally. The image is then instantiated as a container, also known as an application instance. To scale up the number of application instances handling traffic, multiple containers are started in parallel based on the same image. When an application is terminated, its associated containers are destroyed. If the process running inside the container crashes, the health monitor terminates the container and creates a new container automatically. A container only ever runs one process, ensuring isolation, security, and resilience.

Customer application instances are distributed amongst “cells” (see “Container Security” below). Only the EC2 instances running “cells” host containers. Customer traffic goes from the Elastic Load Balancer (ELB) through the cloud.gov virtual router layer to the cell. The load-balancing router sits at the front of cloud.gov to route incoming requests to the correct application — essentially to one of the containers where the application’s process is running. The only access points visible on a public network are the ELBs that map to one or more cloud.gov virtual routers and a Network Address Translation (NAT) Virtual Machine (VM). The limited number of contact points with the public internet minimizes the surface area for possible security vulnerabilities. Refer to *Figure 10‑1 Customer Data Flow Diagram* for a visual representation. Further references to the virtual routers will just be referenced as “routers”.

Applications deployed to cloud.gov containers access resources via Services. Applications can access any Service that can be reached through the network (either public or private) if the application has appropriate credentials. In the cloud.gov environment, all external dependencies such as databases, messaging systems, and file systems provided by the platform are considered Services.

Application System Owners provision Services and receive credentials via requests to the cloud.gov API. “Bindings” created by the Application System Owner express an intentional relationship between the Service and a given application. When an application is pushed to cloud.gov, the existence of a binding causes the appropriate credential for accessing the Service to be injected into the application’s environment before it starts. Application System Owners cannot cause the platform to inject service credentials for services that they otherwise do not have permission to see. Injecting these credentials at runtime significantly improves the security of the Service, by preventing credentials from being stored locally on an ever-increasing number of staff and customer laptops and systems.

## cloud.gov Virtual Private Cloud Environment

### Production Public Subnets

The public subnets are used for ELBs that provide HTTPS termination and load balancing. The public subnets limit inbound and outbound access to the internet using AWS Security Groups.

### Production Private Subnets

The private subnets are split into three tiers: Core, Services, and Database.

The Core Tier private subnets are where the cloud.gov EC2 instances, containers, and therefore customer applications reside. Access to these subnets is restricted to Cloud Operations. Private subnets in this tier are split between those reserved for customer application development, maintenance and deployment, while the others are reserved for core Cloud Foundry components. This includes the cloud.gov fallback identity provider (IDP), which functions as a SAML IDP and integrates with cloud.gov Client UAA as described in IA-2 (1) and IA-5 (2).

The Services Tier consists of subnets reserved for external dependencies that are brokered to customer applications, for example data stores such as Redis and Elasticsearch. These services also include the service account (machine user) service, CDN service (for custom domains), and volume services. This tier also hosts the **Elasticsearch**, **Logstash**, **Kibana** (ELK) stack for collection of logging from customer applications.

The Database Tier hosts the cloud.gov configuration (i.e. users, Orgs, and Spaces) within AWS RDS PostgreSQL. These RDS databases are synchronously replicated to a standby replica in a separate hosting location for data redundancy and availability. This is implemented via the configuration of AWS RDS.

### cloud.gov Tooling VPC

The Tooling VPC provides a clear boundary between staging and production and is peered with both Production and Staging VPCs respectively. The Tooling VPC hosts the cloud.gov continuous integration and continuous deployment (CI/CD) services. A VPC peering connection allows the Tooling VPC to route to the Production VPC to support deployments of cloud.gov itself.

The Tooling VPCs subnets are assigned to different AWS Availability Zones.

#### Tooling Public Subnets

The public subnets within the Tooling VPC are used for ELBs that provide HTTPS termination and load balancing to services in the private subnet used by the Cloud Operations team.

#### Tooling Private Subnets

The private subnet is home to three tiers: **Operations**, **Concourse**, and **Database**.

The Operations Tier is home to multiple management services and components, including:

* BOSH
* User Account and Authentication (UAA) servers
* Nessus Manager
* Prometheus / Grafana

**BOSH** is discussed in Section 9.2 above (under “cloud.gov Components and Boundaries”).

**UAA** servers are discussed in Section 10.3 below (under “Identification and Authentication Control”).

**Nessus Manager** provides a web user interface for the Cloud Operations team to review findings about system vulnerabilities (including severity, description, CVE information, and other data). Nessus Manager receives reports of findings from the Nessus Agents that are on every VM (EC2 instance) in the Production VPC; the agents scan those VMs for potential vulnerabilities.

Nessus Manager reports these findings (over a HTTPS connection on port 8834, using the built-in multi-scanner functionality) to the “primary” Nessus Manager (Tenable Security Center) at GSA Information Security (in a GSA VPC), which consolidates vulnerability reporting across the agency.

Nessus Manager continuously fetches threat definition updates from the Tenable website via the Tenable API (over a HTTPS connection on port 443). Nessus Manager retrieves settings updates from the GSA “primary” Nessus Manager (over a HTTPS connection on port 8834, using the built-in multi-scanner functionality), ensuring consistent scans across GSA systems.

**Prometheus** ( <https://prometheus.io/> ), an open source monitor for distributed systems, aggregates information from multiple AWS and cloud.gov components. Principally, Prometheus collects information from security tools running on EC2 hosts (Snort and ClamAV).

**Grafana** ( <http://grafana.org/> ) visualizes Prometheus information for Cloud Operations and GSA Information Security at https://grafana.fr.cloud.gov/. Prometheus also alerts on any events that might require investigation or intervention via sending notifications to PagerDuty. PagerDuty, an external service, notifies on-call Cloud Operations staff via text, phone call, email, or Slack notification that action may be required.

The Concourse Tier is home to **Concourse**. Concourse is cloud.gov’s CI/CD tool. In many ways, it is similar to a Jenkins server. Concourse is not used for cloud.gov customer applications, it is only used for cloud.gov itself. The Concourse Tier consists of web servers that provide the web frontend (bound to an ELB), and worker instances where the CI/CD pipeline jobs and tasks are run by Docker images in containers.

The image base for these containers is an extremely limited version of Linux, with as few dependencies as possible, in order to run tests as quickly as possible. This also radically limits the security surface area, even outside of production. In the Production VPC, the only container runtime currently in use is Garden.

The Cloud Operations team, once authenticated, can run a job that will create a container that can be used as a jumpbox. This jumpbox container is ephemeral. Cloud Operationscan only access production resources by using jumpboxes that are provisioned by Concourse. Direct access to all cloud.gov VMs (for example, by SSH) is prevented by AWS Security Groups on the private subnets.

The Database Tier hosts the cloud.gov deployment configuration used by BOSH (i.e. Cloud Operations users, EC2 instance IDs, and current EC2 health information) within a PostgreSQL RDS database that is synchronously replicated to a standby replica in a separate AWS Availability Zone location for data redundancy and availability.

### cloud.gov Development VPC

cloud.gov includes a development environment deployed into its own VPC, which has security groups configured to only allow access from GSA networks and to isolate it from the the staging and production VPCs.

Code from the development environment is never promoted directly to production.  Any changes developed in this environment are introduced to the staging environment following the procedures documented in RA-5, SA-3, and SI-2.

This development environment is outside of our authorization boundary.

The VPC Peering Connection enables the Tooling VPC to deploy and monitor applications in the Development VPC.

## cloud.gov Logical System Environment

cloud.gov has a flexible model for isolating customers, defined through Organizations, Spaces, and user roles. The illustration in *Figure 9‑3 cloud.gov Customer Internal and External Separation* provides a high-level view of how these are arranged within cloud.gov. cloud.gov uses buildpacks to provision custom filesystem content as needed for each customer application deployed in a Space.

### Organizations

At the top of the structural hierarchy are Organizations (Orgs). They serve as the governance boundary for all the users in the Org along three dimensions: quotas, service availability, and custom domains. cloud.gov hosts different Orgs representing agencies or programs and keeps the resources associated with each of them separate. User accounts can access an Org if they have been granted a role within it. See *Table 9‑1 Personnel Roles and Privileges*for details.

### Spaces

Within organizations are Spaces, which define a set of resources scoped to a particular project, team, or environment. Resource types include service instances and routes for user traffic. A Space provides a shared location for application development, deployment, and maintenance, and users will have specific space-related roles. See *Table 9‑1 Personnel Rol*es and Privilegesfor more details.

cloud.gov automatically creates a specialized “sandbox” Space (in a sandbox Org) for each user who has a federal email address, for use as a test environment -- not for production applications or production data. The user receives “Space Manager”, “Space Developer”, and “Space Auditor” access to that Space. Sandbox Space data is automatically deleted periodically.

### Buildpacks

Customer applications are deployed using buildpacks, which scan the desired application in order to identify which required libraries should be installed and provide application language (Ruby, Python, Go, etc.) support. Buildpacks install language runtimes, libraries, and configurations inside the image, alongside the application content. From that image, the platform instantiates containers, isolated from other tenants, within which the application’s process will run.

Customer Responsibility for compliance and security of their application is minimized by using one of the platform’s supported buildpacks: <https://cloud.gov/overview/technology/responsibilities/>

Buildpack technical specifications and configuration options are exhaustively documented for each supported application language: <https://docs.cloudfoundry.org/buildpacks/>

For each supported buildpack, the table below contains a pointer to general documentation as well as specific links to notable subsections detailing how it can be configured by the customer.

|  |  |  |
| --- | --- | --- |
| Buildpack | Documentation | Configurable items (from that documentation) |
| Java | <https://docs.cloudfoundry.org/buildpacks/java/index.html> | Custom trusted certificates (<https://docs.cloudfoundry.org/buildpacks/java/bosh_custom_trusted_certs.html>) |
| Ruby | <https://docs.cloudfoundry.org/buildpacks/ruby/index.html> | Ruby version (<https://docs.cloudfoundry.org/buildpacks/ruby/index.html#runtime>)  Proxy support (<https://docs.cloudfoundry.org/buildpacks/ruby/index.html#proxy_support>)  Custom Trusted Certificate Support (<https://docs.cloudfoundry.org/buildpacks/ruby/index.html#bosh_trusted_cert>) |
| Node.js | <https://docs.cloudfoundry.org/buildpacks/node/index.html> | Node.js and NPM version (<https://docs.cloudfoundry.org/buildpacks/node/index.html#runtime>)  Proxy support (<https://docs.cloudfoundry.org/buildpacks/node/index.html#proxy_support>)  Custom Trusted Certificate Support (<https://docs.cloudfoundry.org/buildpacks/node/index.html#bosh_trusted_cert>)  Node-specific environment variables (<https://docs.cloudfoundry.org/buildpacks/node/node-environment.html>) |
| Binary | <https://docs.cloudfoundry.org/buildpacks/binary/index.html> | Port (<https://docs.cloudfoundry.org/buildpacks/binary/index.html#compiling>)  Custom Trusted Certificate Support (<https://docs.cloudfoundry.org/buildpacks/binary/index.html#bosh_trusted_cert>) |
| Go | <https://docs.cloudfoundry.org/buildpacks/go/index.html> | Start command (<https://docs.cloudfoundry.org/buildpacks/go/index.html#start_command>)  Passing a Symbol and String to the Linker (<https://docs.cloudfoundry.org/buildpacks/go/index.html#passing_symbol_linker>)  Building with C dependencies (<https://docs.cloudfoundry.org/buildpacks/go/index.html#c_dependencies>)  Proxy support (<https://docs.cloudfoundry.org/buildpacks/go/index.html#proxy_support>)  Custom Trusted Certificate Support (<https://docs.cloudfoundry.org/buildpacks/go/index.html#bosh_trusted_cert>) |
| PHP | <https://docs.cloudfoundry.org/buildpacks/php/index.html> | This buildpack has its own page of documentation about all its configurable items: <https://docs.cloudfoundry.org/buildpacks/php/gsg-php-config.html> |
| Python | <https://docs.cloudfoundry.org/buildpacks/python/index.html> | Python version (<https://docs.cloudfoundry.org/buildpacks/python/index.html#runtime>)  Start command (<https://docs.cloudfoundry.org/buildpacks/python/index.html#start-command>)  Proxy support (<https://docs.cloudfoundry.org/buildpacks/python/index.html#proxy_support>)  Custom Trusted Certificate Support (<https://docs.cloudfoundry.org/buildpacks/python/index.html#bosh_trusted_cert>) |
| Staticfile | <https://docs.cloudfoundry.org/buildpacks/staticfile/index.html> | This buildpack has its own section of documentation about all its configurable items: <https://docs.cloudfoundry.org/buildpacks/staticfile/index.html#configuration> |

### Secrets

Customer applications consume services by binding to service instances using the Cloud Foundry Service Broker interface. Binding a service instance to an application causes the platform to inject secrets (credentials) associated with the service instance to the local environment of the application when it runs. The application can then reference the credentials using local environment variables, which cannot be accessed by other platform customers without access to that space.

* Cloud Foundry Security Concepts: <https://docs.cloudfoundry.org/concepts/security.html>
* Cloud Foundry Service Broker interface: [https://docs.cloudfoundry.org/services/api.html](https://docs.cloudfoundry.org/concepts/security.html)

### Services

Services available for customer applications:

|  |  |  |
| --- | --- | --- |
| Service | Major plan types | Managed AWS service access (if any) |
| CDN |  | AWS CloudFront |
| Elasticsearch |  |  |
| Redis |  |  |
| Relational databases | PostgreSQL, MySQL, Oracle | AWS RDS |
| S3 |  | AWS S3 |
| Identity provider |  |  |
| Service account |  |  |
| Volume services |  |  |

## cloud.gov Security Domain Stack

### Identification and Authentication Control

#### AWS

The AWS Identity and Access Management (IAM) service is accessed via a unique username, password, and a one-time random password generated via a local authenticator application on a mobile device, such as Google Authenticator, Duo, or Authy. MFA is required. IAM access is extremely minimal.

IAM controls access to all AWS-provided components and services used. Each user is assigned specific permissions within IAM with the absolute minimum privileges required to perform their job. With the exception of the IAM permissions granted while bootstrapping and deploying cloud.gov from scratch, Cloud Operations staff are restricted to read-only IAM roles. This enables them troubleshoot by inspecting the environment while ensuring that changes to the deployment are repeatable via CI/CD and auditable via version control. Read-write IAM roles are restricted to BOSH, which is then invoked by the CI/CD system.

#### cloud.gov

Staff with internal cloud.gov roles per ***Table 9-1*** ***User Roles and Privileges*** always use MFA. All cloud.gov User Account and Authentication (UAA) servers are integrated with GSA’s enterprise-wide single-sign on provider, GSA SecureAuth. (GSA SecureAuth is managed by the GSA CIO, and it has its own ATO under the GSA CIO.) Currently cloud.gov has two UAA servers. The **Operations UAA server** is for Cloud Operations – the **Client UAA server** is for customers or GSA users of cloud.gov.

GSA SecureAuth access is bound to the internal user successfully being issued a GSA personal identity verification (PIV) card according to Homeland Security Presidential Directive 12 (HSPD-12). Staff with internal roles login via a unique username, password, and one-time random password generated by the GSA SecureAuth system and sent via email, text, automatic phone call, or generated locally via a mobile application using the Time-based One Time Passwords (TOTP) method ( <https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm> ).

To access EC2 instances within cloud.gov, Cloud Operations spin up ephemeral jumpbox containers as detailed in the ***Tooling Private Subnets*** section. Access to ephemeral jumpbox containers for Cloud Operations is implemented via the Operations UAA server, a UAA server just for Cloud Operations. The Operations UAA server is integrated into GSA SecureAuth as well, and the authentication flow is identical to the above.

Once authentication is complete, Cloud Operations staff request shell access to the ephemeral jumpbox container with network access to the EC2 instances within the relevant VPC. This container is temporary, and it is destroyed as soon as the operator’s session ends. The operator invokes BOSH within this ephemeral container to establish an SSH session with the target host. BOSH establishes a new credential on the target host, starts the operator’s SSH session using that credential, and removes the credential when the operator’s SSH session ends. Refer to *Figure 10‑2 Jumpbox Data Flow Diagram* for a visual representation of this workflow.

Customers log into the cloud.gov web user interface ( <https://dashboard.fr.cloud.gov/> ) or establish a session via a terminal command-line interface. Both interfaces use the Client UAA to establish the user’s session. Customers cannot establish a valid session without using MFA. All traffic from the public internet is non-optional HTTPS. Once a session is established, customers are able to access Orgs and Spaces according to their assigned roles. Customers are responsible for enabling their own authentication, authorization, and MFA for any end users of their applications.

Customers can integrate their agency single sign-on (SSO) identity providers with cloud.gov in order to use them to authenticate with cloud.gov, using SAML integration. If they do not integrate their identity providers, they can use the cloud.gov fallback identity provider (IDP).

Customers can create machine users (service accounts), with automatically-generated usernames and passwords, with limited permissions, for use in deployment scripts and other programs.

### ACLs, Software Defined Firewalls, and Security Groups

#### AWS

VPCs are configured to utilize routing tables, network access control lists, subnet rules, and security group (firewall) rules. Each of these controls must have appropriate rules and routes in-place before any external service is able to reach a host within cloud.gov.

Amazon S3 Access Control Lists (ACLs) enable Cloud Operations to manage access to buckets and objects. Each bucket and object has an ACL attached to it as a sub-resource. The ACL defines which AWS accounts or groups are granted access and the type of access. When a request is received against a resource, Amazon S3 checks the corresponding ACL to verify the requester has the necessary access permissions. When a bucket or an object is created, Amazon S3 creates a default ACL that grants the resource owner full control over the resource. A grantee can be an AWS account or one of the predefined Amazon S3 groups.

Each cloud.gov EC2 instance or group of instances is assigned to at least one Security Group with specific assigned roles. These roles delineate what traffic is allowed inbound and outbound for each instance by allowing or denying ports, protocols, and services.

#### cloud.gov

cloud.gov application security groups (ASGs) control the traffic flowing out of applications. Each container hosting an application uses the container namespaces above to provide a dedicated virtual network interface. Security groups are set before an application starts. Application security groups are a collection of “allow” rules that can be made with global or application specific assignments, enabling access to be set on individual application requirements. These rules are exclusively whitelists, which are layered on top of a series of container-centric lock-downs, allowing for extremely limited access.

### Audit Logging, Monitoring, and Intrusion Detection

#### AWS

**CloudTrail** provides visibility into user activity by recording all actions (including API calls) taken on an AWS account. CloudTrail records important information about each action, including the name of the API, the identity of the caller, the time of the API call, the request parameters, and the response elements returned by the AWS service. This information ensures changes can be tracked, security logs correlated, and operational issues resolved quickly.

**CloudWatch** provides resource monitoring. CloudWatch allows monitoring in near real-time, of EC2 instances, Amazon Elastic Block Store (EBS) volumes, Amazon Elastic Load Balancers ELBs), and Amazon Relational Database Service (RDS) instances. Metrics such as CPU utilization, latency, and request counts are provided automatically. CloudWatch Logs Agents captures all log output on EC2 hosts.

#### cloud.gov

**Elasticsearch**, **Logstash**, and **Kibana** (the ELK or Elastic stack) provides centralized audit logging and monitoring of cloud.gov components, applications, and data APIs. In other systems, this capability is provided by services such as Splunk. The logs captured from the ELK ( <https://www.elastic.co/> ) stack can be used in forensic analysis to track down the time of intrusion, as well as the method used to penetrate into the network.

Logstash is the centralized logging and parsing data pipeline that is used to process logs in different formats. Logstash uses different rules to format each log message into multiple fields, which are indexed by the Elasticsearch engine for deep searches and data analytics. Kibana is the web visualization interface to the collected data. Customers can easily view and analyze collected application logs according to their permissions. Cloud Operations can additionally view logs from the platform itself. Grafana then provides a centralized dashboard for all events and metrics monitored by Cloud Operations within the environment.

All logs in Elasticsearch are also sent to CloudWatch Logs as an additional secure storage location.

**Snort** ( <https://www.snort.org/> ) is cloud.gov’s network Intrusion Detection System (IDS) providing real-time traffic analysis and packet logging. It detects attacks and anomalies based on general rulesets and threat signatures published on a regular basis to the security community.

**Tripwire** ( <https://github.com/Tripwire/tripwire-open-source> ) provides cloud.gov’s file integrity monitoring (FIM) system. Tripwire validates the integrity of critical files, ensuring alerts are sent out if the desired and “good” baseline is altered by adversarial actors or systems. File integrity checks are performed via checksum comparison. Tripwire runs on all EC2 hosts in cloud.gov’s AWS account.

**ClamAV** ( <https://www.clamav.net/> ) is an engine for detecting trojans, viruses, malware and other malicious threats. ClamAV runs on all EC2 hosts in cloud.gov’s AWS account.

Refer to *Figure 10‑3 Monitoring and Alerting Data Flow Diagram* for a visual representation of the relationship between these components.

### Vulnerability Scanning and Penetration Testing

GSA Information Security uses Nessus for vulnerability scanning of the environment. Nessus runs baseline configurations scans, compliance scans, virtual infrastructure, and network scans using custom scan policies and templates. Access to the Nessus Manager is limited to the GSA IP addresses space only. Nessus runs authenticated scans against cloud.gov components. Nessus allows Cloud Operations and GSA Information Security to track risk level changes based on remediation efforts.

Cloud Operations, GSA Information Security, and 18F Infrastructure utilize OWASP ZAP for web application scanning of information systems and components. Similar to Burp, it provides the capabilities needed for automated and manual penetration testing. 18F’s 3PAO also uses a collection of penetration testing tools when conducting assessments, including but not limited to Nessus, Nmap, Acunetix WVS, AppDetectivePro, Burp Suite Pro, Cobalt Strike, John the Ripper, and other tools that may be including in the Kali Linux operating system distribution.

Penetration testing tools installed locally on assessor machines and not installed onto servers into the cloud.gov environment; they are therefore not part of the cloud.gov system ATO boundary.

### Cloud Network Inventory and Asset Management

AWS Config provides a complete inventory of AWS resources with all configuration details and audits how a resource was configured at any point in time, and it can send notifications when the configuration of a resource changes. AWS Config provides a complete configuration history. Snapshots of the history can be exported using AWS APIs and sent to a specified Amazon S3 bucket.

### Static and Dynamic Code Analysis

18F requires continuous code scanning as described in SI-3.

### Incident Response Resolution and Communication

Internal users use PagerDuty for incident response and communication. PagerDuty integrates with cloud.gov’s monitoring and alerting tools, and it also sends notifications to our communication tools. PagerDuty allows Cloud Operations and the entire team to quickly detect, triage, and resolve incidents from development through production.

The team reports all incidents to the GSA Information Security Incident Response Team in the Security Engineering Division, in agreement with the GSA *Incident Handling* procedural guide. The Incident Response Team coordinates formal actions and facilitates required reporting to GSA management, US-CERT, other agencies, and external law enforcement organizations, as necessary.

### Configuration Management and Version Control

cloud.gov’s configuration management process consists of GitHub, which provides distributed version control of all code, Terraform ( <https://www.terraform.io/> ) which provides “infrastructure configuration as code”, Concourse, and BOSH. Baselines, configuration files, and all “infrastructure as code” is stored in GitHub and local (on cloud.gov team government laptops) Git repositories to provide distributed version control. All builds run inside their own containers, so installing packages does not pollute other builds.

See CM-1 and CM-2 for detailed information, policies, and procedures.

## Hardware Inventory

cloud.gov is completely virtualized within the boundary of AWS. There are no hardware components within the scope or authorization boundary.

## Software Inventory

See the cloud.gov inventory provided as an attachment to this SSP.

## Network Inventory

cloud.gov is completely virtualized within the boundary of AWS. There are no network components within the scope or authorization boundary.

## Data Flow

Figure ‑ Customer Data Flow Diagram

*This diagram is available as an SSP attachment and at* [*https://diagrams.fr.cloud.gov/10-4.1-customer-data-flow.html*](https://diagrams.fr.cloud.gov/10-4.1-customer-data-flow.html)

Figure ‑ Jumpbox Data Flow Diagram

*This diagram is available as an SSP attachment and at* [*https://diagrams.fr.cloud.gov/10-4.2-jumpbox.html*](https://diagrams.fr.cloud.gov/10-4.2-jumpbox.html)

Figure ‑ Monitoring and Alerting Data Flow Diagram

*This diagram is available as an SSP attachment and at* [*https://diagrams.fr.cloud.gov/10-4.3-monitoring.html*](https://diagrams.fr.cloud.gov/10-4.3-monitoring.html)

Figure ‑ Software Deployment Data Flow Diagram

*This diagram is available as an SSP attachment and at* [*https://diagrams.fr.cloud.gov/10-4.4-software-deployment.html*](https://diagrams.fr.cloud.gov/10-4.4-software-deployment.html)

### Firewall Rules

There are multiple architecture components which restrict traffic, protocol and port access:

* **ELB – Elastic Load Balancer**
  + These virtual devices are the only publicly-accessible endpoints in the architecture. These devices are configured to allow traffic from 80, 443, and 4443 to specific servers.
* **Routers** 
  + These components route traffic according to the API endpoint called and the authorization credentials presented by the request. See <https://docs.cloudfoundry.org/concepts/architecture/router.html> and <https://docs.cloudfoundry.org/concepts/security.html#containers>
* **VPC – Virtual Private Cloud**
  + Settings are configured via automation through <https://github.com/18F/cg-provision>
* **Visibility**
  + Traffic in and out of a VPC is noted in Flow Logs which are sent to Amazon CloudWatch Logs and retained indefinitely.

## Ports, Protocols and Services

The table below lists the Ports, Protocols, and Services enabled in this information system.

Table ‑ Ports, Protocols and Services

| Ports (TCP/UDP)\* | Protocols | Services | Purpose | Used By |
| --- | --- | --- | --- | --- |
| 443 (T) on \*.fr.cloud.gov ELB | HTTPS | HTTPS | cloud.gov web services, communication between services | AWS, cloud.gov, some services (such as Nessus Manager) |
| 443 (T) on Loggregator ELB | TCP | WebSockets over TLS | WebSocket traffic | From outside of system boundary to inside: Loggregator/Doppler (cf logs) |
| 80 (T) | HTTP | HTTP | Redirect to HTTPS | AWS, cloud.gov |
| 22 (T), 2222 (T), 443 (T) | SSH | Secure Shell (SSH) | Secure command line interface | From outside of system boundary to inside: customer CF SSH access to apps |
| 53 (U) | DNS | DNS | Inbound DNS requests | AWS, cloud.gov |
| 4222 (T) | TCP | NATS bus messaging service | Provides publish-subscribe and distributed queueing messaging system internally between relevant cloud.gov components | cloud.gov |
| 6868 (T) | HTTP | BOSH agent interface | The BOSH Agent executes tasks in response to messages it receives from the BOSH Director. | cloud.gov |
| 123 (T) | NTP | Network Time Protocol (NTP) | Sync time within the network | AWS CloudTrail, cloud.gov syslogs |
| NA | ICMP | Internet Control Message | Information and diagnostics for network devices | AWS, cloud.gov |
| 2222 (T) | SSH | Secure Shell (SSH) | External port for SSH access for apps | cloud.gov ephemeral jumpbox |
| 4443 (T) | TCP | WebSockets over TLS | WebSocket traffic | cloud.gov |
| 3000 (T) | HTTPS | Grafana HTTPS server | Grafana back-end | Grafana |
| 5432 | TCP | PostgreSQL | BOSH’s database | BOSH |
| 8081 (T) | TCP | User account and authentication servers (UAA) | Provide identity management and authorization services | UAA Servers |
| 25250 (T) | TCP | BOSH Blobstore | Storage repository for BOSH | cloud.gov ephemeral jumpbox |
| 25555 (T) | HTTP | BOSH Director | Coordinates the Agents and responds to user requests and system events | cloud.gov ephemeral jumpbox |
| 25777 (T) | TCP | BOSH | Tracks all AWS infrastructure that has been provisioned by BOSH (EC2, EBS, etc.) | cloud.gov ephemeral jumpbox |
| 8834 (T) | HTTPS | Nessus multi-scanner and Nessus Agents | Send findings and receive settings | Nessus |

\* Transmission Control Protocol (TCP), User Diagram Protocol (UDP)

# System Interconnections

cloud.gov has no system interconnections. This is consistent with Table 13‑3 CA-3 Authorized Connections.

# Laws, Regulations, Standards and Guidance

A summary of FedRAMP Laws and Regulations is included in ATTACHMENT 12 – FedRAMP Laws and Regulations.

## Applicable Laws and Regulations

The FedRAMP Laws and Regulations can be found on this web page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

Table 12‑1 cloud.gov Laws and Regulations includes additional laws and regulations specific to cloud.gov.

Table ‑ cloud.gov Laws and Regulations

|  |  |  |  |
| --- | --- | --- | --- |
| Identification Number | Title | Date | Link |
| N/A | N/A | N/A | N/A |

## Applicable Standards and Guidance

The FedRAMP Standards and Guidance be found on this web page: [Templates](https://www.fedramp.gov/resources/templates-2016/)

Table 12‑2 cloud.gov Standards and Guidance includes in this section any additional standards and guidance specific to cloud.gov.

Table ‑ cloud.gov Standards and Guidance

|  |  |  |  |
| --- | --- | --- | --- |
| Identification Number | Title | Date | Link |
| N/A | N/A | N/A | N/A |

# Minimum Security Controls

Security controls must meet minimum security control baseline requirements. Upon categorizing a system as Low, Moderate, or High sensitivity in accordance with FIPS 199, the corresponding security control baseline standards apply. Some of the control baselines have enhanced controls which are indicated in parentheses.

Security controls that are representative of the sensitivity of cloud.gov are described in the sections that follow. Security controls that are designated as “Not Selected” or “Withdrawn by NIST” are not described unless they have additional FedRAMP controls. Guidance on how to describe the implemented standard can be found in NIST 800-53, Rev 4. Control enhancements are marked in parentheses in the sensitivity columns.

Systems that are categorized as FIPS 199 Low use the controls designated as Low, systems categorized as FIPS 199 Moderate use the controls designated as Moderate and systems categorized as FIPS 199 High use the controls designated as High. A summary of which security standards pertain to which sensitivity level is found in Table 13‑1 Summary of Required Security Controls that follows.

Table ‑ Summary of Required Security Controls

| ID | Control Description |  | | Sensitivity Level |  |
| --- | --- | --- | --- | --- | --- |
| Low | | Moderate | High |
| AC | Access Control |  | |  |  |
| AC-1 | Access Control Policy and Procedures | AC-1 | | AC-1 | AC-1 |
| AC-2 | Account Management | AC-2 | | AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12) | AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (11) (12) (13) |
| AC-3 | Access Enforcement | AC-3 | | AC-3 | AC-3 |
| AC-4 | Information Flow Enforcement | Not Selected | | AC-4 (21) | AC-4 (8) (21) |
| AC-5 | Separation of Duties | Not Selected | | AC-5 | AC-5 |
| AC-6 | Least Privilege | Not Selected | | AC-6 (1) (2) (5) (9) (10) | AC-6 (1) (2) (3) (5) (7) (8) (9) (10) |
| AC-7 | Unsuccessful Logon Attempts | AC-7 | | AC-7 | AC-7 (2) |
| AC-8 | System Use Notification | AC-8 | | AC-8 | AC-8 |
| AC-10 | Concurrent Session Control | Not Selected | | AC-10 | AC-10 |
| AC-11 | Session Lock | Not Selected | | AC-11 (1) | AC-11 (1) |
| AC-12 | Session Termination | Not Selected | | AC-12 | AC-12 (1) |
| AC-14 | Permitted Actions Without Identification or Authentication | AC-14 | | AC-14 | AC-14 |
| AC-17 | Remote Access | AC-17 | | AC-17 (1) (2) (3) (4) (9) | AC-17 (1) (2) (3) (4) (9) |
| AC-18 | Wireless Access | AC-18 | | AC-18 (1) | AC-18 (1) (3) (4) (5) |
| AC-19 | Access Control For Mobile Devices | AC-19 | | AC-19 (5) | AC-19 (5) |
| AC-20 | Use of External Information Systems | AC-20 | | AC-20 (1) (2) | AC-20 (1) (2) |
| AC-21 | Information Sharing | Not Selected | | AC-21 | AC-21 |
| AC-22 | Publicly Accessible Content | AC-22 | | AC-22 | AC-22 |
| AT | Awareness and Training |  | |  |  |
| AT-1 | Security Awareness and Training Policy and Procedures | AT-1 | | AT-1 | AT-1 |
| AT-2 | Security Awareness Training | AT-2 | | AT-2 (2) | AT-2 (2) |
| AT-3 | Role-Based Security Training | AT-3 | | AT-3 | AT-3 (3) (4) |
| AT-4 | Security Training Records | AT-4 | | AT-4 | AT-4 |
| AU | Audit and Accountability |  | |  |  |
| AU-1 | Audit and Accountability Policy and Procedures | AU-1 | | AU-1 | AU-1 |
| AU-2 | Audit Events | AU-2 | | AU-2 (3) | AU-2 (3) |
| AU-3 | Content of Audit Records | AU-3 | | AU-3 (1) | AU-3 (1) (2) |
| AU-4 | Audit Storage Capacity | AU-4 | | AU-4 | AU-4 |
| AU-5 | Response to Audit Processing Failures | AU-5 | | AU-5 | AU-5 (1) (2) |
| AU-6 | Audit Review, Analysis and Reporting | AU-6 | | AU-6 (1) (3) | AU-6 (1) (3) (4) (5) (6) (7) (10) |
| AU-7 | Audit Reduction and Report Generation | Not Selected | | AU-7 (1) | AU-7 (1) |
| AU-8 | Time Stamps | AU-8 | | AU-8 (1) | AU-8 (1) |
| AU-9 | Protection of Audit Information | AU-9 | | AU-9 (2) (4) | AU-9 (2) (3) (4) |
| AU-10 | Non-repudiation | Not Selected | | Not Selected | AU-10 |
| AU-11 | Audit Record Retention | AU-11 | | AU-11 | AU-11 |
| AU-12 | Audit Generation | AU-12 | | AU-12 | AU-12 (1) (3) |
| CA | Security Assessment and Authorization | | |  |  |
| CA-1 | Security Assessment and Authorization Policies and Procedures | CA-1 | | CA-1 | CA-1 |
| CA-2 | Security Assessments | CA-2 (1) | | CA-2 (1) (2) (3) | CA-2 (1) (2) (3) |
| CA-3 | System Interconnections | CA-3 | | CA-3 (3) (5) | CA-3 (3) (5) |
| CA-5 | Plan of Action and Milestones | CA-5 | | CA-5 | CA-5 |
| CA-6 | Security Authorization | CA-6 | | CA-6 | CA-6 |
| CA-7 | Continuous Monitoring | CA-7 | | CA-7 (1) | CA-7 (1) (3) |
| CA-8 | Penetration Testing | Not Selected | | CA-8 (1) | CA-8 (1) |
| CA-9 | Internal System Connections | CA-9 | | CA-9 | CA-9 |
| CM | Configuration Management |  | |  |  |
| CM-1 | Configuration Management Policy and Procedures | CM-1 | | CM-1 | CM-1 |
| CM-2 | Baseline Configuration | CM-2 | | CM-2 (1) (2) (3) (7) | CM-2 (1) (2) (3) (7) |
| CM-3 | Configuration Change Control | Not Selected | | CM-3 (2) | CM-3 (1) (2) (4) (6) |
| CM-4 | Security Impact Analysis | CM-4 | | CM-4 | CM-4 (1) |
| CM-5 | Access Restrictions For Change | Not Selected | | CM-5 (1) (3) (5) | CM-5 (1) (2) (3) (5) |
| CM-6 | Configuration Settings | CM-6 | | CM-6 (1) | CM-6 (1) (2) |
| CM-7 | Least Functionality | CM-7 | | CM-7 (1) (2) (5)\* | CM-7 (1) (2) (5) |
| CM-8 | Information System Component Inventory | CM-8 | | CM-8 (1) (3) (5) | CM-8 (1) (2) (3) (4) (5) |
| CM-9 | Configuration Management Plan | Not Selected | | CM-9 | CM-9 |
| CM-10 | Software Usage Restrictions | CM-10 | | CM-10 (1) | CM-10 (1) |
| CM-11 | User-Installed Software | CM-11 | | CM-11 | CM-11 (1) |
| \*FedRAMP does not include CM-7 (4) in the Moderate Baseline. NIST supplemental guidance states that CM-7 (4) is not required if (5) is implemented. | | | | | |
| CP | Contingency Planning |  | |  |  |
| CP-1 | Contingency Planning Policy and Procedures | CP-1 | | CP-1 | CP-1 |
| CP-2 | Contingency Plan | CP-2 | | CP-2 (1) (2) (3) (8) | CP-2 (1) (2) (3) (4) (5) (8) |
| CP-3 | Contingency Training | CP-3 | | CP-3 | CP-3 (1) |
| CP-4 | Contingency Plan Testing | CP-4 | | CP-4 (1) | CP-4 (1) (2) |
| CP-6 | Alternate Storage Site | Not Selected | | CP-6 (1) (3) | CP-6 (1) (2) (3) |
| CP-7 | Alternate Processing Site | Not Selected | | CP-7 (1) (2) (3) | CP-7 (1) (2) (3) (4) |
| CP-8 | Telecommunications Services | Not Selected | | CP-8 (1) (2) | CP-8 (1) (2) (3) (4) |
| CP-9 | Information System Backup | CP-9 | | CP-9 (1) (3) | CP-9 (1) (2) (3) (5) |
| CP-10 | Information System Recovery and Reconstitution | CP-10 | | CP-10 (2) | CP-10 (2) (4) |
| IA | Identification and Authentication |  | |  |  |
| IA-1 | Identification and Authentication Policy and Procedures | IA-1 | | IA-1 | IA-1 |
| IA-2 | Identification and Authentication (Organizational Users) | IA-2 (1) (12) | | IA-2 (1) (2) (3) (5) (8) (11) (12) | IA-2 (1) (2) (3) (4) (5) (8) (9) (11) (12) |
| IA-3 | Device Identification and Authentication | Not Selected | | IA-3 | IA-3 |
| IA-4 | Identifier Management | IA-4 | | IA-4 (4) | IA-4 (4) |
| IA-5 | Authenticator Management | IA-5 (1) (11) | | IA-5 (1) (2) (3) (4) (6) (7) (11) | IA-5 (1) (2) (3) (4) (6) (7) (8) (11) (13) |
| IA-6 | Authenticator Feedback | IA-6 | | IA-6 | IA-6 |
| IA-7 | Cryptographic Module Authentication | IA-7 | | IA-7 | IA-7 |
| IA-8 | Identification and Authentication (Non-Organizational Users) | IA-8 (1) (2) (3) (4) | | IA-8 (1) (2) (3) (4) | IA-8 (1) (2) (3) (4) |
| IR | Incident Response |  | |  |  |
| IR-1 | Incident Response Policy and Procedures | IR-1 | | IR-1 | IR-1 |
| IR-2 | Incident Response Training | IR-2 | | IR-2 | IR-2 (1) (2) |
| IR-3 | Incident Response Testing | Not Selected | | IR-3 (2) | IR-3 (2) |
| IR-4 | Incident Handling | IR-4 | | IR-4 (1) | IR-4 (1) (2) (3) (4) (6) (8) |
| IR-5 | Incident Monitoring | IR-5 | | IR-5 | IR-5 (1) |
| IR-6 | Incident Reporting | IR-6 | | IR-6 (1) | IR-6 (1) |
| IR-7 | Incident Response Assistance | IR-7 | | IR-7 (1) (2) | IR-7 (1) (2) |
| IR-8 | Incident Response Plan | IR-8 | | IR-8 | IR-8 |
| IR-9 | Information Spillage Response | Not Selected | | IR-9 (1) (2) (3) (4) | IR-9 (1) (2) (3) (4) |
| MA | Maintenance |  | |  |  |
| MA-1 | System Maintenance Policy and Procedures | MA-1 | | MA-1 | MA-1 |
| MA-2 | Controlled Maintenance | MA-2 | | MA-2 | MA-2 (2) |
| MA-3 | Maintenance Tools | Not Selected | | MA-3 (1) (2) (3) | MA-3 (1) (2) (3) |
| MA-4 | Nonlocal Maintenance | MA-4 | | MA-4 (2) | MA-4 (2) (3) (6) |
| MA-5 | Maintenance Personnel | MA-5 | | MA-5 (1) | MA-5 (1) |
| MA-6 | Timely Maintenance | Not Selected | | MA-6 | MA-6 |
| MP | Media Protection |  | |  |  |
| MP-1 | Media Protection Policy and Procedures | MP-1 | | MP-1 | MP-1 |
| MP-2 | Media Access | MP-2 | | MP-2 | MP-2 |
| MP-3 | Media Marking | Not Selected | | MP-3 | MP-3 |
| MP-4 | Media Storage | Not Selected | | MP-4 | MP-4 |
| MP-5 | Media Transport | Not Selected | | MP-5 (4) | MP-5 (4) |
| MP-6 | Media Sanitization | MP-6 | | MP-6 (2) | MP-6 (1) (2) (3) |
| MP-7 | Media Use | MP-7 | | MP-7 (1) | MP-7 (1) |
| PE | Physical and Environmental Protection | | |  |  |
| PE-1 | Physical and Environmental Protection Policy and Procedures | PE-1 | | PE-1 | PE-1 |
| PE-2 | Physical Access Authorizations | PE-2 | | PE-2 | PE-2 |
| PE-3 | Physical Access Control | PE-3 | | PE-3 | PE-3 (1) |
| PE-4 | Access Control For Transmission Medium | Not Selected | | PE-4 | PE-4 |
| PE-5 | Access Control For Output Devices | Not Selected | | PE-5 | PE-5 |
| PE-6 | Monitoring Physical Access | PE-6 | | PE-6 (1) | PE-6 (1) (4) |
| PE-8 | Visitor Access Records | PE-8 | | PE-8 | PE-8 (1) |
| PE-9 | Power Equipment and Cabling | Not Selected | | PE-9 | PE-9 |
| PE-10 | Emergency Shutoff | Not Selected | | PE-10 | PE-10 |
| PE-11 | Emergency Power | Not Selected | | PE-11 | PE-11 (1) |
| PE-12 | Emergency Lighting | PE-12 | | PE-12 | PE-12 |
| PE-13 | Fire Protection | PE-13 | | PE-13 (2) (3) | PE-13 (1) (2) (3) |
| PE-14 | Temperature and Humidity Controls | PE-14 | | PE-14 (2) | PE-14 (2) |
| PE-15 | Water Damage Protection | PE-15 | | PE-15 | PE-15 (1) |
| PE-16 | Delivery and Removal | PE-16 | | PE-16 | PE-16 |
| PE-17 | Alternate Work Site | Not Selected | | PE-17 | PE-17 |
| PE-18 | Location of Information System Components | Not Selected | | Not Selected | PE-18 |
| PL | Planning |  | |  |  |
| PL-1 | Security Planning Policy and Procedures | PL-1 | | PL-1 | PL-1 |
| PL-2 | System Security Plan | PL-2 | | PL-2 (3) | PL-2 (3) |
| PL-4 | Rules of Behavior | PL-4 | | PL-4 (1) | PL-4 (1) |
| PL-8 | Information Security Architecture | Not Selected | | PL-8 | PL-8 |
| PS | Personnel Security |  | |  |  |
| PS-1 | Personnel Security Policy and Procedures | PS-1 | | PS-1 | PS-1 |
| PS-2 | Position Risk Designation | PS-2 | | PS-2 | PS-2 |
| PS-3 | Personnel Screening | PS-3 | | PS-3 (3) | PS-3 (3) |
| PS-4 | Personnel Termination | PS-4 | | PS-4 | PS-4 (2) |
| PS-5 | Personnel Transfer | PS-5 | | PS-5 | PS-5 |
| PS-6 | Access Agreements | PS-6 | | PS-6 | PS-6 |
| PS-7 | Third-Party Personnel Security | PS-7 | | PS-7 | PS-7 |
| PS-8 | Personnel Sanctions | PS-8 | | PS-8 | PS-8 |
| RA | Risk Assessment |  | |  |  |
| RA-1 | Risk Assessment Policy and Procedures | RA-1 | | RA-1 | RA-1 |
| RA-2 | Security Categorization | RA-2 | | RA-2 | RA-2 |
| RA-3 | Risk Assessment | RA-3 | | RA-3 | RA-3 |
| RA-5 | Vulnerability Scanning | RA-5 | | RA-5 (1) (2) (3) (5) (6) (8) | RA-5 (1) (2) (3) (4) (5) (6) (8) (10) |
| SA | System and Services Acquisition |  | |  |  |
| SA-1 | System and Services Acquisition Policy and Procedures | SA-1 | | SA-1 | SA-1 |
| SA-2 | Allocation of Resources | SA-2 | | SA-2 | SA-2 |
| SA-3 | System Development Life Cycle | SA-3 | | SA-3 | SA-3 |
| SA-4 | Acquisition Process | SA-4 (10) | | SA-4 (1) (2) (8) (9) (10) | SA-4 (1) (2) (8) (9) (10) |
| SA-5 | Information System Documentation | SA-5 | | SA-5 | SA-5 |
| SA-8 | Security Engineering Principles | Not Selected | | SA-8 | SA-8 |
| SA-9 | External Information System Services | SA-9 | | SA-9 (1) (2) (4) (5) | SA-9 (1) (2) (4) (5) |
| SA-10 | Developer Configuration Management | Not Selected | | SA-10 (1) | SA-10 (1) |
| SA-11 | Developer Security Testing and Evaluation | Not Selected | | SA-11 (1) (2) (8) | SA-11 (1) (2) (8) |
| SA-12 | Supply Chain Protection | Not Selected | | Not Selected | SA-12 |
| SA-15 | Development Process, Standards and Tools | Not Selected | | Not Selected | SA-15 |
| SA-16 | Developer-Provided Training | Not Selected | | Not Selected | SA-16 |
| SA-17 | Developer Security Architecture and Design | Not Selected | | Not Selected | SA-17 |
| SC | System and Communications Protection | | |  |  |
| SC-1 | System and Communications Protection Policy and Procedures | | SC-1 | SC-1 | SC-1 |
| SC-2 | Application Partitioning | | Not Selected | SC-2 | SC-2 |
| SC-3 | Security Function Isolation | | Not Selected | Not Selected | SC-3 |
| SC-4 | Information In Shared Resources | | Not Selected | SC-4 | SC-4 |
| SC-5 | Denial of Service Protection | | SC-5 | SC-5 | SC-5 |
| SC-6 | Resource Availability | | Not Selected | SC-6 | SC-6 |
| SC-7 | Boundary Protection | | SC-7 | SC-7 (3) (4) (5) (7) (8) (12) (13) (18) | SC-7 (3) (4) (5) (7) (8) (10) (12) (13) (18) (20) (21) |
| SC-8 | Transmission Confidentiality and Integrity | | Not Selected | SC-8 (1) | SC-8 (1) |
| SC-10 | Network Disconnect | | Not Selected | SC-10 | SC-10 |
| SC-12 | Cryptographic Key Establishment and Management | | SC-12 | SC-12 (2) (3) | SC-12 (1) (2) (3) |
| SC-13 | Cryptographic Protection | | SC-13 | SC-13 | SC-13 |
| SC-15 | Collaborative Computing Devices | | SC-15 | SC-15 | SC-15 |
| SC-17 | Public Key Infrastructure Certificates | | Not Selected | SC-17 | SC-17 |
| SC-18 | Mobile Code | | Not Selected | SC-18 | SC-18 |
| SC-19 | Voice Over Internet Protocol | | Not Selected | SC-19 | SC-19 |
| SC-20 | Secure Name / Address Resolution Service (Authoritative Source) | | SC-20 | SC-20 | SC-20 |
| SC-21 | Secure Name / Address Resolution Service (Recursive or Caching Resolver) | | SC-21 | SC-21 | SC-21 |
| SC-22 | Architecture and Provisioning for Name / Address Resolution Service | | SC-22 | SC-22 | SC-22 |
| SC-23 | Session Authenticity | | Not Selected | SC-23 | SC-23 (1) |
| SC-24 | Fail in Known State | | Not Selected | Not Selected | SC-24 |
| SC-28 | Protection of Information At Rest | | Not Selected | SC-28 (1) | SC-28 (1) |
| SC-39 | Process Isolation | | SC-39 | SC-39 | SC-39 |
| SI | System and Information Integrity | |  |  |  |
| SI-1 | System and Information Integrity Policy and Procedures | | SI-1 | SI-1 | SI-1 |
| SI-2 | Flaw Remediation | | SI-2 | SI-2 (2) (3) | SI-2 (1) (2) (3) |
| SI-3 | Malicious Code Protection | | SI-3 | SI-3 (1) (2) (7) | SI-3 (1) (2) (7) |
| SI-4 | Information System Monitoring | | SI-4 | SI-4 (1) (2) (4) (5) (14) (16) (23) | SI-4 (1) (2) (4) (5) (11) (14) (16) (18) (19) (20) (22) (23) (24) |
| SI-5 | Security Alerts, Advisories and Directives | | SI-5 | SI-5 | SI-5 (1) |
| SI-6 | Security Function Verification | | Not Selected | SI-6 | SI-6 |
| SI-7 | Software, Firmware and Information Integrity | | Not Selected | SI-7 (1) (7) | SI-7 (1) (2) (5) (7) (14) |
| SI-8 | Spam Protection | | Not Selected | SI-8 (1) (2) | SI-8 (1) (2) |
| SI-10 | Information Input Validation | | Not Selected | SI-10 | SI-10 |
| SI-11 | Error Handling | | Not Selected | SI-11 | SI-11 |
| SI-12 | Information Handling and Retention | | SI-12 | SI-12 | SI-12 |
| SI-16 | Memory Protection | | SI-16 | SI-16 | SI-16 |

Note: The -1 Controls (AC-1, AU-1, SC-1, etc.) cannot be inherited and must be provided in some way by the service provider.

The definitions in Table 13‑2 Control Origination and Definitions indicate where each security control originates.

Table ‑ Control Origination and Definitions

| Control Origination | Definition | Example |
| --- | --- | --- |
| Service Provider Corporate | A control that originates from the 18F / GSA corporate network. | DNS from the corporate network provides address resolution services for the information system and the service offering. |
| Service Provider System Specific | A control specific to a particular system at the 18F / GSA and the control is not part of the standard corporate controls. | A unique host based intrusion detection system (HIDs) is available on the service offering platform but is not available on the corporate network. |
| Service Provider Hybrid | A control that makes use of both corporate controls and additional controls specific to a particular system at the 18F / GSA. | There are scans of the corporate network infrastructure; scans of databases and web based application are system specific. |
| Configured by Customer | A control where the customer needs to apply a configuration in order to meet the control requirement. | User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http\* or https, etc.), entering an IP range specific to their organization are configurable by the customer. |
| Provided by Customer | A control where the customer needs to provide additional hardware or software in order to meet the control requirement. | The customer provides a SAML SSO solution to implement two-factor authentication. |
| Shared | A control that is managed and implemented partially by the 18F / GSA and partially by the customer. | Security awareness training must be conducted by both the CSPN and the customer. |
| Inherited from pre-existing FedRAMP Authorization | A control that is inherited from another 18F / GSA system that has already received a FedRAMP Authorization. | A PaaS or SaaS provider inherits PE controls from an IaaS provider. |

\*Hyper Text Transport Protocol (http)

Responsible Role indicates the role of CSP employee who can best respond to questions about the particular control that is described.

## Access Control (AC)

### AC-1 Access Control Policy and Procedures Requirements (L) (M)

The organization:

1. Develops, documents and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
2. Reviews and updates the current:
   1. Access control policy [FedRAMP Assignment: at least every 3 years]; and
   2. Access control procedures [FedRAMP Assignment: at least annually].

| AC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter AC-1(a): cloud.gov development and design team | |
| Parameter AC-1(b)(1): at least every 3 years | |
| Parameter AC-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/AC-Policy.md> for the Access Control procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b1 | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.” |
| Part b2 | The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### AC-2 Account Management (L) (M)

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];
2. Assigns account managers for information system accounts;
3. Establishes conditions for group and role membership;
4. 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;
5. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
6. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
7. Monitors the use of information system accounts;
8. 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;
9. 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;
10. Reviews accounts for compliance with account management requirements [FedRAMP Assignment: at least annually]; and
11. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

| AC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations, GSA Information Security | |
| Parameter AC-2(a): User and System account types | |
| Parameter AC-2(e): System Owner, Program Manager | |
| Parameter AC-2(f): 18F Access Control Policy | |
| Parameter AC-2(j): Continuous | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | ***Table 9-1 User Roles and Privileges*** identifies the user and system account types for cloud.gov. |
| Part b | The System Owner determines which team members who should have the Cloud Operations role and be considered part of the Cloud Operations team. The System Owner designates the Cloud Operations role as the account managers for all information system accounts in AWS and cloud.gov. Cloud Operations team members do not manage their own accounts; the System Owner or a different member of Cloud Operations manages their accounts.  “Cloud Operations” is both the name of the role and the name of the sub-team that has this role.  GSA IT has oversight of and visibility into cloud.gov operations; since the System Owner and Cloud Operations log into cloud.gov using accounts and systems under GSA control (see part c), GSA Information Security can also terminate their access if necessary.  **Customer Responsibility**  External Application System Owners, whose applications reside on the cloud.gov platform, have the responsibility to assign personnel to all the roles labeled as “external” in the ***Table 9-1 User Roles and Privileges*** and are responsible for *all* subsequent elements of AC-1, except where noted. |
| Part c | Cloud Operations is granted access to AWS and cloud.gov if:   1. User has passed all pre-requisites, background checks, and biometric collections necessary for a position of "Public Trust" at GSA. This is inclusive of all requirements necessary to receive a Personal Identity Verification (PIV) Credential that is in compliance with the Homeland Security Presidential Directive 12 (HSPD-12) via the USAccess Program ( <http://fedidcard.gov/> ), itself a program run by GSA. 2. Contingent on the above, user has been entered into the GSA Credential and Identity Management System (GCIMS), per the approval of the GSA Office of Mission Assurance (OMA) Identity, Credential and Access Management (ICAM) Division. 3. Contingent on the above, user has received final approval in GCIMS and has received a username, password, and multi-factor authentication token (per system) to access GSA SecureAuth. 4. User has completed all necessary training in GSA's Online Learning University (OLU) as required by AC-1. 5. User's 18F Supervisor has assigned the user to a technical internal role through 18F staffing processes, or an 18F Contracting Officer Representative (COR) has assigned a contractor to a technical internal role.   cloud.gov development and design team members (without the Cloud Operations role) are granted limited non-administrative access as described in ***Table 9-1 User Roles and Privileges.*** They must also pass items a) through d), and they must be assigned to the cloud.gov team through 18F’s staffing processes by their 18F Supervisor. |
| Part d | See ***Table 9-1 User Roles and Privileges****.* |
| Part e | See ***Table 9-1 User Roles and Privileges***.  18F Supervisors assign staff to cloud.gov. Internal staff then follow the instructions in the onboarding checklist template ( <https://github.com/18F/cg-product/blob/master/OnboardingChecklist.md> ). |
| Part f | The conditions for the creation and enablement of system accounts is upon entrance to GSA, 18F, and the cloud.gov team respectively. The On-boarding Checklist linked above contains the relevant procedures. Conversely, the Off-boarding Checklist ( <https://github.com/18F/cg-product/blob/master/OffboardingChecklist.md> ) is used if system accounts need to be modified, disabled, or removed. |
| Part g | Cloud Operations and GSA Information Security use the following tools to monitor information system accounts.  **AWS**  AWS CloudTrail captures all IAM API calls from command-line tools, the AWS SDK, and the AWS Management Console. Monitoring data is retained for two weeks, even if AWS resources have been terminated.  **cloud.gov**  The UAA API is used to monitor all roles. The API returns information about each user account, including the user’s universally unique identifier (UUID), given name, permission groups, activity status, and other metadata.  ELK collects and visualizes all UAA logs along with the logs of other components at <https://logs.fr.cloud.gov>. |
| Part h | 18F Supervisors are ultimately responsible for notifying, or ensuring that Cloud Operations is notified, regarding transfers, reassignments, terminations, need-to-know, or clearance changes. 18F Supervisors notify Cloud Operations via an approved GSA communication method, such as GSA Gmail or 18F Slack. |
| Part i | The origination of all permissions starts with the System Owner, and the System Owner delegates it by granting staff the Cloud Operations role. From there, Cloud Operations and the other internal roles work together to ensure that all information is collected from all user roles to create system accounts. See parts (c), (f), and the ***Table 9-1 User Roles and Privileges***for details*.* |
| Part j | **AWS**  AWS automatically provides *continuous* review of AWS IAM compliance, including if AWS IAM API access keys are exposed, if MFA is enabled, and if password content requirements are enabled.  **cloud.gov**  Accounts are managed by GSA SecureAuth. GSA Information Security is responsible for *continuous* monitoring of all accounts. |
| Part k | AWS or cloud.gov have no shared or group account credentials. |

#### AC-2 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to support the management of information system accounts.

| AC-2(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-2 (1) What is the solution and how is it implemented? |
| --- |
| **AWS**  IAM automatically deactivates account via automatic password expiration every 90 days. All account creations, modifications, and deletions are automatically recorded by CloudTrail.  **cloud.gov**  UAA Servers have their passwords reset every 90 days, implemented via automation in GSA SecureAuth. The deletion of a GSA SecureAuth account deactivates user access across all integrations. |

#### AC-2 (2) Control Enhancement (M)

The information system automatically [Selection: removes; disables] temporary and emergency accounts after [FedRAMP Assignment: no more than 30 days for temporary and emergency account types].

| AC-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AC-2(2)1: Not Applicable: cloud.gov does not possess temporary accounts | |
| Parameter AC-2(2)2: Not Applicable: cloud.gov does not possess temporary accounts | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-2 (2) What is the solution and how is it implemented? |
| --- |
| Not applicable. cloud.gov does not contain any guest/anonymous, group, or temporary user accounts. Cloud Operations team members only create individual user accounts and grant role-based access to users within cloud.gov. There are no guest/anonymous, group, or temporary user accounts in the cloud.gov virtual environment. |

#### AC-2 (3) Control Enhancement (M)

The information system automatically disables inactive accounts after [FedRAMP Assignment: ninety (90) days for user accounts].

AC-2 (3) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the Joint Authorization Board (JAB)/AO. Where user management is a function of the service, reports of activity of consumer users shall be made available.

|  |  |
| --- | --- |
| AC-2 (3) | Control Enhancement Summary Information |
| Responsible Role: Cloud Operations | |
| Parameter AC-2(3): ninety (90) days for user accounts | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-2 (3) What is the solution and how is it implemented |
| --- |
| **AWS**  AWS account passwords are configured to expire after 60 days, thereby disabling access.  **cloud.gov**  The UAA servers integrate with GSA SecureAuth, whose accounts are configured to deactivate inactive accounts every 90 days via password expiration.  **cloud.gov fallback identity provider**  Passwords expire after 90 days, which automatically disables inactive accounts.  **Customer Responsibility**  Customers using cloud.gov for application development are responsible for monitoring inactive user accounts created within their cloud.gov Org.  For customers who do not use the cloud.gov fallback identity provider, cloud.gov delegates authentication to customer enterprise identity systems. Therefore, customers are responsible for monitoring inactive user accounts. |

#### AC-2 (4) Control Enhancement (M)

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].

| AC-2 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO), System Owner | |
| Parameter AC-2(4): Cloud Operations, Information Systems Security Officer (ISSO), System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-2 (4) What is the solution and how is it implemented? |
| --- |
| cloud.gov automatically audits account creation, modification, enabling, disabling, and removal actions. cloud.gov provides notifications on demand to Cloud Operations, GSA Information Security, ISSOs, and the System Owner.  **AWS**  CloudTrail captures and audits all actions in regard to information system accounts in AWS IAM.  **cloud.gov**  GSA SecureAuth is responsible for notifying GSA Information Security regarding all actions taken on accounts. Once authenticated to cloud.gov UAA servers through GSA SecureAuth, all account activity is logged and fed into the Prometheus event processor. |

#### AC-2 (5) Control Enhancement (M)

The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out].

AC-2 (5) Additional FedRAMP Requirements and Guidance:

Guidance: Should use a shorter timeframe than AC-12

| AC-2 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AC-2(5): Not applicable to AWS; 15 minutes for Operations UAA Server; 15 minutes for Client UAA Server | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-2 (5) What is the solution and how is it implemented? |
| --- |
| **AWS**  AWS user sessions automatically terminate after 12 hours of inactivity ( <https://aws.amazon.com/console/faqs/> ).  **cloud.gov**  Sessions to the Operations UAA Server last for 15 minutes before they terminate due to inactivity.  Sessions to the Client UAA Server last for 15 minutes before they terminate due to inactivity.  **cloud.gov fallback identity provider**  IDP users are covered by the Client UAA 15 minute timeout.  **Customer Responsibility**  cloud.gov delegates authentication to customer enterprise identity systems. Those systems determine how long the period of inactivity can last before the session is terminated. |

#### AC-2 (7) Control Enhancement (M)

The organization:

1. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
2. Monitors privileged role assignments; and
3. Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate.

| AC-2 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter AC-2(7)(c): removes users from privileged access rights | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-2 (7) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Owner and Cloud Operations are the only roles who are allowed to perform security-relevant functions. See ***Table 9-1 User Roles and Privileges***for details. |
| Part b | All information system accounts are fully monitored, regardless of privilege. See AC-2 part g for details. |
| Part c | The System Owner or Cloud Operations removes users from privileged access rights when privileged role assignments are no longer appropriate due to project transfer or agency off-boarding.  In the case of project transfer, the user’s 18F Supervisor is responsible for notifying the System Owner and Cloud Operations of the necessary change. In the case of a user leaving GSA, the 18F Talent team initiates the enterprise off-boarding checklist, which notifies the System Owner to start the cloud.gov Off-boarding Checklist ( <https://github.com/18F/cg-product/blob/master/OffboardingChecklist.md> ). |

#### AC-2 (9) Control Enhancement (M)

The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for establishing shared/group accounts].

AC-2 (9) Additional FedRAMP Requirements and Guidance: Required if shared/group accounts are deployed.

| AC-2 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AC-2(9): Group Accounts are not allowed | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-2 (9) What is the solution and how is it implemented? |
| --- |
| 18F does not allow group or shared accounts in AWS or cloud.gov.  **cloud.gov fallback identity provider**  IDP users have a Rule of Behavior that does not permit shared/group accounts (<https://cloud.gov/docs/getting-started/accounts/#use-your-account-responsibly>): “Don’t share your account with another person or create anonymous or group accounts. Your account is just for you.”  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, customers access cloud.gov using their enterprise identity accounts. It is the customer’s responsibility to restrict use of shared/group enterprise identity accounts.  It is the customer’s responsibility to restrict the use of shared or group access to their Orgs, Spaces, and applications. |

#### AC-2 (10) Control Enhancement (M) (H)

The information system terminates shared/group account credentials when members leave the group.

AC-2 (10) Additional FedRAMP Requirements and Guidance: Required if shared/group accounts are deployed.

| AC-2 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-2 (10) What is the solution and how is it implemented? |
| --- |
| 18F does not allow group or shared accounts in AWS or cloud.gov.  **cloud.gov fallback identity provider**  Not applicable to the IDP because it does not allow shared/group accounts.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, customers access cloud.gov using their enterprise identity accounts. It is the customer’s responsibility to appropriately terminate use of shared/group enterprise identity accounts.  It is the customer’s responsibility to appropriately terminate shared or group access to their Orgs, Spaces, and applications. |

#### AC-2 (12) Control Enhancement (M)

The organization:

1. Monitors information system accounts for [Assignment: organization-defined atypical use]; and
2. Reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles].

AC-2 (12) (a) and AC-2 (12) (b) Additional FedRAMP Requirements and Guidance: Required for privileged accounts.

| AC-2 (12) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Parameter AC-2(12)(a): atypical use | |
| Parameter AC-2(12)(b): Cloud Operations, System Owner, Program Manager, Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM), Authorizing Official | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-2 (12) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Cloud Operations and ISSOs actively monitor information system accounts related to cloud.gov for suspicious activities, atypical usage, and unused or expired accounts.  The Cloud Operations team has implemented continuous (1 hour intervals) monitoring of key metrics that are indicators of atypical usage. These metrics are:   * Unknown users attempting to authenticate * Authentication failures for known users * Number of password changes * HTTP 4xx and 5xx responses from key Cloud Foundry components * Number of applications / workloads running on the system   For each of these metrics, the cloud.gov monitoring system computes a baseline based on historical system activity in Prometheus and raises alerts to the Cloud Operations team (via PagerDuty) when any metric exceeds 1.5 standard deviations from the mean, calculated over the preceding two weeks.  Additionally, we track all key metrics on a single unified dashboard in Grafana.  18F reduces potential risk of atypical or suspicious usage by enforcing that all changes must be under distributed version control. The system also keeps detailed logs that support after-the-fact investigations and audits. |
| Part b | All reports of suspicious activities and atypical usage of information system accounts are sent to the Cloud Operations team via PagerDuty.  Cloud Operations escalates when necessary to System Owner, Program Manager, Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM), and Authorizing Official, as guided by the cloud.gov Incident Response Guide ( <https://cloud.gov/docs/ops/security-ir/> ). |

### AC-3 Access Enforcement (L) (M) (H)

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

| AC-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-3 What is the solution and how is it implemented? |
| --- |
| **AWS**  Access is enforced through the use of AWS IAM policies, where IAM administrators specify the actions that are permitted and the AWS resource that can be acted upon. Access is impossible without a valid AWS IAM username, password, and multifactor authenticator or without valid AWS IAM public and secret API Keys.  **cloud.gov**  cloud.gov team access requires the use of GSA SecureAuth. Without an active GSA SecureAuth session, access to either the Client UAA server or Operations UAA Server is impossible. |

### AC-4 Information Flow Enforcement (M) (H)

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].

| AC-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AC-4: 18F Access Control Policy | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-4 What is the solution and how is it implemented? |
| --- |
| **AWS**   1. cloud.gov incorporates security features within its VPC such as AWS Identity and Access Management (IAM) security groups, network Access Control Lists (ACLs), routing tables, and external gateways. Each of these items is complementary to providing a secure, isolated network. 2. Network Access Control Lists (ACLs) are created to allow or deny traffic entering or exiting these subnets. Each subnet has routing tables attached to them to direct the flow of network traffic to Internet gateways, virtual private gateways, and Network Address Translation (NAT) for private subnets. 3. The Virtual Private Cloud infrastructure has firewalls enabling filtering on both ingress and egress traffic from its instances. The default group enables inbound communication from other members of the same group and outbound communication to any destination. 4. Traffic is restricted by IP protocol, by service port, as well as source/destination IP address (individual IP or Classless Inter-Domain Routing (CIDR) block). For a list of ports allowable for inbound connections and within the system, see section 10.8. (*Ports, Protocols, and Services*). 5. As described in SC-12, [cloud.gov](http://cloud.gov) uses TLS encryption for public connections and some internal connections (other internal connections are protected by firewalls described above). For additional details about encryption used to transmit data externally and at key internal boundaries, see details in SC-7 part a about HTTPS.   **Cloud Foundry Application Security Groups (ASGs)**   1. cloud.gov enforces security groups and other network traffic rules in a strict priority order. It returns an allow, deny, or reject result for the first rule that matches the outbound traffic request parameters, and does not evaluate any lower-priority rules. See <https://docs.cloudfoundry.org/concepts/security.html#network-traffic> for additional details. 2. cloud.gov implements network traffic rules using Linux iptables on the component VMs. Cloud Operations configures rules to prevent system access from external networks and between internal components, and to restrict applications from establishing connections over the cell network interface. cloud.gov Application Security Groups (ASGs) consist of a list of access rules to control application outbound traffic. 3. Cell network properties allow Cloud Operations to configure the *allow\_networks* and *deny\_networks* parameters to prohibit communication between system components and applications.   **Customer Applications**  Client hosted applications and websites on cloud.gov inherit all information flow enforcement functions from the cloud.gov platform. When an app instance starts, an IP address and an arbitrary port is assigned to the Application Container. The application uses the PORT environment variable provided in the container environment to determine which port to listen on. Because Cells are assigned a random value to the PORT environment variable, the value is generally unique for each application instance. The cloud.gov routers handle all inbound traffic to applications, routing traffic to one of the application instances.  All incoming traffic to customer applications is encrypted with TLS. |

#### AC-4 (21) Control Enhancement (M) (H)

The information system separates information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].

| AC-4 (21) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AC-4(21)-1: security groups, routers, and containers | |
| Parameter AC-4(21)-2: separation of public vs. nonpublic information, and information between customers | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-4 (21) What is the solution and how is it implemented? |
| --- |
| cloud.gov separates information flows logically using software firewalls, restricted port access, and application security groups. The Virtual Private Cloud logically separates the cloud.gov PaaS from other information systems within its environment. cloud.gov is hosted within its own VPC and has its own dedicated Elastic Load Balancers for incoming traffic.  cloud.gov application security groups act as virtual firewalls to control outbound traffic from the applications in deployment. cloud.gov evaluates security groups and other network traffic rules in a strict priority order. Cloud Foundry returns an allow, deny, or reject result for the first rule that matches the outbound traffic request parameters, and does not evaluate any lower-priority rules. Cloud Foundry evaluates the network traffic rules for an application in the following order:   1. Security Groups: The rules described by the Default Staging set, the Default Running set, and all security groups bound to the space. 2. Garden ALLOW rules: Any Garden Cell configuration `allow` rules. Set Garden Cell configuration rules in the Cell configuration section of your deployment manifest. 3. Garden DENY rules: Any Garden Cell configuration `deny` rules. Set Garden Cell configuration rules in the configuration section of your deployment manifest. 4. Hard-coded REJECT rule: Cloud Foundry returns a `reject` result for all outbound traffic from a container if not allowed by a higher-priority rule.   For details about allowable ports for connections and encryption for internal and external connections, see AC-4 under “AWS”. |

### AC-5 Separation of Duties (M) (H)

The organization:

1. Separates [Assignment: organization-defined duties of individuals];
2. Documents separation of duties of individuals; and
3. Defines information system access authorizations to support separation of duties.

AC-5 Additional FedRAMP Requirements and Guidance:

Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP. Directions for attaching the Separation of Duties Matrix document may be found in Section 15.11 ATTACHMENT 11 - Separation of Duties Matrix.

| AC-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Program Manager | |
| Parameter AC-5(a): Duties as listed in ***Table 9-1 User Roles and Privileges*** | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | See ***Table 9-1 User Roles and Privileges*** for additional information.  **AWS**  Cloud Operations implements (IAM) Policies roles and individual user accounts for separation of duties at the AWS layer.  **cloud.gov**  cloud.gov uses UAA role-based access controls to maintain separation of duties.  **Customer Responsibility**  Application System Owners have the ability to assign roles in their cloud.gov Orgs and Spaces with granular levels of access, such as Org Manager and Space Developer. Application System Owners are responsible for appropriately assigning these roles. |
| Part b | See ***Table 9-1 User Roles and Privileges*** for documentation on the separations between roles. |
| Part c | See ***Table 9-1 User Roles and Privileges*** for documentation that supports different duties and roles. |

### AC-6 Least Privilege (M) (H)

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 Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-6 What is the solution and how is it implemented? |
| --- |
| **AWS**  The only roles with privileged access to AWS are the System Owner and Cloud Operations.  **cloud.gov**  The only roles with privileged access to cloud.gov are the System Owner and Cloud Operations.  **Customer Responsibility**  Customers are responsible for employing the principle of least privilege for access to privileged roles within their orgs, spaces, and applications (such as Org Manager and Space Developer). |

#### AC-6 (1) Control Enhancement (M)

The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].

| AC-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Program Manager, Information Systems Security Officer (ISSO) | |
| Parameter AC-6(1): security-related administrative functions | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-6 (1) What is the solution and how is it implemented? |
| --- |
| Refer to ***Table 9-1 User Roles and Privileges*** fordetails. Also see AC-2 for details on explicit authorization.  **Customer Responsibility**  Customers are not granted privileged access to cloud.gov or AWS. Customers are explicitly responsible for managing security-related administrative access within their own Orgs. The System Owner, Program Manager, or a Cloud Operations team member explicitly grants Org Manager roles to appropriate customers on their respective cloud.gov Orgs, which permits them to create and modify applications on cloud.gov, and to authorize access to users within their Orgs. |

#### AC-6 (2) Control Enhancement (M) (H)

The organization requires that users of information system accounts, or roles, with access to [FedRAMP Assignment: all security functions], use non-privileged accounts or roles, when accessing non-security functions.

AC-6 (2) Additional FedRAMP Requirements and Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.

| AC-6 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations, Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO) | |
| Parameter AC-6(2): all security functions | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for 6/21/2016 , | |

| AC-6 (2) What is the solution and how is it implemented? |
| --- |
| All actions (including security functions) carried out by Cloud Operations staff use accounts with minimum necessary privilege.  For example, automated deployments that require read access to AWS S3 use specific AWS IAM permissions that can read (but not write) to AWS S3. |

#### AC 6 (5) Control Enhancement (M) (H)

The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].

| AC-6 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations, Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM), Authorizing Official | |
| Parameter AC-6 (5): Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-6 (5) What is the solution and how is it implemented? |
| --- |
| The System Owner restricts privileged accounts such as administrator and root access accounts to Cloud Operations. |

#### AC-6 (9) Control Enhancement (M) (H)

The information system audits the execution of privileged functions.

| AC-6 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-6 (9) What is the solution and how is it implemented? |
| --- |
| All AWS and cloud.gov logging activity, regardless of the privilege used to take an action, is automatically collected and forwarded to Prometheus. These logs are kept to support after-the-fact investigations. |

#### AC-6 (10) Control Enhancement (M) (H)

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

| AC-6 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM), System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-6 (10) What is the solution and how is it implemented? |
| --- |
| All privileged actions must either have an AWS IAM credential or a GSA SecureAuth credential bound to the Operations UAA Server, in order to be accepted by AWS or cloud.gov. As a result, no users other than those with System Owner or Cloud Operations roles (who are given these credentials) can execute privileged functions. |

### AC-7 Unsuccessful Login Attempts (L) (M)

The organization:

1. Enforces a limit of [FedRAMP Assignment: not more than three (3)] consecutive invalid logon attempts by a user during a [FedRAMP Assignment: fifteen (15) minutes]; and
2. Automatically [Selection: locks the account/node for a [FedRAMP Assignment: thirty (30) minutes]; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

| AC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM) | |
| Parameter AC-7(a)-1: not more than three | |
| Parameter AC-7(a)-2: fifteen minutes | |
| Parameter AC-7(b)-1: locks the account for 30 minutes or until released by an administrator | |
| Parameter AC-7(b)-2: for 15 minutes | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **AWS**  See the Provisional Authorization for AWS GovCloud.  **cloud.gov**  GSA SecureAuth limits attempts to five login attempts per a 30-minute window.  **cloud.gov fallback identity provider**  The IDP enforces a limit of 3 consecutive invalid logon attempts by a user during 15 minutes.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, user management is delegated to each agency’s enterprise user management system. cloud.gov is not responsible for enforcing a limit on consecutive invalid login attempts. |
| Part b | **AWS**  See the Provisional Authorization for AWS GovCloud.  **cloud.gov**  After exceeding the limit on failed login attempts, users are prevented from logging in for 30 minutes or until an administrator manually ends the lockout period. The 30-minute timeout is the alternative implementation for this requirement.  **cloud.gov fallback identity provider**  When that limit is reached, the IDP automatically locks the account for 30 minutes and delays the next logon prompt for at least 15 minutes for each additional unsuccessful attempt.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, user management is delegated to each agency’s enterprise user management system. cloud.gov is not responsible for automatically locking these accounts. |

### AC-8 System Use Notification (L) (M) (H)

The information system:

1. Displays to users [Assignment: organization-defined system use notification message or banner (FedRAMP Assignment: see additional Requirements and Guidance)] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
   1. Users are accessing a U.S. Government information system;
   2. Information system usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
   4. Use of the information system indicates consent to monitoring and recording;
2. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
3. For publicly accessible systems:
   1. Displays system use information [Assignment: organization-defined conditions (FedRAMP Assignment: see additional Requirements and Guidance)], before granting further access;
   2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. Includes a description of the authorized uses of the system.

AC-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO.

Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

| AC-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Parameter AC-8(a): system use notification on login screen | |
| Parameter AC-8(c)-1: on login screen | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **cloud.gov**  UAA Servers display system use notifications to users (both internal and external) before they can log in.  The notification reads:  “This is a U.S. government service. Your use indicates your consent to monitoring, recording, and no expectation of privacy. Misuse is subject to criminal and civil penalties.”  It also provides a “Read more details” link that explains these warnings, including that this is a government system for official use only, all use is monitored and recorded, use indicates consent to monitoring and recording, and unauthorized use is prohibited.  This system use notification is visible at <https://login.fr.cloud.gov/login> |
| Part b | cloud.gov retains the system use notification (the summary of notices and a link to more details) until the user actively acknowledges and consents to the usage conditions by clicking the “Agree and continue” button. Then the user may log into their cloud.gov account. |
| Part c | Along with displaying privacy and security notices, this system use notification includes a description of the authorized uses of the system, available under the “Read more details” link. This description is viewable by the public (since this system use notification displays before login).  A description of authorized uses of the system is also available to any member of the public by directly viewing the cloud.gov documentation page about cloud.gov accounts: <https://cloud.gov/docs/getting-started/accounts/> |

Additional FedRAMP Requirements and Guidance

Requirement 1: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement 2: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO. If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement 3: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

| AC-8 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, System Owner, Information Systems Security Officer (ISSO), Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | The system use notification is exclusively provided on UAA Server endpoints. |
| Req. 2 | The periodicity of the check is quarterly. The verification process is manual, via a check by the ISSO of the UAA Server endpoints. |
| Req. 3 | See Requirement 2 above. This will be performed as part of any Configuration Baseline check. |

### AC-10 Concurrent Session Control (M) (H)

The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [FedRAMP Assignment: three (3) sessions for privileged access and two (2) sessions for non-privileged access].

| AC-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AC-10-1: Client UAA refresh token | |
| Parameter AC-10-2: 1 refresh token | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-10 What is the solution and how is it implemented? |
| --- |
| **AWS**  AWS does not limit concurrent sessions. As compensation, AWS notifies users of atypical login patterns.  **cloud.gov Client UAA**  Client UAA has unique refresh tokens, which means that logging in invalidates all existing authentication sessions. A refresh token enables the customer to receive authentication tokens for each individual application they log into, such as the cloud.gov dashboard or log management system.  This means that customers may have multiple concurrent authentication tokens for applications, but they can only have one refresh token. This is an alternative control for limiting concurrent sessions.  Client UAA controls the sessions for customers logged in via both the cloud.gov fallback identity provider and via customer enterprise user management systems.  **cloud.gov Operations UAA**  Operations UAA cannot have unique refresh tokens because this would break concurrent Concourse Continuous Integration jobs, which are required for the functioning of the system. |

### AC-11 Session Lock (M) (H)

The information system:

1. Prevents further access to the system by initiating a session lock after [FedRAMP Assignment: fifteen (15) minutes] of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

| AC-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AC-11(a): 15 Minutes | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **AWS**  AWS does not use session locks. AWS uses session terminations instead. Sessions terminate after 12 hours of inactivity ( <https://aws.amazon.com/console/faqs/> ).  **cloud.gov**  cloud.gov does not use session locks. The Client UAA Server terminates sessions after 15 minutes of inactivity. The Operations UAA Server terminates sessions after 15 minutes of inactivity. |
| Part b | Not applicable. As mentioned in Part a, sessions are not locked, but rather terminated completely. |

#### AC-11 (1) Control Enhancement (M) (H)

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

| AC-11 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-11 (1) What is the solution and how is it implemented? |
| --- |
| **AWS**  AWS does not use session locks. AWS uses session terminations instead. Sessions terminate after 12 hours of inactivity ( <https://aws.amazon.com/console/faqs/> ).  **cloud.gov**  cloud.gov does not use session locks. The Client UAA Server terminates sessions after 15 minutes of inactivity. The Operations UAA Server terminates sessions after 15 minutes of inactivity. |

### AC-12 Session Termination (M) (H)

The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

| AC-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AC-12: after 12 hours of inactivity; after 20 minutes of inactivity | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-12 What is the solution and how is it implemented? |
| --- |
| **AWS**  Sessions terminate after 12 hours of inactivity ( <https://aws.amazon.com/console/faqs/> ).  **cloud.gov**  The Client UAA Server terminates sessions after 15 minutes of inactivity. The Operations UAA Server terminates sessions after 15 minutes of inactivity. |

### AC-14 Permitted Actions without Identification or Authentication (L) (M) (H)

The organization:

1. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
2. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

| AC-14 | Control Summary Information |
| --- | --- |
| Responsible Role: Authorizing Official, Cloud Operations, System Owner, Information Systems Security Officer (ISSO) | |
| Parameter AC-14(a): public web page requests, requesting an email to create a user account | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The only actions that that can be taken without authentication or authorization are:   * Public web page requests, such as viewing <https://cloud.gov> or cloud.gov code repositories in GitHub * Requesting an email to create a user account (restricted to people with federal email addresses only)   All actions requiring authentication or authorization are listed in **Table 9-1 User Roles and Privileges**. |
| Part b | Supporting rationales:   * Viewing public web pages without authentication or authorization has no effect on the confidentiality, integrity, or availability of AWS or cloud.gov. * Requesting an email to create a user account has no effect on the confidentiality, integrity, or availability of AWS or cloud.gov.   The Authorizing Official accepts the rationale in this control by putting the system into operation via an Authority to Operate (ATO). |

### AC-17 Remote Access (L) (M) (H)

The organization:

1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
2. Authorizes remote access to the information system prior to allowing such connections.

| AC-17 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | AWS and cloud.gov enforce HTTPS connections for all remote access. No information is allowed to be transmitted unencrypted to or from these systems. All HTTPS endpoints must receive an “A” rating or higher from Qualys SSL Labs Server Test ( <https://www.ssllabs.com/ssltest/> ) before being used or put into production.  Any change to endpoint HTTPS configurations under 18F control must result in retesting the configuration via the Qualys SSL Labs Server Test. |
| Part b | Since everything in the information system is completely virtualized, all remote access is inherently authorized and approved. Section 10.1 (*Tooling Private Subnets*) describes how the Cloud Operations team authenticates for remote connections. |

#### AC-17 (1) Control Enhancement (M) (H)

The information system monitors and controls remote access methods.

| AC-17 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM), Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-17 (1) What is the solution and how is it implemented? |
| --- |
| Since all access is remote, see AC-2 (4) for details. |

#### AC-17 (2) Control Enhancement (M) (H)

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

| AC-17 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-17 (2) What is the solution and how is it implemented? |
| --- |
| All HTTPS endpoints must receive an “A” rating or higher from Qualys SSL Labs Server Test ( <https://www.ssllabs.com/ssltest/> ). before being used or put into production. Any change to endpoint HTTPS configurations under 18F control must result in retesting the configuration via the Qualys SSL Labs Server Test. |

#### AC-17 (3) Control Enhancement (M) (H)

The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points.

| AC-17 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Parameter AC-17(3): one | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-17 (3) What is the solution and how is it implemented? |
| --- |
| All remote access passes through virtual AWS internet gateways, whose configuration is controlled by Cloud Operations, and are instantiated through continuous integration and deployment tasks via Concourse. |

#### AC-17 (4) Control Enhancement (M) (H)

The organization:

1. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and
2. Documents the rationale for such access in the security plan for the information system.

| AC-17 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, System Owner, Information Systems Security Officer (ISSO) | |
| Parameter AC-17(4)(a): monitoring, managing, and troubleshooting | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-17 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Since the system is entirely virtualized, all access is remote. Therefore, there are no specific authorizations for this control, beyond those already found elsewhere. |
| Part b | Since the system is entirely virtualized, all access is remote. Therefore, there are no specific authorizations for this control, beyond those already found elsewhere. |

#### AC-17 (9) Control Enhancement (M) (H)

The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [FedRAMP Assignment: fifteen (15) minutes].

| AC-17 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations, Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM) | |
| Parameter AC-17(9): nearly instant (within 1 minute) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-17 (9) What is the solution and how is it implemented? |
| --- |
| Since all access must pass through virtual AWS internet gateways, remote access to the system can be immediately disconnected nearly instantaneously through multiple mechanisms. Either AWS internet gateway can be deleted completely, or the AWS security group can simply be set to deny connections to all ports. The timeline to implement either change is only limited by the latency of the network speed between AWS and the Cloud Operations staff issuing the command, and the system latency within AWS itself to fully execute the command. |

### AC-18 Wireless Access Restrictions (L) (M) (H)

The organization:

1. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
2. Authorizes wireless access to the information system prior to allowing such connections.

| AC-18 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Since cloud.gov is completely virtualized within AWS, there are no wireless capabilities possible, as all access to AWS is over Ethernet connections to AWS datacenters. |
| Part b | No authorization is necessary or applicable; see part a above. |

#### AC-18 (1) Control Enhancement (M) (H)

The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.

| AC-18 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Parameter AC-18 (1): Not Applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-18 (1) What is the solution and how is it implemented? |
| --- |
| Not applicable. See AC-18 for details. |

### AC-19 Access Control for Portable and Mobile Systems (L) (M) (H)

The organization:

1. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
2. Authorizes the connection of mobile devices to organizational information systems.

| AC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | GSA mobile devices are managed at the enterprise level, through software like MaaS360. However, since mobile devices enjoy no special or privileged access to either AWS or cloud.gov, mobile device controls and configurations are outside the scope and boundary of this authorization.  In order to access AWS or cloud.gov, mobile devices must connect through a mobile client or web browser (such as Safari on an iPhone) in the same fashion as other computing devices, such as laptops. GSA mobile devices do not possess any special HTTPS certificates or other types of keys or authenticators.  Therefore, all relevant controls are the same. |
| Part b | Since all controls are only relevant in the context of a client or web browser, no additional authorizations are necessary before connections are made. |

#### AC-19 (5) Control Enhancement (M) (H)

The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

| AC-19 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Parameter AC-19(5)-1: full-device disk encryption | |
| Parameter AC-19(5)-2: all mobile devices | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-19 (5) What is the solution and how is it implemented? |
| --- |
| It is both GSA and 18F policy to use disk encryption everywhere, at minimum. All devices are encrypted, either using the native encryption of iOS for iPhones, or FileVault 2 for GSA Apple laptops. |

### AC-20 Use of External Information Systems (L) (M) (H)

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

1. Access the information system from external information systems; and
2. Process, store, or transmit organization-controlled information using external information systems.

| AC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: Authorizing Official, System Owner, Cloud Operations, GSA Office of the General Counsel (OGC), GSA Information Security | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | As a federal agency, GSA follows all necessary laws, regulations, policies and Executive Orders in executing terms and conditions with any second or third-party to GSA and 18F, whether the other organization is another federal agency or not. This is controlled at the enterprise level, which also reflects GSA’s overall role in defining procurement and agreement procedures for the entire federal government. Each term or condition is specific to the external service being used. Appropriate staff in GSA Information Security or the GSA Office of the General Counsel (OGC) are consulted where appropriate, before accepting an inter-agency agreement or awarding a contract.  The only individuals authorized to access these non-sensitive components of the information system via external services are the System Owner and Cloud Operations. All access is either governed by “read-only” AWS IAM policies or other public API endpoints via cloud.gov, using an authentication mechanism like API keys.  The Authorizing Official must always expressly accept the risk of all external services that can access 18F’s production AWS account and production cloud.gov environment(s).  See the attachment ***Services Table*** for a comprehensive listing of external services. |
| Part b | See above. Specifically, consult the ***Services Table*** for a listing of what each external service does. |

#### AC-20 (1) Control Enhancement (M) (H)

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

1. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan; or
2. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

| AC-20 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-20 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All relevant and selected security controls are evaluated before an external system can access either 18F’s production AWS account or production cloud.gov environment. See AC-20 for details. |
| Part b | Depending on the nature of the agreement, GSA follows all relevant records retention laws and policies. GSA stores all documents requiring temporary retention in its enterprise Google Apps for Government account. All documents requiring permanent retention are forwarded to the National Archives and Records Administration (NARA) as appropriate. |

#### AC-20 (2) Control Enhancement (M) (H)

The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

| AC-20 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: AWS GovCloud | |
| Parameter AC-20(2): Not Applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-20 (2) What is the solution and how is it implemented? |
| --- |
| cloud.gov is entirely an external information system. Neither GSA staff or cloud.gov customers have access to AWS datacenters, so they cannot connect portable storage devices into cloud.gov.  See the Provisional Authorization for AWS GovCloud for additional details. |

### AC-21 Information Sharing (M) (H)

The organization:

1. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and
2. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.

| AC-21 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Parameter AC-21(a): customer defined | |
| Parameter AC-21(b): not applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-21 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov does not maintain information at either the platform level itself, or in AWS, that has special administrative or legal restrictions that must be analyzed when shared. The only information maintained is either completely open to the public, such as the code itself, or cannot be shared with anyone, such as environment variables or passwords.  **Customer Responsibility**  If a customer decides to use cloud.gov to store privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, or information that is otherwise compartmentalized, they are wholly responsible for this control. |
| Part b | **Customer Responsibility**  See part a above. Customers are wholly responsible for this control. |

### AC-22 Publicly Accessible Content (L) (M) (H)

The organization:

1. Designates individuals authorized to post information onto a publicly accessible information system;
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
3. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
4. Reviews the content on the publicly accessible information system for nonpublic information [FedRAMP Assignment: at least quarterly] and removes such information, if discovered.

| AC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Parameter AC-22: continuously | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AC-22 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Anyone in the world can *propose* changes to all of 18F’s publicly accessible information systems. This is accomplished by making a “pull request” ( <https://guides.github.com/introduction/flow/> ) on an 18F GitHub repository. The System Owner determines the appropriate settings ( <https://help.github.com/articles/defining-the-mergeability-of-pull-requests/> ) on each repository. These settings designate the role(s) that can actually merge these changes into the master or “canonical” version of the information system.  **Customer Responsibility**  Customers are wholly responsible for this control for their applications. |
| Part b | All 18F staff receive the 18F Handbook ( <https://handbook.18f.gov/> ) and training on the 18F Open Source Policy.  This training includes:   * 18F GitHub Rules, which note sensitive information that shouldn’t be shared (<https://handbook.18f.gov/github/#rules>). * 18F Open Source Policy practices, which also note sensitive information (i.e. controlled unclassified information) that shouldn’t be shared (<https://github.com/18F/open-source-policy/blob/master/practice.md#protecting-sensitive-information>).   All GSA staff also receive required training through the GSA Online Learning University (OLU), including but not limited to the mandatory annual training on IT Security Awareness and Privacy. Among other topics, this ensures staff always follow appropriate procedures when handling sensitive information, such as personally identifiable information (PII) or controlled unclassified information (CUI).  In addition, cloud.gov team members must take the cloud.gov-specific Nonpublic Information Training within 60 days of joining the team (and annually after that), as documented in the team Onboarding Checklist. The System Owner is responsible for ensuring this training is conducted and addresses cloud.gov system needs.  **Customer Responsibility**  Customers are wholly responsible for this control for their applications. |
| Part c | Since GitHub “pull requests” (proposed changes to public information) are themselves public, all GSA staff are responsible for ensuring that their pull requests do not include non-public information.  If staff need to discuss sensitive information, or if they are uncertain whether information is sensitive or not, they discuss the information in a pre-existing GSA chat or email system.  **Customer Responsibility**  Customers are wholly responsible for this control for their applications. |
| Part d | The cloud.gov team continuously reviews changes to public information: each proposed change needs to be “merged” (approved) by another team member.  **Customer Responsibility**  Customers are wholly responsible for this control for their applications. |

## Awareness and Training (AT)

### AT-1 Security Awareness and Training Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
2. Reviews and updates the current:
   1. Security awareness and training policy [FedRAMP Assignment: at least every 3 years]; and
   2. Security awareness and training procedures [FedRAMP Assignment: at least annually].

| AT-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter AT-1(a): cloud.gov development and design team | |
| Parameter AT-1(b)(1): At least every three years | |
| Parameter AT-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AT-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/AT-Policy.md> for the Awareness and Training procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### AT-2 Security Awareness (L) (M) (H)

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

1. As part of initial training for new users;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| AT-2 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO) | |
| Parameter AT-2(c): As part of a new hire and a least annually thereafter | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AT-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | As part of GSA, all cloud.gov team members are required to take basic security awareness training provided by the GSA Office of the Chief Information Security Officer (OCISO). All GSA employees and contractors with a GSA account are provided training by the GSA OCISO.  The GSA Information Security Policy and Compliance (ISP) division is responsible for the management and coordination of security related training for GSA. ISP develops and updates training materials for security awareness training on an annual basis. For new users entering GSA (employee or contractor), ISP coordinates with Online University (OLU) and Comprehensive Human Resources Integrated System (CHRIS) to ensure new users take the required training as soon as they receive network access. ISP utilizes OLU to provide training to all GSA users.  New GSA staff, which includes 18F/cloud.gov team members, are required to complete the IT Security Awareness And Privacy 101 Training course within the first 60 days of their assignment. Users must complete the course and pass the accompanying mandatory test with a score of 70% or better to receive credit for the course. If a user fails to successfully complete the course, their e-mail account is deactivated.  New users are notified via their GSA Gmail account, and have 30 days from notification to successfully complete the course.  The IT Security Awareness And Privacy 101 course includes training in guarding against the following   1. Hackers 2. Malicious code / malware 3. Identity theft 4. Phishing / spear phishing   Contractors/vendors with GSA email accounts are required to receive this training by OLU as well. Those individuals without a GSA email account receive training by hardcopy and may be supplemented by the contractors/vendors. This is administered and tracked by the program office utilizing the vendor. |
| Part b | GSA provides additional basic security training when GSA information systems change, through Adobe Connect meetings and additional documentation such as white papers or training materials. |
| Part c | GSA provides annual refresher training with the updated release of GSA Security Policies. GSA refresher training is held through OLU. Basic material for refresher trainings is the same as initial employee training. Information security awareness training is a mandatory annual requirement for all GSA staff, including but not limited to employees and consultants. |

#### AT-2 (2) Control Enhancement (M) (H)

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

| AT-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AT-2 (2) What is the solution and how is it implemented? |
| --- |
| The GSA OLU training program includes security awareness training on recognizing and reporting potential indicators of insider threat. More information regarding insider threat training can be found in the GSA Memorandum *ADM P 2400.1 Insider Threat Program* (Final Policy Signed on 6-20-2014). |

### AT-3 Role-Based Security Training (L) (M) (H)

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

1. Before authorizing access to the information system or performing assigned duties;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| AT-3 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Parameter AT-3(c): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AT-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Agency Security Awareness and Training Policy**  Role-Based Security Training is provided by GSA Information Security Policy and Compliance Division (ISP) of the Office of the Chief Information Security Officer (OCISO). ISP is responsible for the management and coordination of role-based security training for GSA. ISP develops and updates training materials (such as CBTs, Slides) for role-based security training periodically. In the event ISP employs vendors to provide role-based training, ISP will coordinate with the vendor on the type of training that is required. Users with security roles and responsibilities are trained prior to performing their duties and every year (1) thereafter.  **cloud.gov Program Security Awareness and Training Policy**  The Program Manager ensures that Cloud Operations staff with significant information system security roles complete role-based security-related training at or upon being granted access, and subsequent refresher training at least annually.  Contingency planning personnel are provided training, as a part of periodic disaster recovery exercises. Additional training will be performed pending outcome of test exercises. Outside of these personnel, 18F encourages their employees to take training opportunities but does not enforce any specialized (role based) security training mandates. |
| Part b | Additional Security Training is provided when there are information system changes through video conferencing and/or additional documentation such as white papers or training materials. |
| Part c | Annual refresher training is provided each year with the updated release of Cloud Operations, 18F and GSA Security Policies. Refresher training depending on department is held in either the form of a meeting, or through OLU. Basic material for refresher trainings is the same as initial employee training. Role based security awareness training is a mandatory annual requirement for all Cloud Operations staff, including but not limited to employees and consultants. |

#### AT-4 Security Training Records (L) (M)

The organization:

1. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
2. Retains individual training records for [FedRAMP Assignment: at least one year].

| AT-4 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter AT-4(b): at least one year | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AT-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Agency Security Awareness and Training Policy**  Security Training Records are provided by the GSA Information Security Policy and Compliance Division (ISP) of the Office of the Chief Information Security Officer (OCISO. ISP is responsible for the management and retaining of security awareness and role-based security training records. If the security training is provided using GSA’s OLU then OLU provides reports to ISP on individuals that require security training. If OLU is not used, a tracking spreadsheet is used to track individuals that have taken training and those that still needs to take them. If ISP employs a vendor for training, ISP coordinates with the vendor to provide them with a way of tracking individuals assigned to take a specific training to ensure training is completed.  **Cloud Operations Program Security Awareness and Training Policy**  Whenever a new person joins the Cloud Operations team, the cloud.gov Program Manager creates a story card documenting a checklist of required training materials. The new team member is assigned a peer to assist with the completion of all required training.  The story card is closed when the required training is complete.  The same process is applied to each team member annually as if they were a new team member. |
| Part b | **Agency Security Awareness and Training Policy**  GSA retains records of initial security awareness training in respective HR records for at least a year, and subsequent refresher training on file in management records for each individual, until the GSA personnel leave or are terminated. Managers are the point of contact for all role-based training.  **Cloud Operations Program Security Awareness and Training Policy**  Story cards are stored permanently for auditing and compliance purposes. |

## Audit and Accountability (AU)

### AU-1 Audit and Accountability Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
2. Reviews and updates the current:
   1. Audit and accountability policy [FedRAMP Assignment: at every 3 years]; and
   2. Audit and accountability procedures [FedRAMP Assignment: at least annually].

| AU-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter AU-1(a): cloud.gov development and design team | |
| Parameter AU-1(b)(1): At least every three years | |
| Parameter AU-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AU-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See https://github.com/18F/compliance-docs/blob/master/AU-Policy.md for the Audit and Accountability procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### AU-2 Audit Events (L) (M) (H)

The organization:

1. Determines that the information system is capable of auditing the following events: [FedRAMP Assignment: [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];
2. 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;
3. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
4. Determines that the following events are to be audited within the information system: [FedRAMP Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited continually for each identified event].

AU-2 Additional FedRAMP Requirements and Guidance:

Requirement: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO.

| AU-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, System Owner, Cloud Operations, Information Systems Security Officer (ISSO) | |
| Parameter AU-2(a): 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. | |
| Parameter AU-2(d): All events defined in AU-2(a). | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **AWS**  Cloud Operations has implemented CloudTrail and CloudWatch Logs for its account and system monitoring of AWS virtual infrastructure. These tools provide visibility into user activity by recording API calls made on an AWS account and its cloud infrastructure.  **cloud.gov**  cloud.gov provides an audit trail through the BOSH *tasks* command. This command shows all actions that an operator has taken with the platform. These BOSH events are sent to CloudWatch Logs.  For end users, cloud.gov records an audit trail of all relevant API invocations of an app. The CLI command *cf events* returns this information.  Loggregator, the Cloud Foundry component responsible for logging, provides a stream of log output from hosted applications and from cloud.gov system components that interact with applications during updates and execution. Loggregator allows users to:   1. Tail their application logs. 2. Dump a recent set of application logs (where recent is a configurable number of log packets). 3. Continually drain their application logs to the ELK stack log archive and analysis services.   The ELK stack includes Logstash, a centralized logging and parsing data pipeline that is used to process logs in different formats. Logstash uses different rules to format each log message into multiple fields, which are indexed by the Elasticsearch search engine used for deep searches and data analytics. Kibana is a web interface that provides an overview of the collected data, so 18F can easily view and analyze the collected logs.  cloud.gov scans code on the platform for malicious code elements. See SI-4 for information about tools that detect potentially malicious activity (including ClamAV, Snort, and Tripwire). These ClamAV, Snort, and Tripwire events are sent to CloudWatch Logs.  **Customer Responsibility**  All applications inherit the ELK stack auditing functions and capabilities that reside on the cloud.gov PaaS, including log storage and the Kibana log viewing/searching application. Application System Owners must ensure their application’s activities are monitored and captured within audit logs. |
| Part b | Cloud Operations makes audit logs available to client organizations and for mutual support in response to security breaches, system and user access, incident reporting and continuous monitoring. Cloud Operations generates and distributes audit reports, provides dashboard access for audited events, and sends audit log data to SIEM and log analysis systems as needed. |
| Part c | Cloud Operations regularly reviews and updates the defined events, as described in AU-2 (3). The cloud.gov Program Manager oversees Cloud Operations work on auditing and logging, to ensure that the auditable events are adequate to support after-the-fact investigations of security incidents. |
| Part d | cloud.gov automatically captures all the auditable events that the system is capable of capturing, with automated continuous monitoring and auditing. Part a and the following details help explain how this is accomplished.  **AWS**  Because CloudTrail logging is enabled, API calls made to EC2, EBS, and VPC actions are tracked in log files, along with any other AWS service records. Every log entry contains information about who generated the request. When looking at the full details of an event, the audit trail shows the full information described in AU-3.  **cloud.gov**  cloud.gov provides an audit trail through the BOSH *tasks* commands. This command shows all actions that an operator has taken with the platform.  For users, cloud.gov records an audit trail of all relevant API invocations of an application using the *cf logs* or *cf logs --recent* command. The logs are fed to the Loggregator component which is responsible for logging and provides a stream of log output from cloud.gov applications and system components that interact with a hosted app during updates and execution.  The BOSH CLI captures audit events from several log types within the cloud.gov platform itself. These logs consist of VM logs ([Job logs](https://bosh.io/docs/job-logs.html#job-logs), [Errand logs](https://bosh.io/docs/job-logs.html#errand-logs), [Monit logs](https://bosh.io/docs/job-logs.html#monit-logs), [Agent logs](https://bosh.io/docs/job-logs.html#agent-logs), [Log rotation](https://bosh.io/docs/job-logs.html#log-rotation) and [Syslog configuration](https://bosh.io/docs/job-logs.html#syslog-conf)) and [Director task logs](https://bosh.io/docs/job-logs.html#director-logs). See <https://bosh.io/docs/job-logs.html#vm-logs> for details.  **Customer Responsibility**  Application System owners are responsible for making sure audit events are captured based on AU-2(d) parameter requirements for their web applications. |

#### AU-2 (3) Control Enhancement (M) (H)

The organization reviews and updates the audited events [FedRAMP Assignment: annually or whenever there is a change in the threat environment].

AU-2 (3) Additional FedRAMP Requirements and Guidance:

Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the JAB/AO.

| AU-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Parameter AU-2(3): annually or whenever there is a change in the threat environment | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-2 (3) What is the solution and how is it implemented? |
| --- |
| Cloud Operations updates the defined auditable events on a quarterly basis or when changes in the threat environment occur or are identified by risk assessment. This quarterly Security Policy and Account Review meeting is on the cloud.gov team’s GSA Google Apps calendar as a recurring event. The meeting is conducted with a quorum of the Cloud Operations team present and reviews incidents, alerts, logs, metrics, postmortems and events for the prior period. Once reviewed, alerting policy and procedures are updated to reflect identified issues. All updates and changes in the threat environment will be included in updates provided to the FedRAMP Joint Authorization Board (JAB). |

### AU-3 Content of Audit Records (L) (M) (H)

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

| AU-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-3 What is the solution and how is it implemented? |
| --- |
| CloudTrail, CloudWatch Logs, Snort, Tripwire, ClamAV, and Prometheus collect, monitor, and maintain audit logs for both AWS and cloud.gov.  For all logging, all events are timestamped. Each tool has a log format with additional details that vary based on tool but are comprehensive enough to answer the who, what, and where of any event.  For example, AWS CloudTrail captures and records the following information about each API call for the list of auditable events:   1. User – the IAM user name of the person who was interacting with the AWS account. 2. IP Address – the IP Address where the interactions originated from. 3. Event Name – the type of interaction that occurred. 4. Service – the AWS Service that was interacted with. 5. Time – the date and time that the event occurred. 6. Region – the AWS Region(s) where the interactions occurred. 7. Resource ID – the resource ID from the event.   cloud.gov provides an audit trail through the BOSH tasks command. As described in the BOSH documentation ( <https://bosh.io/docs/sysadmin-commands.html#tasks> ), *tasks* lists items with ID number, state, timestamp, user, description, and result. |

#### AU-3 (1) Control Enhancement (M)

The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information].

AU-3 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines audit record types [FedRAMP Assignment: session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon]. The audit record types are approved and accepted by the JAB.

Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.

| AU-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, System Owner, Information Systems Security Officer (ISSO) | |
| Parameter AU-3(1): session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-3 (1) What is the solution and how is it implemented? |
| --- |
| cloud.gov generates and collects comprehensive audit records, due to the complete virtualization of the environment and the comprehensive tooling. See descriptions in detail in AU-2 and AU-3.  For example, AWS CloudTrail logs include comprehensive details about each log item, including the “event name” (the type of interaction that occurred), with specific details depending on the type of AWS API call. The CloudTrail documentation shows the level of activity detail that CloudTrail typically captures: <http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-examples.html>  As another example, Cloud Foundry customer application logs include the comprehensive details documented at <https://docs.cloudfoundry.org/devguide/deploy-apps/streaming-logs.html> - always including timestamp, log type (origin code), channel, and message. |

### AU-4 Audit Storage Capacity (L) (M) (H)

The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

| AU-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AU-4: retain logs for 180 days online and one year offline | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-4 What is the solution and how is it implemented? |
| --- |
| Cloud Operations defines the amount of storage dedicated to audit log records on their EC2 instances and S3 buckets. cloud.gov uses elastic file storage (EBS volumes) that allows the information system to grow storage capacity as required. The use of elastic file storage reduces the likelihood of such capacity being exceeded within the information system. This system also includes automated alerts that notify Cloud Operations (via PagerDuty) if they may need to manually expand the space soon, as noted in AU-5.  Cloud Operations team members are responsible for maintaining the configuration that enforces the audit settings.  The log management framework provides the capability to retain logs for 180 days online, with sufficient capacity as to mitigate the risk of exceeding storage space. In the event the threshold is exceeded, administrators can add additional storage capacity without impacting the system.  This system includes customer application logs. cloud.gov is responsible for storing customer application logs, and it provides a "drain" feature that allows customers to also store their own logs automatically. |

### AU-5 Response to Audit Processing Failures (L) (M) (H)

The information system:

1. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and
2. Takes the following additional actions: [FedRAMP Assignment: organization-defined actions to be taken; (overwrite oldest record)].

| AU-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AU-5(a): Cloud Operations, Information Systems Security Officer (ISSO), Program Manager | |
| Parameter AU-5(b): shut down the system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov has the ability to elastically grow the audit storage capacity, which reduces the likelihood of such capacity being exceeded within the information system.  Logstash is configured to ship logs to CloudWatch Logs as well as ELK, so that if there is a fault in the ELK subsystem, the platform’s ability to capture logs and serve traffic is not impacted.  Cloud Operations has implemented alerting to notify of insufficient audit storage capacity or if no new logs have been written to the ELK stack or CloudWatch Logs within a five-minute timeframe.  All hosts are configured to send canary logs to CloudWatch Logs at a regular interval. Prometheus is configured to monitor CloudWatch Logs and react when logs stop flowing from a host. |
| Part b | If logs stop flowing from a host, Prometheus sends an alert to Cloud Operations via PagerDuty, snapshots the host that is failing to log as expected for later forensics/log-mining/re-ingestion, then shuts down the host. BOSH then notices the expected host is missing, destroys the instance, and replaces it with a fresh instance. Cloud Operations then investigates the PagerDuty incident and marks it resolved when complete.  **Customer Responsibility**  If the Loggregator subsystem is a bottleneck for upstream customer applications, it may operate in a degraded fashion by dropping some logs until it can keep up. In order to keep a single hosted heavily-logging application from affecting the availability of all other hosted applications, we regard it as an operational requirement to keep customer apps up and handling traffic even when Loggregator is operating in this degraded fashion. Customers are responsible for configuring a separate logging facility directly in their hosted app if this behavior doesn’t suit their agency standards for satisfying AU-5. |

### AU-6 Audit Review, Analysis, and Reporting (L) (M) (H)

The organization:

1. Reviews and analyzes information system audit records [FedRAMP Assignment: at least weekly] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and
2. Reports findings to [Assignment: organization-defined personnel or roles].

AU-6 Additional FedRAMP Requirements and Guidance:

Requirement: Coordination between service provider and consumer shall be documented and accepted by the Authorizing Official. In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer shall be documented.

| AU-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Parameter AU-6(a)-1: At least weekly | |
| Parameter AU-6(a)-2: virus signatures, known exploits, unauthorized network activity | |
| Parameter AU-6(b): System Owner, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Through the use of CloudTrail, CloudWatch Logs, BOSH, Nessus, ClamAV, Snort, GitHub, and the ELK logging system, the Cloud Operations team monitors and reviews audit logs for unapproved and unusual activities on a continual basis. This monitoring and reviewing process includes monitoring for potentially malicious insider activities.  Details:   * CloudTrail provides a detailed listing of all AWS events, with both users and system accounts, with a timestamp and the access ID used. * CloudWatch Logs aggregates all system logs from all cloud.gov servers. * BOSH records all system logins and software deployments. * Nessus continuously scans for security vulnerabilities and reports results. * ClamAV continuous monitors each server for signature and behavior vulnerabilities and raises alerts based on defined rules. * Snort continuously monitors network traffic, signatures and behaviors and raises alerts based on defined rules. * GitHub provides a list of source code changes including the author and strong hashing to verify integrity of the code. * ELK provides an aggregate of all cloud.gov tenant application logs.   We use reporting rulesets developed by the Snort, Nessus and ClamAV teams, which look for, identify, and report potentially inappropriate or unusual activity to be reviewed regularly.  In all cases, these tools scan for deviations from historical traffic patterns either in type or quantity. Some alert based on defined rules, and some alert on thresholds through Prometheus. Together, these tools help identify virus signatures, known exploits, unauthorized network activity, and potentially malicious insider activities. See diagram 10-4.3 *(Monitoring and Alerting Data Flow)* for a diagram of how each tool sends data to the aggregation points.  Security vulnerabilities and system inconsistencies are reviewed by the Cloud Operations team (notified by email, text message and voice phone call). Security vulnerabilities which are not classified as high are reviewed weekly and resolved by Cloud Operations. The *GSA IT Security Policy* includes: "All critical and high vulnerabilities identified must be mitigated within 30 days and all moderate vulnerabilities mitigated within 90 days."  Regular security reports are automatically generated by Nessus and sent to the System Owner, GSA’s Information Security team, and other partner agencies as required.  See SI-4 for more detail.  **Customer Responsibility**  Customers can review their own application logs by accessing the ELK stack, which has a customer-facing web frontend at <https://logs.fr.cloud.gov>. (Customer logs are protected by a proxy on ELK that filters the user's access according to their permissions.)  Application System Owners are responsible for ensuring they review and analyze application logs. |
| Part b | **cloud.gov Team**  The Cloud Operations team acts on findings that result from its regular audit process according to its incident response guidelines ( <https://cloud.gov/docs/ops/security-ir/> ), including notifying GSA Information Security, the System Owner, and the ISSO.  **GSA Information Security**  When a credible source to GSA provides information that causes reason to enhance audit activities, GSA will develop and implement an enhanced auditing use-case that will adequately enhance auditing practices in a fashion necessary per the identified threat and following the Incident Reporting Procedures in *GSA IT Security Procedural Guide 01-02 (04/07/2015), Incident Response*. GSA may also, through analysis pertaining to the GSA environment, provide additional audit measures that will require an increase in review, analysis, and reporting for a necessary.  GSA monitors information security news and alerts for indications of a need to heighten information system security monitoring. Sources such as product vendors, United States Computer Emergency Readiness Team (US-CERT) and other security community resources will be leveraged to provide information on emerging threats and changes to the landscape. At the agency’s request or the determination of Cloud Operations, the review of audit logs shall be increased and any appropriate changes to audit content collection shall be implemented. |

#### AU-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

| AU-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-6 (1) What is the solution and how is it implemented? |
| --- |
| cloud.gov uses the automated mechanisms CloudTrail, CloudWatch, and Prometheus to integrate audit monitoring, analysis and reporting into an overall process for investigation and response to suspicious activities. Prometheus receives data from multiple sources (see AU-6(a)) and makes that data available for regular auditing. Prometheus stores data in a time series database, which assists in correlating data.  Cloud Operations employs CloudWatch and CloudWatch Logs to collect and track metrics to monitor in real time infrastructure log data and resources. Integration with CloudWatch Logs enables CloudTrail to send events containing API activity in the cloud.gov AWS account to a CloudWatch Logs group. Prometheus amalgamates audit data from most other sources (e.g. Snort, ClamAV) and pushes alerts needing attention to PagerDuty.  See diagram 10-4.3 *(Monitoring and Alerting Data Flow)* for a diagram of how each tool sends data to the aggregation points. |

#### AU-6 (3) Control Enhancement (M) (H)

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

| AU-6 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-6 (3) What is the solution and how is it implemented? |
| --- |
| Cloud Operations and GSA Information Security have set up comprehensive and automated systems, detailed in the sections under 10.3 *(“cloud.gov Security Domain Stack”)*, including 10.3 *(“Audit Logging, Monitoring, and Intrusion Detection”).* Audit records are under constant analysis, and they can be immediately correlated across any tool.  Refer to *Figure 10‑3 Monitoring and Alerting Data Flow Diagram* for a visual representation of this system, including how Snort, Nessus, and ClamAV send events to correlation tools. As illustrated there, Snort and ClamAV send alerts to Prometheus, which sends processed alerts to PagerDuty, which then sends alerts via email/text/call; Nessus delivers reports via email.  **Partial implementation:**  Cloud Operations manually correlates Nessus logs with other logs, rather than automating this, due to Nessus licensing restrictions. |

### AU-7 Audit Reduction and Report Generation (M) (H)

The information system provides an audit reduction and report generation capability that:

1. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
2. Does not alter the original content or time ordering of audit records.

| AU-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **AWS**  CloudWatch Logs provides on-demand audit review for any actions taken on or in the AWS environment.  **cloud.gov**  Prometheus and Grafana provide the capability to evaluate any action taken on the cloud.gov layer.  The ELK stack, which captures logs related to applications hosted on top of cloud.gov, has the capability to provide audit reduction, analysis, and report generation capability. Specifically, Kibana has the capacity to build search queries on numerous criteria regarding application logs, and it can produce reports and exports.  Logs are also captured in CloudWatch for redundancy. GSA Information Security has a SOC with a SIEM system to correlate events across cloud.gov and other systems, which has access to the cloud.gov CloudTrail logs, and can correlate events across cloud.gov and other systems. |
| Part b | CloudWatch Logs, Prometheus, Grafana, and ELK do not alter the original content or time ordering of audit records. All audit files can be viewed in their raw and JSON standard formats. |

#### AU-7 (1) Control Enhancement (M) (H)

The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].

| AU-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AU-7(1): event types (as defined by software rulesets) and event frequency | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-7 (1) What is the solution and how is it implemented? |
| --- |
| **AWS**  Cloud Operations uses CloudTrail to monitor AWS deployments [in the cloud](https://aws.amazon.com/what-is-cloud-computing/) by getting a history of AWS API calls of the cloud.gov account, including API calls made via the AWS Management Console, the command line tools, and higher-level AWS services. Cloud Operations is able to identify which users and accounts called AWS APIs for services that supports CloudTrail, the source IP address the calls were made from, and when the calls occurred. These logs are searchable.  **cloud.gov**  cloud.gov BOSH audit logs display a table listing the following for all currently running tasks: ID number, state, timestamp, user, description, and result.  For BOSH events within the cloud.gov platform, the event details captured include: cloud config update, runtime config update, deployment create/update/delete, VM create/delete, disk create/delete, and BOSH SSH events.  These logs are searchable as well.  **Customer Responsibility**  Customers can review their own application logs by accessing the ELK stack (which has a customer-facing web frontend at <https://logs.fr.cloud.gov>). |

### AU-8 Time Stamps (L) (M) (H)

The information system:

1. Uses internal system clocks to generate time stamps for audit records; and
2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: one second granularity of time measurement].

| AU-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AU-8(b): the granularity requirement of less than one minute | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All cloud.gov VMs use system clocks synchronized by the NTP daemon to generate time stamps for audit records.  VMs pull from NIST NTP servers (<http://tf.nist.gov/tf-cgi/servers.cgi> ).  Systems poll the NTP servers at least hourly to synchronize. |
| Part b | The cloud.gov timestamps are kept in synchrony by the NTP daemon, which ensures that times are accurate to at least within one minute, more accurately to within tens of milliseconds. These timestamps can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). |

#### AU-8 (1) Control Enhancement (M) (H)

The information system:

1. Compares the internal information system clocks with [FedRAMP Assignment: authoritative time source: [[*http://tf.nist.gov/tf-cgi/servers.cgi*](http://tf.nist.gov/tf-cgi/servers.cgi)] [at least hourly]]; and
2. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].

AU-8 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server.

Requirement: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.

Guidance: The service provider selects primary and secondary time servers used by the NIST Internet time service, or by a Stratum-1 time server. The secondary server is selected from a different geographic region than the primary server.

If using Windows Active Directory, all servers should synchronize time with the time source for the Windows Domain Controller. If using some other directory services (e.g., LDAP), all servers should synchronize time with the time source for the directory server

| AU-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AU-8(1)(a)-1: At least hourly | |
| Parameter AU-8(1)(a)-2: authoritative time source: <http://tf.nist.gov/tf-cgi/servers.cgi> | |
| Parameter AU-8(1)(b): 1 minute | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov compares the internal information system clocks *at least hourly* with the servers in AU-8. |
| Part b | Each cloud.gov VM has a NTP daemon that checks the NTP servers at 15 minute intervals. This check automatically syncs the VM time to the NTP server time upon every check.  This corrects any difference in time, including if the time difference is greater than 1 minute. |

AU-8 (1) Additional FedRAMP Requirements and Guidance:

Requirement 1: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server.

Requirement 2: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.

Guidance: Synchronization of system clocks improves the accuracy of log analysis.

| AU-8 (1) Req. | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | cloud.gov uses the “round-robin” feature of NIST’s NTP servers (documented at <http://tf.nist.gov/tf-cgi/servers.cgi> ), which automatically cycles requests among servers in multiple geographic regions in the United States, including Maryland, Colorado, and Oregon. This means that the system does not need to explicitly specify primary and secondary NTP sources in multiple regions. |
| Req. 2 | All cloud.gov VMs run the same operating system, and they are all synced to the NTP servers in the same way. |

### AU-9 Protection of Audit Information (L) (M) (H)

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

| AU-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-9 What is the solution and how is it implemented? |
| --- |
| To maintain the integrity of log data, Cloud Operations carefully manages access around the generation and storage of audit log files. Access is restricted to Cloud Operations staff.  Audit logs from CloudTrail are stored and protected in specified S3 buckets for cloud.gov, which are limited to read-only access and multifactor authentication by Cloud Operations staff.  Audit logs from the cloud.gov platform are only accessible to Cloud Operations personnel, viewed via either the ELK stack or CloudWatch Logs (ELK logs are automatically copied to CloudWatch Logs via a write-only connection, as described in AU-5 part a). Any backend access to the EC2 hosts supporting the ELK stack in violation of policy triggers an alert to the entire Cloud Operations team, including alerting if a person with operator-level permissions attempts to modify the ELK log data.  Further, the Elasticsearch component of ELK has been proxied such that our implementation filters and prevents modifications to existing logs via the HTTP PUT method, and only accepts the creation of new log entries via the HTTP POST method.  Access to CloudWatch Logs is limited using IAM roles, with least privileges. It only allows creation/appending of log entries; deletion and modification are not allowed. |

#### AU-9 (2) Control Enhancement (M) (H)

The information system backs up audit records [FedRAMP Assignment: at least weekly] onto a physically different system or system component than the system or component being audited.

| AU-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter AU-9(2): At least weekly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-9 (2) What is the solution and how is it implemented? |
| --- |
| cloud.gov sends all audit logs to encrypted S3 buckets where data is redundantly stored across multiple facilities and multiple devices in each facility.  All S3 buckets are accessible only to authorized cloud.gov staff using role-based-access-controls and CloudTrail auditing for logging and monitoring purposes.  Cloud Operations has configured weekly backups of all cloud.gov audit logs to the S3 buckets. |

#### AU-9 (4) Control Enhancement (M) (H)

The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users].

| AU-9 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Parameter AU-9(4): designated members of Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-9 (4) What is the solution and how is it implemented? |
| --- |
| The System Owner authorizes access to management of audit functionality to Cloud Operations staff. The System Owner uses IAM policies to restrict access to EC2 instances and S3 bucket logs. BOSH audit logs are only accessible to those Cloud Operations administrators who have access to the BOSH director. The ELK stack uses role-based auditing controls to ensure audits are secured. |

### AU-11 Audit Record Retention (M)

The organization retains audit records for [FedRAMP Assignment: at least ninety (90) days] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

AU-11 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements

| AU-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Parameter AU-11: records on-line for at least ninety days and further preserves audit records off-line for at least 1 year | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-11 What is the solution and how is it implemented? |
| --- |
| Audit logs are kept according to NARA and GSA retention standards to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Our logging systems referenced above retain logs for 180 days online, with sufficient capacity as to mitigate the risk of exceeding storage space. This information helps the System Owner, GSA Information Security, and Cloud Operations track changes made to its resources and to troubleshoot operational issues. Logs are retained for an additional year in an offline system. |

### AU-12 Audit Generation (L) (M) (H)

The information system:

1. Provides audit record generation capability for the auditable events defined in AU-2 a. at [FedRAMP Assignment: all information system components where audit capability is deployed/available];
2. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and
3. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

| AU-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Parameter AU-12(a): all information system components where audit capability is deployed/available | |
| Parameter AU-12(b): Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| AU-12 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov provides comprehensive audit record generation capability for all auditable events defined in AU-2. The following tools capture information about auditable events (see AU-2 part a and part d for details):   * **AWS API:** CloudTrail * **cloud.gov system logs:** BOSH * **cloud.gov custom-defined metrics:** Prometheus and collectd * **Applications on cloud.gov:** Loggregator   The following tools collect events:   * **AWS API:** CloudWatch Logs * **cloud.gov system logs:** CloudWatch Logs * **cloud.gov custom-defined metrics:** grafana.fr.cloud.gov * **Applications on cloud.gov:** logs.fr.cloud.gov   The auditable events, as defined in AU-2:   * Successful and unsuccessful account logon events * Account management events * Object access * Policy changes * Privilege functions * Process tracking * System events   And for web applications:   * Administrator activity * Authentication checks * Authorization checks * Data deletions * Data access * Data changes * Permission changes   The Cloud Operations team is responsible for maintaining the configuration that enforces the audit settings. |
| Part b | Cloud Operations team members select which auditable events are to be audited by specific components of cloud.gov where audit capability is deployed. |
| Part c | Cloud Operations has developed secure configurations that itemize the settings required to provide an audit record generation capability for the list of audited events defined in AU-2, with the content as defined in AU-3 on cloud.gov components and AWS virtual infrastructure operating systems where audit capability is deployed. The content as defined in AU-3 is sufficient information to, at a minimum, establish:   * Type of event * Date and time * Where the event occurred, * The source of the event, * The outcome (success or failure) of the event * The identity of any user/subject associated with the event   Cloud Operations team members are responsible for maintaining the configuration that enforces the audit settings. |

## Security Assessment and Authorization (CA)

### CA-1 Certification, Authorization, Security Assessment Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
2. Reviews and updates the current:
   1. Security assessment and authorization policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Security assessment and authorization procedures [FedRAMP Assignment: at least annually].

| CA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter CA-1(a): cloud.gov development and design team | |
| Parameter CA-1(b)(1): At least every three years | |
| Parameter CA-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/CA-Policy.md> for the Certification, Authorization, Security Assessment procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### CA-2 Security Assessments (L) (M) (H)

The organization:

1. Develops a security assessment plan that describes the scope of the assessment including:
   1. Security controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine security control effectiveness; and
   3. Assessment environment, assessment team, and assessment roles and responsibilities;
2. Assesses the security controls in the information system and its environment of operation [FedRAMP Assignment: at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
3. Produces a security assessment report that documents the results of the assessment; and
4. Provides the results of the security control assessment to [FedRAMP Assignment: individuals or roles to include the FedRAMP Program Management Office (PMO)].

| CA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: 3PAO | |
| Parameter CA-2(b): At least annually | |
| Parameter CA-2(d): System Owner, Information Systems Security Officer (ISSO), and FedRAMP PMO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud 6/21/2016, | |

| CA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The cloud.gov System Owner has developed a plan that describes the scope of cloud.gov security assessments including:   * Security controls and control enhancements under assessment * Assessment procedures to be used to determine security control effectiveness * Assessment environment, assessment team, and assessment roles and responsibilities   cloud.gov is designed for compliance with the Federal Risk and Authorization Management Program and has adopted the FedRAMP Security Assessment Framework as the basis for its current assessment.  Further, cloud.gov engages a FedRAMP Accredited Third Party Assessment Organization (3PAO) to review the system and 18F operations. |
| Part b | The cloud.gov System Owner has engaged the 3PAO to assess the security controls in cloud.gov at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. |
| Part c | The cloud.gov System Owner has engaged the 3PAO to produce a security assessment report that documents the issues, test activities, findings, and recommendations from the assessment. |
| Part d | The cloud.gov System Owner or Program Manager delivers all documents used in or created during the assessment to generate a complete FedRAMP Authorization package. The package is transmitted to the FedRAMP Program Management Office (PMO) for submission to the FedRAMP JAB. |

#### CA-2 (1) Control Enhancement (L) (M) (H)

The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.

CA-2 (1) Additional FedRAMP Requirements and Guidance:

Requirement: For JAB Authorization, must use an accredited Third Party Assessment Organization (3PAO).

| CA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: 3PAO | |
| Parameter CA-2(1): Accredited 3PAO for JAB Authorization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-2 (1) What is the solution and how is it implemented? |
| --- |
| The cloud.gov System Owner has engaged an accredited 3PAO to conduct the independent assessment of security controls for the cloud.gov information system. |

#### CA-2 (2) Control Enhancement (M) (H)

The organization includes as part of security control assessments, [FedRAMP Assignment: at least annually], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]].

CA-2 (2) Additional FedRAMP Requirements and Guidance:

Requirement: To include 'announced', 'vulnerability scanning’ to occur at least annually.

| CA-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM) | |
| Parameter CA-2(2)-1: At least annually | |
| Parameter CA-2(2)-2: Announced | |
| Parameter CA-2(2)-3: Vulnerability scanning and penetration testing | |
| Parameter CA-2(2)-4: FedRAMP security controls assessment | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-2 (2) What is the solution and how is it implemented? |
| --- |
| cloud.gov implements continuous monitoring and vulnerability scanning as documented in RA-5(a).  Manual penetration testing and red-teaming is scheduled to happen on a yearly basis (via cloud.gov’s 3PAO). |

#### CA-2 (3) Control Enhancement (M) (H)

The organization accepts the results of an assessment of [FedRAMP Assignment: organization-defined information system] performed by [FedRAMP Assignment: any FedRAMP Accredited 3PAO] when the assessment meets [FedRAMP Assignment: the conditions of the JAB/AO in the FedRAMP Repository].

| CA-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, System Owner, Authorizing Official | |
| Parameter CA-2(3)-1: the cloud.gov information system | |
| Parameter CA-2(3)-2: any FedRAMP Accredited 3PAO | |
| Parameter CA-2(3)-3: the conditions of the JAB in the FedRAMP Repository | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-2 (3) What is the solution and how is it implemented? |
| --- |
| The cloud.gov System Owner or Program Manager reviews and accepts the assessment results conducted by the 3PAO, according to the FedRAMP JAB P-ATO requirements in the Secure Repository. |

### CA-3 System Interconnections (L) (M) (H)

The organization:

1. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
2. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
3. Reviews and updates Interconnection Security Agreements [FedRAMP Assignment: at least annually and on input from FedRAMP].

Table ‑ CA-3 Authorized Connections

| Authorized Connections Information System Name | Name of Organization 18F / GSA System Connects To | Role and Name of Person Who Signed Connection Agreement | Name and Date of Interconnection Agreement |
| --- | --- | --- | --- |
| N/A | N/A | N/A | N/A |

| CA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, Information Systems Security Officer (ISSO) | |
| Parameter CA-3(c): Not applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | This control is not applicable to the cloud.gov information system. cloud.gov does not have any connections to other external information systems or interconnection security agreements (ISA) with other external agencies. |
| Part b | See above. |
| Part c | See above. |

#### CA-3 (3) Control Enhancement (M) (H)

The organization prohibits the direct connection of an [Assignment: organization-defined unclassified, non-national security system] to an external network without the use of [FedRAMP Assignment: boundary protections which meet Trusted Internet Connection (TIC) requirements].

CA-3 (3) Additional FedRAMP Requirements and Guidance: Refer to Appendix H – Cloud Considerations of the TIC 2.0 Reference Architecture document. Link: https://www.fedramp.gov/files/2015/04/TIC\_Ref\_Arch\_v2-0\_2013.pdf

| CA-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Program Manager, System Owner, Information Systems Security Officer (ISSO) | |
| Parameter CA-3(3)-1: unclassified, non-national security system | |
| Parameter CA-3(3)-2: Boundary Protections which meet Trusted Internet Connection (TIC) requirements | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-3 (3) What is the solution and how is it implemented? |
| --- |
| **GSA Laptops**  *For the network paths from GSA laptops traversing the GSA network on their way to AWS or the internet from GSA office locations or GSA Virtual Private Networks (VPN):*  GSA's network is provided by [CenturyLink's Managed Trusted Internet Protocol Service (MTIPS)](http://www.centurylink.com/business/networx/products/ipbased/mtips.html). MTIPS itself is a GSA program, leveraging the [Networx contracts](http://www.gsa.gov/portal/content/104870), run in consultation with and subject to the [approval of the Department of Homeland Security (DHS)](https://www.dhs.gov/managed-trusted-internet-protocol-services).  The GSA laptops of the staff working as any cloud.gov Role do not have any connections to other external information systems or interconnection security agreements (ISA) with other external agencies at this time.  **AWS and cloud.gov**  *For the inbound and outbound network paths of applications or services within the cloud.gov authorization boundary:*  cloud.gov does not have any connections to other external information systems or interconnection security agreements (ISA) with other external agencies at this time. Nor does it have a connection to any GSA internal network.  For GSA’s applications within the cloud.gov authorization boundary (such as the cloud.gov web user interface and other applications run by the cloud.gov team), GSA is responsible for meeting all TIC requirements for public cloud-based systems. All packets are available if needed to the staff of GSA Information Security's GSA Information Security Center (SOC), who coordinate all TIC or EINSTEIN requirements with DHS.  18F, the FedRAMP PMO, and DHS have all worked closely together to ensure a common understanding of this cloud architecture, and to ensure teams have access to the data they need.  18F collaborated with AWS on documenting AWS TIC options in their *FedRAMP-Trusted Internet Connection (TIC) Overlay Pilot Program* ( <https://aws.amazon.com/blogs/publicsector/fedramp-trusted-internet-connection-tic-overlay-pilot-program/> ). Pages 12-13 of the associated whitepaper ( <https://d0.awsstatic.com/whitepapers/compliance/Guidance_for_Trusted_Internet_Connection_TIC_Readiness_on_AWS.pdf> ) provide an example.  **Customer Responsibility**  Application System Owners are responsible for ensuring that any network paths used by their developers that lead to the boundaries of all cloud.gov endpoints fully comply with their own implementation(s) of the TIC architecture, or that they use a MTIPS provider.  Application System Owners with a need to send “restricted data” over external connections that are gated by a TIC stack (or “access point”) in front of their applications residing in cloud.gov are fully responsible for implementing their own TIC stack in their cloud.gov application space.  Application System Owners must use some combination of the brokered AWS compute, network, memory, storage, and cloud.gov managed service capabilities provided by cloud.gov in order to build their TIC stack.  Combined with the ability to deploy custom buildpacks ( <https://cloud.gov/docs/apps/experimental/custom-buildpacks/> ) or full binary buildpacks ( <http://docs.cloudfoundry.org/buildpacks/binary/index.html> ), Application System Owners may select and deploy whatever technologies they prefer in order to meet their TIC capabilities.  Once a TIC stack that meets all relevant and applicable TIC capabilities has been created in the application Spaces bound to their Organization, Application System Owners may then deploy a user-provided route service ( <https://docs.cloudfoundry.org/services/route-services.html#user-provided> ). Deploying a user-provided route service (also called a custom route service) gives Application System Owners control and assurance that ***no* additional routes are permitted that provide an external connection without passing through their TIC stack.**  Application System Owners must be careful when deploying an app to remove all default routes that would permit external connections that circumvent their TIC-augmented route. They can accomplish this by specifying to the cloud.gov API that no default route should be created. Example: <https://docs.cloudfoundry.org/devguide/deploy-apps/manifest.html#no-route> |

#### CA-3 (5) Control Enhancement (M)

The organization employs [Selection: allow-all, deny-by-exception, deny-all, permit by exception] policy for allowing [Assignment: organization-defined information systems] to connect to external information systems.

CA-3 (5) Additional FedRAMP Requirements and Guidance:

Guidance: For JAB Authorization, CSPs shall include details of this control in their Architecture Briefing

| CA-3 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO), System Owner | |
| Parameter CA-3(5)-1: deny-all, permit-by-exception | |
| Parameter CA-3(5)-2: Not Applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-3 (5) What is the solution and how is it implemented? |
| --- |
| This control is not applicable to the cloud.gov information system.cloud.gov does not have any connections to otherexternal information systems or interconnection security agreements (ISA) withother external agencies at this time. |

### CA-5 Plan of Action and Milestones (L) (M) (H)

The organization:

1. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
2. Updates existing plan of action and milestones [FedRAMP Assignment: at least monthly] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-5 Additional FedRAMP Requirements and Guidance:

Requirement: Plan Of Action & Milestones (POA&M)s must be provided at least monthly.

| CA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM) | |
| Parameter CA-5(b): continuously | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The cloud.gov Plan of Actions and Milestones (POAMs) is updated whenever necessary. |
| Part b | The POAM is updated continuously. |

### CA-6 Security Authorization (L) (M) (H)

The organization:

1. Assigns a senior-level executive or manager as the authorizing official for the information system;
2. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
3. Updates the security authorization [FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs].

CA-6c Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F ([SP 800-37](http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf)). The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the JAB/AO.

| CA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Authorizing Official, FedRAMP JAB | |
| Parameter CA-6(c): in accordance with OMB A-130 requirements or when a significant change occurs | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The FedRAMP JAB serves as the Authorizing Official (AO) for the cloud.gov information system. |
| Part b | The Authorizing Official’s responsibilities include ensuring cloud.gov is assessed and authorized before going to an operational state.  Following review of the assessment package and consultation with key 18F officials, the JAB makes a final risk-based decision on whether or not to grant a P-ATO which may include the following stipulations:   * Authorize system operation without any restrictions or limitations on its operation. * Authorize system operation with restrictions or limitation on its operation. Any POAMs must include detailed corrective actions plans to address/mitigate deficiencies. Resubmit an updated assessment package upon completion of required POAM actions to move to ATO without any restrictions. * Not authorize the system for operation. |
| Part c | The cloud.gov System Owner updates the cloud.gov security authorization as needed based on any significant changes as defined by NIST Special Publication 800-37 Revision 1 or at FedRAMP-assigned periodicity. Examples of this are:   * Major platform changes * New software development bringing new functionality * Increased direct access to the production network. |

### CA-7 Continuous Monitoring (L) (M) (H)

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. Establishment of [Assignment: organization-defined metrics] to be monitored;
2. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring;
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of organization and the information system to [FedRAMP Assignment: to meet Federal and FedRAMP requirements] [Assignment: organization-defined frequency].

CA-7 Additional FedRAMP Requirements and Guidance:

Requirement: Operating System Scans: at least monthly Database and Web Application Scans: at least monthly All scans performed by Independent Assessor: at least annually.

Guidance: CSPs must provide evidence of closure and remediation of a high vulnerability within the timeframe for standard POA&M updates.

| CA-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM) | |
| Parameter CA-7(a): performance, job / program health, malicious code detection, network intrusion, intruder detection, vulnerability detection | |
| Parameter CA-7(b)-1: continuous frequency | |
| Parameter CA-7(b)-2: quarterly frequency | |
| Parameter CA-7(g)-1: to meet Federal and FedRAMP requirements | |
| Parameter CA-7(g)-2: continuous | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov adheres to the *cloud.gov Continuous Monitoring Strategy* (available at <https://cloud.gov/docs/ops/continuous-monitoring/> ). The monitored metrics are defined in the “Automated components” section ( <https://cloud.gov/docs/ops/continuous-monitoring/#automated-components> ). |
| Part b | The Cloud Operations team performs an assessment of the continuous monitoring strategy at a quarterly meeting. See above document for details of the strategy. |
| Part c | The Cloud Operations team reviews its controls as part of the annual 3PAO assessment.  Compliance with security controls that can be tested from the operating system level (e.g. presence of configuration settings, etc.) are monitored and automatically corrected as part of configuration management. Non-automated security processes are handled by the cloud.gov operations team following the cloud.gov Continuous Monitoring Strategy and cloud.gov Incident Response Plan. |
| Part d | The Cloud Operations team follows the Continuous Monitoring Strategy and program, which includes ongoing security status monitoring of FedRAMP and GSA defined metrics. |
| Part e | The Cloud Operations team implements a continuous monitoring program that includes correlation and analysis of security-related information generated by assessments and monitoring in accordance with the FedRAMP and GSA continuous monitoring strategy. |
| Part f | Response actions use the mitigation strategy defined in RA-5(d). |
| Part g | The FedRAMP PMO and the cloud.gov 3PAO will have consistent and continuous access to the latest versions of cloud.gov’s security documentation and security scanning. The Authorizing Official will be briefed at least monthly by the Cloud Operations and GSA Information Security teams. Whenever technical or operational changes require updates to cloud.gov’s security documentation, this package will be updated as soon as possible. |

CA-7 Additional FedRAMP Requirements and Guidance:

Requirement 1: Operating System Scans: at least monthly

Requirement 2: Database and Web Application Scans: at least monthly

Requirement 3: All scans performed by Independent Assessor: at least annually

| CA-7 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | See RA-5 for Operating System scanning details. |
| Req. 2 | See RA-5 for Database and Web Application scanning details. |
| Req. 3 | 18F employs a 3PAO for annual assessments of cloud.gov. |

#### CA-7 (1) Control Enhancement (M) (H)

The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.

| CA-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: 3PAO, GSA Information Security | |
| Parameter CA-7(1): full independence (3PAO) and in the agency but outside the cloud.gov team (GSA Information Security) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-7 (1) What is the solution and how is it implemented? |
| --- |
| The cloud.gov Program Manager and System Owner engage an accredited 3PAO assessment team to conduct annual assessments of security controls for cloud.gov.  GSA Information Security (which is in the same agency as cloud.gov but outside the cloud.gov core team) monitors the security of the cloud.gov system on an ongoing basis. |

### CA-8 Penetration Testing (M) (H)

The organization conducts penetration testing [FedRAMP Assignment: at least annually] on [Assignment: organization-defined information systems or system components].

| CA-8 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Authorizing Official, 3PAO | |
| Parameter CA-8-1: at least annually | |
| Parameter CA-8-2: all cloud.gov components | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-8 What is the solution and how is it implemented? |
| --- |
| **AWS**  See the Provisional Authorization for AWS GovCloud.  **cloud.gov**  cloud.gov’s System Owner engages with 3PAO(s), and other organizations or entities, to perform penetration testing of cloud.gov. Penetration testing of all cloud.gov components occurs *at least* annually, or whenever requested by the System Owner or Authorizing Official.  cloud.gov consults, at minimum, the *GSA IT Security Procedural Guide: Conducting Penetration Test Exercises* when planning or conducting penetration tests.  Findings are captured in cloud.gov’s POAM and tracked to remediation. |

#### CA-8 (1) Control Enhancement (M) (H)

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

| CA-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: GSA Information Security, 3PAO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-8 (1) What is the solution and how is it implemented? |
| --- |
| GSA Information Security performs penetration testing of all 18F systems that are in the purview of GSA. Additionally, upon request or once per year, an independent third-party assessor (3PAO) will perform penetration testing for the cloud.gov platform. |

### CA-9 Internal System Connections (L) (M) (H)

The organization:

1. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and
2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

| CA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Parameter CA-9(a): cloud.gov system components | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The cloud.gov System Owner and Cloud Operations authorize cloud.gov internal connections by agreeing upon the network and logical architecture of cloud.gov. This architecture is codified in Terraform “infrastructure as code” templates, and they go through cloud.gov GitHub approval processes. |
| Part b | All cloud.gov internal connections are documented within the *Dataflow* and *Ports, Protocols, Service* sections. |

## Configuration Management (CM)

### CM-1 Configuration Management Policies and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
2. Reviews and updates the current:
   1. Configuration management policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Configuration management procedures [FedRAMP Assignment: at least annually].

| CM-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter CM-1(a): cloud.gov development and design team | |
| Parameter CM-1(b)(1): At least every 3 years | |
| Parameter CM-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CM-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/CM-Policy.md> for the Configuration Management procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### CM-2 Baseline Configuration (L) (M) (H)

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

| CM-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-2 What is the solution and how is it implemented? |
| --- |
| **All Configurations**  Cloud Operations checks all configurations into 18F GitHub repositories, as well as local git repositories on their GSA-issued laptops, in order to ensure distributed version control and availability of all configurations.  The configuration of cloud.gov is controlled in multiple layers.  **AWS**   * Cloud Operations deploys Concourse ( <https://concourse-ci.org/index.html> ), a continuous integration and deployment pipeline tool, into AWS. cloud.gov's Concourse instance ensures all integration tests are run successfully as further resources and systems are deployed, and it checks if deployment pipelines are successful. * Cloud Operations deploy Terraform ( <https://www.terraform.io/> ) configuration files which bootstrap the initial infrastructure in AWS and manage the configuration of all infrastructure environments (development, staging, tooling, production) at all times. Running automated Terraform scripts via Concourse ensures the state of all initial resources in AWS (EC2, ELBs, S3, RDS, VPCs) are known ahead of time, and the desired state is achieved reliably.   **cloud.gov**  cloud.gov uses Ubuntu, a Debian-based Linux distribution, as its Amazon Machine Instance (AMI) baseline. These AMIs are then the baseline forming the configuration of the operating system (OS) for all EC2 instances in the cloud.gov system.   * Cloud Operations is responsible for 18F's Ubuntu Linux BOSH release, a versioned collection of configuration properties, configuration templates, start up scripts, and source code, required to reproducibly build an Ubuntu AMI according to the 18F/GSA baseline. 18F/GSA's Ubuntu baseline is based on the Center for Internet Security's (CIS) Level 1 benchmark, GSA hardening guidelines, and other configurations necessary for a cloud deployment. * The customized BOSH release itself is deployed onto an Ubuntu "stemcell - a versioned Operating System (OS) image wrapped with IaaS [infrastructure as a service] specific packaging." ( <http://bosh.io/docs/stemcell.html> ) * 18F's BOSH release ensures that cloud.gov:   + Captures all needed configuration options and scripts for deploying Ubuntu   + Records, versions, and keeps track of all dependencies   + Creates a release that can be IaaS agnostic   + Creates a release that is self-contained and *does not* require calling out to resources on the internet for deployment |

#### CM-2 (1) Control Enhancement (M)

The organization reviews and updates the baseline configuration of the information system:

1. [FedRAMP Assignment: at least annually];
2. When required due to [FedRAMP Assignment: to include when directed by the JAB]; and
3. As an integral part of information system component installations and upgrades.

| CM-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Parameter CM-2(1)(a): at least annually | |
| Parameter CM-2(1)(b): to include when directed by the JAB | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-2 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Owner and Cloud Operations review baseline configuration changes at a minimum on an annual basis, and on an as needed basis as a result of any significant change that impacts risk to the system, security audits, or industry guidance. |
| Part b | The System Owner and Cloud Operations review and update the baseline configuration of the information system when required by the FedRAMP JAB.  As referred to in part a, examples of “significant changes” include (but are not limited to):   * Multiple required changes occurring simultaneously * Changes that impact/modify security settings * Major component additions and/or upgrades   The System Owner will put such changes through the 18F Configuration Management Process ( <https://cloud.gov/docs/ops/configuration-management/> ), present them to the FedRAMP assigned ISSO, and if applicable, submit them to the JAB for review, to vet acceptability and to ensure ongoing acceptance of security control implementation(s). |
| Part c | The System Owner and Cloud Operations review all baseline configurations when there is a significant change to the cloud.gov system architecture or when its components undergo installation or upgrades. |

#### CM-2 (2) Control Enhancement (M) (H)

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

| CM-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-2 (2) What is the solution and how is it implemented? |
| --- |
| Terraform and BOSH together ensure a reproducible environment for both AWS and cloud.gov components.  **AWS - Terraform:**  All Terraform scripts are fully automated, and they are themselves automatically controlled and run via Concourse. The configuration of all AWS resources is ensured to be up-to-date by Cloud Operations re-running the Concourse "job" ( <https://concourse.ci/jobs.html> ) whenever there are applicable updates to any software components of cloud.gov. Automated Concourse integration tests ensure the Terraform scripts accurately instantiate all AWS resources.  The Terraform configuration baselines themselves are made readily and highly available by being stored in 18F's GitHub repositories and on local git repositories on the GSA-issued laptops of the Cloud Operations team.  **cloud.gov - BOSH:**  BOSH requires the Cloud Operations team to maintain an accurate, up-to-date, and complete baseline configuration. Steps from stored configuration to deployment:   1. BOSH releases are built by Concourse, based on baseline configuration files (stored in 18F GitHub repositories and on local git repositories on the GSA-issued laptops of the Cloud Operations team) and encrypted cloud.gov secrets stored in a private S3 bucket. The BOSH releases are stored in an S3 bucket for later deployment into the environment. 2. A set of Concourse pipelines listen for new BOSH releases. When a new BOSH release is built, this triggers a build in the deployment pipeline in Concourse. The deployment pipeline uploads a new manifest (including new stemcells and releases) describing the target state to the BOSH Director component. 3. The BOSH Director makes changes in the environment to match the target state, including provisioning new VMs and retiring old ones. |

#### CM-2 (3) Control Enhancement (M)

The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.

| CM-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter CM-2(3): all previous versions | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-2 (3) What is the solution and how is it implemented? |
| --- |
| As described in CM-3(e), all previous baseline configurations are stored in 18F GitHub and git repositories. The System Owner or Cloud Operations can roll back the system to a known-good baseline by retrieving and deploying prior versions of manifests from the GitHub repository or a git repository. |

#### CM-2 (7) Control Enhancement (M) (H)

The organization:

1. Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and
2. Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.

| CM-2 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: GSA Information Security | |
| Parameter CM-2(7) (a)-1: loaner devices | |
| Parameter CM-2(7) (a)-2: appropriate configuration | |
| Parameter CM-2(7) (b): wiped | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-2 (7) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | See the attached *GSA IT Security Policy (GSA Order CIO 2100.1J CHGE 1)*.  Page 52-53 explains GSA's "International travel policy for Portable Electronic Devices (PED)".  This includes:   * “GFE must not be taken on international travel without prior approval from the individual’s supervisor and OMA.” (GFE stands for “Government Furnished Equipment”.) * “GSA employees (with the exception of the OIG employees) that hold a National Security clearance, and at the discretion of OMA, shall be issued loaner devices by GSA IT when traveling outside the United States or European Union, or any area deemed to have an elevated risk during the period of travel. The loaner devices must be returned to GSA IT immediately upon the employee’s return. These loaner devices shall be wiped immediately by GSA IT to ensure no data remains resident on the system(s) issued. Due to technical security controls in place for all mobile devices (encryption and, mobile device management), personnel in Public Trust positions are not required to follow this provision unless deemed to be required by OMA to provide additional safeguards to data these personnel may access.” |
| Part b | See part a. |

### CM-3 Configuration Change Control (M) (H)

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-3 (e) Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with record retention policies and procedures.

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 [FedRAMP Assignment: see additional FedRAMP requirements and guidance] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

CM-3 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the JAB/AO.

| CM-3 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Parameter CM-3(e): forever | |
| Parameter CM-3(g)-1: FedRAMP and agency level configuration management policies | |
| Parameter CM-3(g)-2: Continuously as part of our development lifecycle (during developing and reviewing each significant change), with a quarterly review | |
| Parameter CM-3(g)-3: Defined configuration change conditions | |
| Parameter CM-3(g)-4: Posted within the GitHub repository and in local git repositories | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All changes to the system are under configuration management control.  **AWS**  Terraform ensures the complete state of the AWS environment is always under configuration management control.  **cloud.gov**  All changes to all cloud.gov components are captured within git and GitHub before deployment. Within git or GitHub, built-in *diff* functions compare and contrast any previous or proposed changes to the entirety of the configuration and code of cloud.gov. |
| Part b | 1. The System Owner and Cloud Operations review proposed configuration-controlled changes to all of its information systems and infrastructure and approves or disapproves such changes with explicit consideration for security impact analysis within the AWS and cloud.gov environments. All changes are documented. All system change requests and approvals from Cloud Operations, the System Owner, or the Program Manager are tracked in 18F GitHub repositories. 2. Security impact analysis is always performed and includes a documentation review and automated testing and analysis before the change is implemented in the cloud.gov production environment. The automated tests are “smoke tests” and integration tests that check whether the changes would break any aspect of the system. 3. When proposed changes are due to updates to upstream open source components, the System Owner and Cloud Operations team review the reports generated by the procedures described in SI-3 and perform code review to determine when upstream changes should trigger a full security impact analysis of the system. If it is determined this is required, the impact analysis is performed and managed following the same process as an internal change to the system would require. 4. After any analysis deemed required, upstream changes are deployed to an isolated test environment, and test suites are automatically executed to ensure the change does not cause any unexpected behavior in the system (“smoke tests” / integration tests). Once these tests have completed successfully, Cloud Operations also manually reviews the environment to ensure it is actually working as expected before approving the change to production. 5. The test environment mirrors production and implements all controls described in this SSP. If any CVEs were intentionally or accidentally injected into the upstream code, the scanning systems documented in RA and SI will detect the CVEs and notify Cloud Operations who would then ensure these changes are not promoted to production, and they would revert the test environment to a known good state as described in CM-8. |
| Part c | All configuration change decisions are documented as pull requests (requests for change) to protected branches in 18F GitHub repositories which must be reviewed and accepted by the Program Manager or Cloud Operations. Each repository maintains a full history of change requests including the change requester, approver, and any relevant discussion that contributed to the decision. |
| Part d | When configuration changes have been approved via GitHub pull request, the Cloud Operations team is responsible for implementation and close out of any related story cards. |
| Part e | Records of all configuration-controlled changes are retained forever within 18F git and GitHub repositories, and hashed for uniqueness. |
| Part f | The Cloud Operations team, with the assistance of the Program Manager, conducts a quarterly review of security-related team processes, including configuration control processes, and how to improve them. |
| Part g | During the quarterly review plan, the System Owner and Cloud Operations ensure that the system security plan is aligned with all required controls, policies, and procedures in GSA plans.  The cloud.gov team conducts a biweekly team meeting to review changes we've implemented during the past two weeks and changes we plan to complete soon (“sprint review”), and we communicate major changes to customers by email, the Updates page on our website, and our Status page. |

### CM-4 Security Impact Analysis (L) (M) (H)

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

| CM-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-4 What is the solution and how is it implemented? |
| --- |
| The cloud.gov team analyzes proposed changes to the production components to determine potential security impacts prior to change implementation. A security impact analysis is required to be completed by the change originator and reviewed by the Program Manager and/or Cloud Operations before the work begins. This procedure is one of many tollgates required for any change to be released to production.  Our entire delivery process can be reviewed in the cloud.gov Delivery Process document ( <https://github.com/18F/cg-product/blob/master/DeliveryProcess.md> ). The specific security impact analysis step is in the "grooming" section at <https://github.com/18F/cg-product/blob/master/DeliveryProcess.md#grooming> - this means that before the task can move to the "ready" (ready to implement) column, we must have completed this task: "The team has analyzed and documented any potential security impact of the changes proposed by the story." |

### CM-5 Access Restrictions for Change (M) (H)

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

| CM-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, System Owner, Information Systems Security Officer (ISSO), Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-5 What is the solution and how is it implemented? |
| --- |
| The System Owner only allows pre-defined authorized users to make any changes to the cloud.gov environment. The cloud.gov team uses GitHub to document approved access to changes and track changes made to the cloud.gov platform.  The System Owner has restricted write access to configuration repositories to members of the Cloud Operations team, and has enabled GitHub protected branches with required reviews to ensure that all changes undergo a review by another member of the Cloud Operations team before being deployed. (In detail: the System Owner enforces this peer review process by configuring GitHub's built-in feature that allows enforcing a peer review - see <https://help.github.com/articles/about-pull-request-reviews/#required-reviews> for detail about this feature. Only Cloud Operations team members have write access to configuration repositories, so they are the only people who can review changes in those repositories.)  These changes are tracked in the revision history of the GitHub repository and in the GitHub audit log.  The System Owner, or delegated Cloud Operations staff, add or remove designated Cloud Operations team members from the AWS IAM and the Operations UAA Server. Customers and non-privileged team members do not have access to AWS IAM or the Operations UAA Server.  **Inherited Control**  Physical access to cloud.gov is controlled at AWS GovCloud level. |

#### CM-5 (1) Control Enhancement (M) (H)

The information system enforces access restrictions and supports auditing of the enforcement actions.

| CM-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-5 (1) What is the solution and how is it implemented? |
| --- |
| All changes to the cloud.gov platform are performed using the BOSH CLI and Concourse. Only the Cloud Operations team have access to BOSH to implement configuration changes to the information system. cloud.gov provides an audit trail through the BOSH tasks command. This command shows all actions that an operator has taken with the platform.  The cloud.gov PaaS uses Role Based Access Controls (RBAC) for enforcement. Additionally, the system sends Cloud Foundry component logs to a Logstash syslog server using the *syslog\_daemon\_config* property in the *metron\_agent* job of *cf-release*. For end users, cloud.gov records an audit trail of all relevant API invocations of an app. The CLI command *cf events* returns this information. |

#### CM-5 (3) Control Enhancement (M) (H)

The information system prevents the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

CM-5 (3) Additional FedRAMP Requirements and Guidance:

Guidance: If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be used.

| CM-5 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter CM-5(3): defined software and firmware components | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-5 (3) What is the solution and how is it implemented? |
| --- |
| cloud.gov prevents the installation of software without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. cloud.gov is deployed using a custom manifest file that only has the required software components and configuration settings implemented for use within the production environment.  All of the component YAML files of cloud.gov are stored in 18F GitHub repositories. When a cloud.gov team member commits a file into a repository, Git calculates a hash of the contents of the file. When the files are later retrieved, Git verifies that the hash of the data being retrieved exactly matches the hash that was computed when it was stored. In this fashion, the hash serves as an integrity checksum, ensuring that the data has not been corrupted or altered.  When Concourse deploys changes to the environment from manifests stored in GitHub repositories, it deploys a specific set of changes by referring to the hashes described above. This ensures that the changes were not modified after approval, and that the exact set of changes is deployed. |

#### CM-5 (5) Control Enhancement (M) (H)

The organization:

1. Limits privileges to change information system components and system-related information within a production or operational environment; and
2. Reviews and reevaluates privileges [FedRAMP Assignment: at least quarterly].

| CM-5 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter CM-5(5)(b): At least quarterly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-5 (5) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Owner limits configuration change privileges to the Cloud Operations team. Only Cloud Operations team members receive access privileges that allow them to make changes to the cloud.gov information.  The System Owner, or delegated Cloud Operations staff, add or remove designated Cloud Operations team members from the AWS IAM or the Operations UAA Server. |
| Part b | The Program Manager, System Owner, and Cloud Operations meet on a quarterly basis to review and confirm that all members of the Cloud Operations team still require that level of access.  Any changes made to the Cloud Operations team during this review, or at any other time, are automatically in the audit logs of AWS IAM and the Operations UAA server. |

### CM-6 Configuration Settings (L) (M) (H)

The organization:

1. Establishes and documents configuration settings for information technology products employed within the information system using [FedRAMP Assignment: see CM-6(a) Additional FedRAMP Requirements and Guidance] that reflect the most restrictive mode consistent with operational requirements;

CM-6(a) Additional FedRAMP Requirements and Guidance:

Requirement 1: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available. If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

Requirement 2: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) (<http://scap.nist.gov/>) validated or SCAP compatible (if validated checklists are not available).

Guidance: Information on the USGCB checklists can be found at: <http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc>.

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

| CM-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, System Owner, Information Systems Security Officer (ISSO) | |
| Parameter CM-6(a)-1: see CM-6(a) Additional FedRAMP Requirements and Guidance | |
| Parameter CM-6(a)-2: Center for Internet Security Level 1 controls | |
| Parameter CM-6(c)-1: all | |
| Parameter CM-6(c)-2: System Owner approval | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **AWS**  Cloud Operations follows all relevant AWS security best practices (<https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf> ), especially in regards to the IAM configuration (<http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> ). Given the rapid deployment of features from AWS, Cloud Operations stays up to date on current best practices by consulting <https://aws.amazon.com/security/>.  **cloud.gov**  Cloud Operations follows the applicable Center for Internet Security Level 1 controls for the LTS version of Ubuntu selected by the System Owner. (<https://benchmarks.cisecurity.org/downloads/browse/?category=benchmarks.os.linux.ubuntu> )  Where applicable, Cloud Operations then applies configurations from the FISMA Ready GitHub org ( <https://github.com/fisma-ready> ).  For all other components where either the community or the United States Government Configuration Baseline ( <https://usgcb.nist.gov/index.html> ) is silent on a component used by cloud.gov, or there is no Security Technical Implementation Guide (STIG), the technical experts in Cloud Operations instrument the component with the most restrictive configuration settings possible that are in accordance with any applicable policies or procedures. All configurations can be found in <https://github.com/18F/cg-provision> and the various components listed in 18F’s GitHub repositories prefixed with “cg” ( <https://github.com/18F?utf8=%E2%9C%93&query=cg-> ). |
| Part b | cloud.gov implements the configuration settings through configuration files and code (see <https://github.com/18F/cg-provision> ), enforced by policy (see <https://cloud.gov/docs/ops/configuration-management/> ). |
| Part c | Cloud Operations documents any exceptions to established baseline configurations for all of cloud.gov’s systems and components. The Program Manager maintains a list of exceptions as “stories” in the cloud.gov backlog and reviews them with the System Owner and Cloud Operations at least quarterly to ensure all exceptions are still warranted.  If cloud.gov requires configuration changes not in line with FedRAMP requirements, the cloud.gov team follows the FedRAMP process of formally documenting operational requirements. |
| Part d | Any change to the configuration settings require a pull requests to protected branches and a review (approval) by the System Owner or a Cloud Operations team member before being integrated. Changes to configuration settings are verified by the same cryptographic hashes as any other change to the system. as described in CM-5(3). The process for deploying these changes is described in CM-3 and CM-6(1). |

#### CM-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system components].

| CM-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter CM-6(1): IaaS (Networking, VMs), OS (stemcells), and application configurations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-6 (1) What is the solution and how is it implemented? |
| --- |
| The cloud.gov team configuration management process consists of GitHub, BOSH ( <https://bosh.cloudfoundry.org/> ) and Concourse, which all include automated mechanisms that support consistent configuration management. Controls include:   * Baselines and configuration files are centrally stored in git and GitHub repositories. These files are then deployed using a pipeline file within the Concourse continuous integration platform. * Concourse does not allow any configuration to be deployed outside of version control. * Builds run inside their own containers so that installing packages on the build machine doesn't pollute other builds. * The cloud.gov team uses BOSH for lifecycle management and monitoring of distributed systems. BOSH allows the team easily version, package and deploy software in a reproducible manner.   See <https://github.com/18F/cg-provision> for additional details. |

### CM-7 Least Functionality (L) (M) (H)

The organization:

1. Configures the information system to provide only essential capabilities; and
2. Prohibits or restricts the use of the following functions, ports, protocols, and/or services [FedRAMP Assignment: United States Government Configuration Baseline (USGCB)]

CM-7 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

Guidance: Information on the USGCB checklists can be found at: <http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc>

Partially derived from AC-17 (8).

| CM-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Officer (ISSO), Cloud Operations | |
| Parameter CM-7(b): Prohibits all connections from the Internet except: Port 443, Port 80 (only for redirects to 443) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud 6/21/2016, | |

| CM-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Section 10.8 “Ports, Protocols, and Services” within this SSP lists the Ports, Protocols, and Services enabled for the cloud.gov information system. Based on the “deny all, permit by exception” perspective, Cloud Operations configures cloud.gov to provide only essential capabilities and specifically prohibits all connections from the Internet except: Port 443, Port 80 (only for redirects to 443). This serves as a “white list” methodology for least functionality management. |
| Part b | Cloud Operations restricts services that are not required for operational purposes by either uninstalling the service or otherwise disabling the service. All other physical and logical ports and protocols are disabled since they are unused or unnecessary.  cloud.gov utilizes network scanning tools and intrusion detection and prevention systems to identify and prevent the use of prohibited functions, ports, protocols, and services on the internal network.  Overall, cloud.gov uses the FISMA Ready guidelines for Ubuntu ( <https://github.com/fisma-ready/ubuntu-lts> ), which integrate Center for Internet Security guidelines. |

#### CM-7 (1) Control Enhancement (M) (H)

The organization:

1. Reviews the information system [FedRAMP Assignment: at least Monthly] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
2. Disables [Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure].

| CM-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Officer (ISSO), Cloud Operations, 3PAO | |
| Parameter CM-7(1)(a): at least Monthly | |
| Parameter CM-7(1)(b): unnecessary and non-secure functions, ports, protocols and services | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-7 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The cloud.gov team monitors the information system on an ongoing basis to identify and eliminate any unnecessary functions, ports, protocols and services.  Monitoring is accomplished by reviewing AWS Security Groups. 18F also contracts with a 3PAO to perform penetration tests. 18F and GSA Information security perform monthly internal vulnerability assessments on all components, test procedures, and measure the impact of vulnerabilities. |
| Part b | Cloud Operations disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure when these components are detected by continuous monitoring and during monthly reviews of compliance and vulnerability reports produced by GSA Information Security. |

#### CM-7 (2) Control Enhancement (M) (H)

The information system prevents program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].

CM-7(2) Additional FedRAMP Requirements and Guidance:

Guidance: This control shall be implemented in a technical manner on the information system to only allow programs to run that adhere to the policy (i.e., white listing). This control is not to be based off of strictly written policy on what is allowed or not allowed to run.

| CM-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter CM-7(2): operational requirements and customer terms of use | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-7 (2) What is the solution and how is it implemented? |
| --- |
| In order to secure the system, cloud.gov sandboxes each customer application using containers and fine-grained access control, to ensure one customer's application cannot impact another customer or the platform itself.  Additionally, as described in CM-6, the underlying platform is hardened to FISMA specifications which include setting the *noexec* flag on all mount points where code should not be executed, thus preventing code execution in the case of a sandbox escape. If an attacker manages to deploy an executable program to privileged areas of the filesystem not protected by *noexec*, Tripwire would detect this intrusion and alert Cloud Operations as described in SI-4. Cloud Operations implements this hardening with a BOSH release that runs on all deployed hosts on AWS GovCloud.  **Customer Responsibility**  Application System Owners are responsible for ensuring that their customer applications comply with the cloud.gov Rules of Behavior (“Use your account responsibly” on <https://cloud.gov/docs/getting-started/accounts/> ) and all applicable federal and agency laws and policies. |

#### CM-7 (5) Control Enhancement (M)

The organization:

1. Identifies [Assignment: organization-defined software programs authorized to execute on the information system];
2. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and
3. Reviews and updates the list of authorized software programs [FedRAMP Assignment: at least annually or when there is a change].

| CM-7 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Parameter CM-7(5)(a): All cloud.gov-managed BOSH releases. | |
| Parameter CM-7(5)(c): at least annually or when there is a change | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-7 (5) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Any software to be authorized for use as part of the cloud.gov PaaS must get approval from the System Owner and must go through the cloud.gov development and staging process before getting placed on the production network as described in the cloud.gov Configuration Management plan ( <https://cloud.gov/docs/ops/configuration-management/> ).  **Customer Responsibility**  Application System Owners are responsible for identifying the software programs allowed to execute within their application spaces. |
| Part b | cloud.gov uses BOSH (as described in CM-2) to manage all installed software programs in the environment. BOSH releases are cryptographically hashed when compiled and that hash is verified by BOSH before deploying a release. This prevents any unauthorized applications from being deployed (and thus executed) to cloud.gov. Once a BOSH release has been deployed, Tripwire (as described in SI-4) is used to provided additional verification that all programs installed on the platform by comparing cryptographic checksums of all installed programs to the known good baseline configuration.  **Customer Responsibility**  Application System Owners are responsible for managing authorized software within their application spaces. |
| Part c | Cloud Operations and the ISSOs review and update the list of authorized software programs at least annually or whenever there is a change to the information system.  **Customer Responsibility**  Application System Owners are responsible for managing authorized software within their application spaces. |

### CM-8 Information System Component Inventory (L) (M) (H)

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
2. Reviews and updates the information system component inventory [FedRAMP Assignment: at least monthly].

CM-8 Additional FedRAMP Requirements and Guidance:

Requirement: Must be provided at least monthly or when there is a change.

| CM-8 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Cloud Operations | |
| Parameter CM-8(a)(4): defined information system components for accountability | |
| Parameter CM-8(b): at least monthly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | AWS Information System Component Inventory documentation:   * AWS built-in features automatically provide an accurate, real-time inventory of all system components within the customer account and provides a single view to the granularity of each AWS product, service or compute/networking node, along with all associated configuration information. * AWS Config provides a detailed inventory of all cloud.gov AWS resources and their current configuration, and continuously records configuration changes (e.g., the value of tags on Amazon EC2 instances, ingress/egress rules of security groups, and Network ACL rules for VPCs). It can export a complete inventory of AWS resources with all configuration details, determine how a resource was configured at any point in time, and get notified via Amazon SNS when the configuration of a resource changes. * AWS Config provides configuration snapshots, which is a point-in-time capture of all resources and their configurations. Configuration snapshots are generated on demand via the AWS CLI, or API, and delivered to an Amazon S3 bucket that is specified. * BOSH continuously maintains inventory of all instances and configurations. |
| Part b | Review and update information system component inventory:   * AWS built-in features automatically provide an accurate, near real-time inventory of all AWS system components within the customer account. The AWS management console and AWS API calls provide the capability for the organization to review the inventory. * Cloud Operations reviews and updates the information system component inventory on a monthly basis. * Cloud Operations updates the inventory of information system whenever installations, removals, and other changes are made. * Cloud Operations verifies all components within the authorized boundary of the information system are either inventoried as part of the system or recognized by another system as a component within that system. |

#### CM-8 (1) Control Enhancement (M) (H)

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

| CM-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-8 (1) What is the solution and how is it implemented? |
| --- |
| The Cloud Operations team updates the cloud.gov system components as an integral part of component installations, removals, and information system updates. The team regularly reviews these GitHub repositories to identify updates to Cloud Foundry components:  <https://github.com/cloudfoundry/cli/releases>  [https://github.com/cloudfoundry-community/BOSH-cloudfoundry](https://github.com/cloudfoundry-community/bosh-cloudfoundry)    If there are components to update, remove or test, Cloud Operations follows the update procedures listed here: <https://cloud.gov/docs/ops/updating-cf/>  Additionally, the list of open source components that the system depends upon is reviewed quarterly by the System Owner and Cloud Operations to ensure that:   * The component is still required. * The component is being actively maintained, or if not, it can be supported by Cloud Operations on a go-forward basis. * The component is still acceptable under the current open source policies. |

#### CM-8 (3) Control Enhancement (M) (H)

The organization:

1. Employs automated mechanisms [FedRAMP Assignment: Continuously, using automated mechanisms with a maximum five-minute delay in detection] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
2. Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]].

| CM-8 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, GSA Information Security | |
| Parameter CM-8(3)(a): Continuously, using automated mechanisms with a maximum five-minute delay in detection | |
| Parameter CM-8(3)(b): notifies Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-8 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **AWS**  Detection of unauthorized software in underlying AWS GovCloud components (EC2, RDS, etc.) is inherited from and managed by AWS.  Under 18F’s responsibility, Terraform configurations are the approved baseline for all changes to the infrastructure. They provide an automated method to assess the status of an operational infrastructure against an approved baseline, and to return our infrastructure to that baseline should any unauthorized change occur. Concourse is used to run Terraform at regular intervals to ensure the configuration state of all components match their approved baselines.  **cloud.gov**  Known malicious software (viruses, rootkits, malware, etc.) is detected in real-time by ClamAV. Nessus and Tripwire also run at regularly scheduled intervals on all hosts. |
| Part b | If an automated tool identifies a potential incident (such as an unauthorized component), the tool automatically raises an alert to Cloud Operations via q. Upon receiving the alert, Cloud Operations follows the cloud.gov Security Incident Response Guide ( <https://cloud.gov/docs/ops/security-ir/> ) to investigate and remediate the issue as necessary.  This may include destroying and recreating the affected system components using automated tools that rely on version-controlled manifests. |

#### CM-8 (5) Control Enhancement (M) (H)

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

| CM-8 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-8 (5) What is the solution and how is it implemented? |
| --- |
| The System Owner, Cloud Operations team, and ISSO verify that all components within the authorization boundary of the information system are inventoried in the AWS console, which ensures there are no duplicated components in other information system inventories.  The cloud.gov team uses a dedicated cloud.gov account for AWS resources, separate from other 18F projects, which ensures that the AWS console inventory accurately represents the cloud.gov system.  **Customer Responsibility**  cloud.gov is a Platform as a Service where applications are staged and deployed on top of the platform itself. Customer applications are not part of the cloud.gov authorization boundary, so it is the responsibility of the customer to inventory their own applications appropriately. |

### CM-9 Configuration Management Plan (M) (H)

The organization develops, documents, and implements a configuration management plan for the information system that:

1. Addresses roles, responsibilities, and configuration management processes and procedures;
2. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
3. Defines the configuration items for the information system and places the configuration items under configuration management; and
4. Protects the configuration management plan for unauthorized disclosure and modification.

| CM-9 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The cloud.gov team has developed a Configuration Management Plan for cloud.gov that addresses configuration management processes and procedures, including the specific tools and workflow steps that the team uses for configuration management. This plan is publicly available at <https://cloud.gov/docs/ops/configuration-management/> as part of cloud.gov documentation. |
| Part b | The cloud.gov Configuration Management Plan provides a broad definition of configuration items ("everything needed to run and operate the platform that is not a secret") with several specific examples, so that team members can identify configuration items throughout the system development life cycle. This development lifecycle defines specific tollgates where Cloud Operations must ensure that all relevant items are managed as described by the plan.  These tollgates are documented in our Delivery Process: <https://github.com/18F/cg-product/blob/master/DeliveryProcess.md> (for example, see under “In Progress”: “The deployment must follow our Configuration Management plan. If not possible, a new issue is filed in cg-site to update the plan.”) |
| Part c | The cloud.gov Configuration Management Plan provides a broad definition of configuration items ("everything needed to run and operate the platform that is not a secret") with several specific examples and explains how we manage them. This includes all IaaS (Networking, VMs), OS, and application configurations.  These items are all maintained in a GitHub repositories using protected branches which forbid the unauthorized deletion of revision history and provides the ability to compare and identify differences between releases and who was responsible for them.  Controls have been enabled on these protected branches to ensure that all change requests undergo a review by Cloud Operations before being deployed. In the case of a change being requested by a member of Cloud Operations the control ensures that the review is performed by another member of the team. This prevents a single operator from making unauthorized changes to the system configuration. |
| Part d | The Configuration Management Plan is stored in GitHub as a public open source file (in <https://github.com/18F/cg-site> ). The branch from which the document is generated is a protected branch forbidding the unauthorized deletion of revision history. Moreover, the cloud.gov team has both configured the repository and provided team policies to ensure strict controls on who has authority to approve changes to this guide. |

### CM-10 Software Usage Restrictions (L) (M) (H)

The organization:

1. Uses software and associated documentation in accordance with contract agreements and copyright laws;
2. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
3. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

| CM-10 | Control Summary Information |
| --- | --- |
| Responsible Role: All internal roles, specifically Infrastructure | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All 18F staff always consult contracts and copyright laws before using a software component. Since the majority of cloud.gov is free and open-source, this is only applicable in a handful of cases itemized in the *Services Table* (e.g. Nessus, New Relic, PagerDuty, etc.). |
| Part b | The 18F Infrastructure team tracks the use of all licenses needed to control usage, copying, or distribution. |
| Part c | The cloud.gov platform does not use any peer to peer technology. |

#### CM-10 (1) Control Enhancement (M) (H)

The organization establishes the following restrictions on the use of open source software: [Assignment: organization-defined restrictions].

| CM-10 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Parameter CM-10(1): 18F open source policy | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-10 (1) What is the solution and how is it implemented? |
| --- |
| As part of 18F, cloud.gov follows the 18F open source policy ( <https://github.com/18F/open-source-policy/blob/master/policy.md> ) which requires the use of open source software except when prohibited by specific exceptions ( <https://github.com/18F/open-source-policy/blob/master/policy.md#exceptions> ).  When evaluating new open source components for inclusion in the cloud.gov platform, the System Owner and Cloud Operations team perform an initial review of each component to ensure it meets all documented corporate and system specific requirements for inclusion in the platform.    These include:   * The origin of the component and current maintainers of the component. * The recent development activity of the component; is it frequently updated in response to discovered vulnerabilities / coding best practices? * Are the maintainers known members of the open source community or employees of trusted organizations? * Is the component in use in other high-value systems / by other large organizations known to have a robust security program? * Does the component have a well-defined contribution process and a history of properly vetting contributions from external developers?   All open source code that is used in the system is regularly scanned as described in SI-3.  The list of open source components that the system depends upon is audited on a regular basis as described in CM-8. |

### CM-11 User-Installed Software (M) (H)

The organization:

1. Establishes [Assignment: organization-defined policies] governing the installation of software by users;
2. Enforces software installation policies through [Assignment: organization-defined methods]; and
3. Monitors policy compliance [FedRAMP Assignment: Continuously (via CM-7 (5))].

| CM-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter CM-11(a): GSA IT Security Policy | |
| Parameter CM-11(b): technical measures and management oversight | |
| Parameter CM-11(c): continuously (via CM-7 (5)) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CM-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All software integrated into the cloud.gov system must follow the cloud.gov Configuration Management plan ( <https://cloud.gov/docs/ops/configuration-management/> ) and the GSA IT Security Policy. The cloud.gov Delivery Process ( <https://github.com/18F/cg-product/blob/master/DeliveryProcess.md#definition-of-done> ) also includes requirements along with recommended items.  **Customer Responsibility**  Application System Owners are responsible for establishing policies for software in their orgs, spaces, and apps on cloud.gov. |
| Part b | cloud.gov software installation policies are enforced both by technical measures (such configuring GitHub repositories to require reviews, as explained in the Configuration Management plan) and management oversight from the Program Manager and System Owner. GSA IT also supports enforcement of GSA policies.  **Customer Responsibility**  Application System Owners are responsible for enforcing policies for software in their orgs, spaces, and apps on cloud.gov. |
| Part c | The cloud.gov team, under the direction of the Program Manager and System Owner, continuously monitors cloud.gov for compliance with relevant policies regarding software installation. GSA Information Security also monitors for compliance with GSA policy.  **Customer Responsibility**  Application System Owners are responsible for monitoring policy compliance in their orgs, spaces, and apps on cloud.gov. |

## Contingency Planning (CP)

### CP-1 Contingency Planning Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
2. Reviews and updates the current:
   1. Contingency planning policy [FedRAMP Assignment: at least every three (3) years].; and
   2. Contingency planning procedures [FedRAMP Assignment: at least annually].

| CP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter CP-1(a): cloud.gov development and design team | |
| Parameter CP-1(b)(1): at least every three years | |
| Parameter CP-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/CP-Policy.md> for the Contingency Planning procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### CP-2 Contingency Plan (L) (M) (H)

The organization:

1. Develops a contingency plan for the information system that:
   1. Identifies essential missions and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
   6. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
2. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
3. Coordinates contingency planning activities with incident handling activities;
4. Reviews the contingency plan for the information system [FedRAMP Assignment: at least annually];
5. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
6. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and
7. Protects the contingency plan from unauthorized disclosure and modification.

CP-2 Additional FedRAMP Requirements and Guidance:

Requirement: For JAB authorizations the contingency lists include designated FedRAMP personnel.

| CP-2 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO) | |
| Parameter CP-2(a)(6): System Owner | |
| Parameter CP-2(b): all internal users | |
| Parameter CP-2(d): at least annually | |
| Parameter CP-2(f): all internal users | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | 18F has developed a Contingency Plan for cloud.gov that documents basic contingency requirements for the system, including recovery objectives, restoration priorities, roles, responsibilities, team contact information, and workarounds for maintaining the system even if some aspects are disrupted.  This plan is publicly available in the cloud.gov documentation here: <https://cloud.gov/docs/ops/contingency-plan/> (which is visible to all cloud.gov staff).  This plan addresses the AWS contingency relationship on a platform level. It doesn't address the AWS contingency relationship for customer data since our SLA is lower than the AWS SLA. |
| Part b | Reading this plan is part of the Onboarding Checklist (<https://github.com/18F/cg-product/blob/master/OnboardingChecklist.md> ) when a new person joins the cloud.gov team as an internal user. |
| Part c | The Contingency Plan coordinates with the Incident Response Guide: the supplement links to the Incident Response Guide and explains example situations where an Incident Response process may cause the team to need to activate the Contingency Plan. |
| Part d | The cloud.gov team reviews the Contingency Plan annually. |
| Part e | This Contingency Plan is structured so that it should not easily become inaccurate when ordinary parts of the system or organization change: rather than embedding detailed documentation in the plan itself, it links to documentation that the team already maintains as part of the ordinary operations of cloud.gov.  The cloud.gov team will review and update this Contingency Plan as necessary as the organization, system, and environment change.  cloud.gov team standard practice is to continuously update all documentation (via our GitHub repository and GSA Google Drive) as needed. |
| Part f | All changes to all documents are communicated through GSA Gmail, Slack, meetings, or GitHub notifications as appropriate. |
| Part g | All relevant cloud.gov master GitHub branches are protected ( <https://help.github.com/articles/about-protected-branches/> ), and updates to the canonical version of the plan can only be merged by authorized cloud.gov team members. GSA Google Docs are similarly protected by the appropriate permissions. |

#### CP-2 (1) Control Enhancement (M) (H)

The organization coordinates contingency plan development with organizational elements responsible for related plans.

| CP-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-2 (1) What is the solution and how is it implemented? |
| --- |
| The cloud.gov Contingency Plan includes directions to coordinate with 18F Infrastructure staff, GSA Information Security, and designated FedRAMP personnel.  The Contingency Plan also directs the team to use the cloud.gov Incident Response Guide when appropriate, which includes coordinating with GSA Information Security and their incident response teams. |

#### CP-2 (2) Control Enhancement (M) (H)

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

| CP-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, System Owner, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-2 (2) What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. AWS provides all the excess capacity necessary at cloud.gov’s current scale. |

#### CP-2 (3) Control Enhancement (M) (H)

The organization plans for the resumption of essential missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.

| CP-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter CP-2(3): 3 hours | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-2 (3) What is the solution and how is it implemented? |
| --- |
| See the *Contingency Plan* for our current recovery objective(s): “More than 3 hours of cloud.gov being offline would be unacceptable. Our objective is to recover from any significant problem (disruption, compromise, or failure) within that span of time.” |

#### CP-2 (8) Control Enhancement (M) (H)

The organization identifies critical information system assets supporting essential missions and business functions.

| CP-2 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-2 (8) What is the solution and how is it implemented? |
| --- |
| The cloud.gov *Contingency Plan* identifies services and system components that are critical to supporting the mission and business of cloud.gov. See the attachment and <https://cloud.gov/docs/ops/contingency-plan/> - specifically <https://cloud.gov/docs/ops/contingency-plan/#external-dependencies>. This includes GitHub, PagerDuty, New Relic, GSA SecureAuth, and AWS. |

### CP-3 Contingency Training (L) (M) (H)

The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

1. Within [FedRAMP Assignment: ten (10) days] of assuming a contingency role or responsibility;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| CP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO) | |
| Parameter CP-3(a): ten (10) days | |
| Parameter CP-3(c): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-3 What is the solution and how is it implemented? |
| --- |
| 18F provides contingency training to information system users consistent with assigned roles and responsibilities: within 10 days of assuming a contingency role or responsibility, when required by information system changes and provides contingency training on an annual basis thereafter. |

### CP-4 Contingency Plan Testing (H)

The organization:

1. Tests the contingency plan for the information system [FedRAMP Assignment: at least annually] using [FedRAMP Assignment: functional exercises] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

CP-4(a) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to FedRAMP prior to initiating testing. Test plans are approved and accepted by the JAB/AO prior to initiating testing.

1. Reviews the contingency plan test results; and
2. Initiates corrective actions, if needed.

| CP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Cloud Operations | |
| Parameter CP-4(a)-1: test contingency plan at least annually | |
| Parameter CP-4(a)-2: test using functional exercises for a moderate impact system | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | 18F tests the contingency plan for cloud.gov *on an annual basis* using FedRAMP functional test procedures for a moderate baseline system to determine the effectiveness of the plan and the organizational readiness to execute the plan. |
| Part b | After exercises are completed, the disaster recovery team reviews the exercise results. |
| Part c | After the team reviews the exercise results, they initiate corrective actions if necessary. If a disaster recovery test finding leads to a change to cloud.gov’s IT infrastructure, 18F will require the change to be documented, tested and approved by going through 18F’s change control process. |

#### CP-4 (1) Control Enhancement (M) (H)

The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

| CP-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-4 (1) What is the solution and how is it implemented? |
| --- |
| Prior to testing contingency plans, the cloud.gov team requests approval for test plans from the Authorizing Official.  The cloud.gov team will coordinate testing of contingency plans with individuals that have contingency plan and incident response plan responsibilities, including the cloud.gov Authorizing Official.  The individuals that have contingency plan responsibilities are listed in the plan, which includes:   * cloud.gov Director (System Owner) * cloud.gov Deputy Director * cloud.gov Program Manager * cloud.gov Cloud Operations * 18F leadership * GSA Information Security * FedRAMP JAB representatives |

### CP-6 Alternate Storage Site (M) (H)

The organization:

1. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
2. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

| CP-6 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov leverages AWS GovCloud for its alternate storage site capabilities. This implementation employs the use of multiple Availability Zones within one AWS Region, which constitute a built-in alternate storage site capability for data stored in Amazon S3 and Amazon RDS databases. S3 uses multiple availability zones by default, and RDS databases deployed by this package are replicated across multiple availability zones.  cloud.gov uses the leveraged AWS services for both platform data and customer data. If customers create multiple instances of their applications, cloud.gov automatically schedules those instances across Availability Zones. |
| Part b | Through leveraging the AWS GovCloud, 18F ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site for cloud.gov. The multiple AWS availability zones employed by Amazon S3 storage and Amazon RDS replication provide identical security safeguards. |

#### CP-6 (1) Control Enhancement (M) (H)

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

| CP-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-6 (1) What is the solution and how is it implemented? |
| --- |
| cloud.gov leverages the use of AWS GovCloud. The replication of S3 and RDS databases across Availability Zones within one AWS Region constitutes a built-in multi-storage site capability to automatically mitigate typical network, power, and hardware outages. Optional configuration of storage replication across multiple geographic AWS Regions addresses organizational requirements related to major regional disasters.  cloud.gov uses the leveraged AWS services for both platform data and customer data. If customers create multiple instances of their applications, cloud.gov automatically schedules those instances across Availability Zones. |

#### CP-6 (3) Control Enhancement (M) (H)

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

| CP-6 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-6 (3) What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control.  AWS provides completely separate Availability Zones in the GovCloud region, and cloud.gov uses two of these Availability Zones.  cloud.gov uses the leveraged AWS Availability Zones for both platform data and customer data. If customers create multiple instances of their applications, cloud.gov automatically schedules those instances across Availability Zones. |

### CP-7 Alternate Processing Site (M) (H)

The organization:

1. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [FedRAMP Assignment: see additional FedRAMP requirements and guidance] when the primary processing capabilities are unavailable;

CP-7a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

1. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
2. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

| CP-7 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM), Cloud Operations | |
| Parameter CP-7(a)-1: Inherited from pre-existing Provisional Authorization | |
| Parameter CP-7(a)-2: Inherited from pre-existing Provisional Authorization | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov leverages the established alternate processing sites within AWS GovCloud including necessary agreements to permit the transfer and resumption of cloud.gov *operations* for essential missions/business functions when the primary processing capabilities are unavailable.  cloud.gov uses the leveraged AWS services for both platform data and customer data. |
| Part b | cloud.gov is leverages AWS GovCloud to implement the use of multiple AWS Availability Zones within one AWS Region which are dynamically in place and available to support resumption of operations. |
| Part c | The use of multiple AWS Availability Zones employed by the AWS GovCloud provides identical security safeguards equivalent to that of the primary site. |

#### CP-7 (1) Control Enhancement (M) (H)

The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

CP-7(1) Additional FedRAMP Requirements and Guidance

Guidance: The service provider may determine what is considered a sufficient degree of separation between the primary and alternate processing sites, based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites will be less relevant.

| CP-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM), Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-7 (1) What is the solution and how is it implemented? |
| --- |
| 18F and cloud.gov leverages the replication of EC2 and RDS instances across Availability Zones in conjunction with Elastic Load Balancing constitutes a built-in multi-processing site capability to automatically mitigate typical network, power, and hardware outages.  cloud.gov uses the leveraged AWS services for both platform data and customer data. |

#### CP-7 (2) Control Enhancement (M) (H)

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

| CP-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-7 (2) What is the solution and how is it implemented? |
| --- |
| 18F and cloud.gov will leverage AWS Availability Zones and Regions. AWS console and remote API calls can be made from other networks across the public internet, provided the appropriate credentials are supplied.  cloud.gov uses the leveraged AWS services for both platform data and customer data. |

#### CP-7 (3) Control Enhancement (M) (H)

The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

| CP-7 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-7 (3) What is the solution and how is it implemented? |
| --- |
| 18F and cloud.gov will leverage AWS Availability Zones to include priority of service provisions identical to the others.  cloud.gov uses the leveraged AWS services for both platform data and customer data. |

### CP-8 Telecommunications Services (M) (H)

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information system operations] for essential missions and business functions within [FedRAMP Assignment: See CP-8 additional FedRAMP requirements and guidance] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

CP-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

| CP-8 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Parameter CP-8-1: resumption of cloud.gov operations | |
| Parameter CP-8-2 Inherited from the Infrastructure as a Service provider | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-8 What is the solution and how is it implemented? |
| --- |
| To permit the resumption of information system operations for essential missions and business functions without impact to consumers/customers, 18F has provisioned and leveraged redundant, always-on, internet connections through AWS GovCloud. 18F has accepted the AWS service agreement to provide always-on internet connections which assure continuous service. |

#### CP-8 (1) Control Enhancement (M) (H)

The organization:

1. Develops primary and alternate telecommunications service agreements that contain priority- of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and
2. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

| CP-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | 18F has provisioned and leveraged redundant, primary and alternate telecommunications always-on, internet connections through AWS GovCloud. 18F has accepted the AWS service agreement to provide always-on internet connections which assure continuous service. |
| Part b | 18F does not require telecommunications services used for national security emergency preparedness. |

#### CP-8 (2) Control Enhancement (M) (H)

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

| CP-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-8 (2) What is the solution and how is it implemented? |
| --- |
| 18F has provisioned and leveraged redundant, primary and alternate telecommunications always-on, internet connections through AWS GovCloud. 18F has accepted the AWS service agreement to provide always-on internet connections which assure continuous service. |

### CP-9 Information System Backup (L) (M) (H)

The organization:

CP-9 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine what elements of the cloud environment require the Information System Backup control. The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check.

1. Conducts backups of user-level information contained in the information system [FedRAMP Assignment: daily incremental; weekly full]

CP-9 (a) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online).

1. Conducts backups of system-level information contained in the information system [FedRAMP Assignment: daily incremental; weekly full];

CP-9 (b) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online).

1. Conducts backups of information system documentation including security-related documentation [FedRAMP Assignment: daily incremental; weekly full ]; and

CP-9 (c) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online).

1. Protects the confidentiality, integrity, and availability of backup information at storage locations.

| CP-9 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Program Manager | |
| Parameter CP-9(a): daily incremental; weekly full | |
| Parameter CP-9(b): daily incremental; weekly full | |
| Parameter CP-9(c): daily incremental; weekly full | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Customers are responsible for backups of their own application data, either within AWS GovCloud, or to other systems outside of cloud.gov.  The cloud.gov team retains business/account metadata about customers, such as digital copies of inter-agency agreements (IAAs), statements-of-work (SOWs), memoranda of understanding (MOUs) and associated billing information, as GSA Google Drive documents that have backups handled by the GSA Google Drive system. |
| Part b | Customers are responsible for backups, either within AWS GovCloud, or to other systems outside of cloud.gov.  All versions of cloud.gov system code, configuration, and documentation files are primarily stored in git repositories hosted in GitHub. As part of routine work with these git repositories, Cloud Operations and other cloud.gov team members check out (download) copies of the latest code files to their local systems (laptops). These local copies also serve as backups of the GitHub-hosted files. The cloud.gov Contingency Plan uses these local backups if GitHub is not available (see the GitHub section of the Contingency Plan). |
| Part c | Customers are responsible for backups, either within AWS GovCloud, or to other systems outside of cloud.gov. |
| Part d | Customers are responsible for backups, either within AWS GovCloud, or to other systems outside of cloud.gov. |

#### CP-9 (1) Control Enhancement (M)

The organization tests backup information [FedRAMP Assignment: at least annually] to verify media reliability and information integrity.

| CP-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO) | |
| Parameter CP-9(1): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-9 (1) What is the solution and how is it implemented? |
| --- |
| Currently, customers are responsible for backups, either within AWS GovCloud, or to other systems outside of cloud.gov.  cloud.gov team business/account metadata is stored as GSA Google Drive documents that have backups handled by the GSA Google Drive system. GSA Google Drive is managed by GSA Information Security. |

#### CP-9 (3) Control Enhancement (M) (H)

The organization stores backup copies of [Assignment: organization-defined critical information system software and other security-related information] in a separate facility or in a fire-rated container that is not collocated with the operational system.

| CP-9 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Parameter CP-9(3): Inherited from the Infrastructure as a Service provider | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-9 (3) What is the solution and how is it implemented? |
| --- |
| cloud.gov utilizes AWS GovCloud as the redundant storage, processing, and backup sites for all 18F systems including its platform as a service cloud. Amazon Web Services (AWS) handles durability, availability and monitoring of regional and global services. |

### CP-10 Information System Recovery and Reconstitution (L) (M) (H)

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

| CP-10 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-10 What is the solution and how is it implemented? |
| --- |
| See CP-1 and CP-2. All of cloud.gov’s components and infrastructure are represented as code, are maintained in a distributed version control system, and are instantiated via automated mechanisms. Every deploy of cloud.gov, whether in response to an incident or not, is to a “known state”. |

#### CP-10 (2) Control Enhancement (M) (H)

The information system implements transaction recovery for systems that are transaction-based.

| CP-10 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| CP-10 (2) What is the solution and how is it implemented? |
| --- |
| cloud.gov implements the goal of transaction recovery by using modern infrastructure-as-code and database high availability methodologies.  cloud.gov manages infrastructure configuration in version control and deploys it via Concourse; each deployment can be considered a transaction. Cloud Operations can roll back a deployment by deploying a previous known-good version, since all versions are retained in version control.  The AWS services that cloud.gov uses, such as the Relational Database Service, have built-in resiliency instead of requiring implementation of specific transaction recovery features. |

## Identification and Authentication (IA)

### IA-1 Identification and Authentication Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
2. Reviews and updates the current:
   1. Identification and authentication policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Identification and authentication procedures [FedRAMP Assignment: at least annually].

| IA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owners | |
| Parameter IA-1(a): cloud.gov development and design team | |
| Parameter IA-1(a): At least every three years | |
| Parameter IA-1(b)(1): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| IA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/IA-Policy.md> for the Identification and Authentication procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### IA-2 User Identification and Authentication (L) (M) (H)

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

| IA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-2 What is the solution and how is it implemented? |
| --- |
| GSA and 18F are in full compliance with Homeland Security Presidential Directive 12 (HSPD-12). Personal identity verification (PIV) cards are issued for all internal users, in accordance with HSPD-12. The existence of a valid PIV card, an official GSA email address, and access to GSA SecureAuth are checked before accounts are created.  **AWS**  AWS IAM accounts are only granted by the System Owner or Cloud Operations after a PIV card has been successfully provisioned. See IA-5 part a, for more information.  **cloud.gov**  GSA SecureAuth authentication must also be successful upon any subsequent request for an authenticated session to any UAA server. |

#### IA-2 (1) Control Enhancement (L) (M) (H)

The information system implements multifactor authentication for network access to privileged accounts.

| IA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-2 (1) What is the solution and how is it implemented? |
| --- |
| **AWS**  AWS multi-factor Authentication (MFA) for privileged IAM users of the AWS Management Console is implemented using mobile device authenticator apps, such as Google Authenticator, Duo, or Authy. MFA is required for all AWS IAM accounts. The mobile device authenticator app is synchronized with AWS IAM via the capture of a QR code. Once the device and AWS IAM are synchronized via the Time-based One Time Passwords (TOTP) method, the QR code is immediately destroyed by AWS.  With MFA enabled, all users are prompted for their username and password, as well as for the authentication code from their MFA device.  **cloud.gov**  To gain access to EC2 instances in production, the System Owner and Cloud Operations first create an ephemeral jumpbox, which is gated by GSA SecureAuth, which requires MFA via either text, automated phone call, or mobile device application token.  **cloud.gov fallback identity provider**  MFA is implemented using mobile device authenticator apps, such as Google Authenticator, Duo, or Authy. The mobile device authenticator app is synchronized with the IDP via the capture of a QR code. Once the device and IDP are synchronized via the Time-based One Time Passwords (TOTP) method, the QR code is immediately destroyed. All users are prompted for their username and password, as well as for the authentication code from their MFA device.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, cloud.gov delegates authentication to customer enterprise identity systems. The customer must implement MFA to that system.  To enable a new federated identity provider, the Cloud Operations team provides the customer agency with a SAML (Security Assertion Markup Language) payload that has to be loaded in the agency's IDP (identity provider). Once that is loaded and an "application" is created, the IDP generates a new SAML payload that is loaded into the cloud.gov system. For additional detail about this integration, see IA-5 (2). |

#### IA-2 (2) Control Enhancement (M) (H)

The information system implements multifactor authentication for network access to non-privileged accounts.

| IA-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-2 (2) What is the solution and how is it implemented? |
| --- |
| cloud.gov enforces the same authentication requirements for privileged and non-privileged accounts. See IA-2 (1) for more details. |

#### IA-2 (3) Control Enhancement (M) (H)

The information system implements multifactor authentication for local access to privileged accounts.

| IA-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-2 (3) What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud, which provides no local access.  For access to privileged accounts in general, cloud.gov implements multifactor authentication. See IA-2 (1) for details. |

#### IA-2 (5) Control Enhancement (M) (H)

The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

| IA-2 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-2 (5) What is the solution and how is it implemented? |
| --- |
| All authentication on the cloud.gov platform relies on individual authentication as described in IA-2 and IA-8(4). cloud.gov does not support group authenticators. |

#### IA-2 (8) Control Enhancement (M) (H)

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

| IA-2 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-2 (8) What is the solution and how is it implemented? |
| --- |
| Replay protection is implemented using unique RelayState values. Additional details on cloud.gov’s SAML configuration can be found in IA-8 (4). |

#### IA-2 (11) Control Enhancement (M) (H)

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [FedRAMP Assignment: FIPS 140-2, NIAP\* Certification, or NSA approval].

\*National Information Assurance Partnership (NIAP)

Additional FedRAMP Requirements and Guidance:

Guidance: PIV = separate device. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials. FIPS 140-2 means validated by the Cryptographic Module Validation Program (CMVP).

| IA-2 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter IA-2(11): varies based on account | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-2 (11) What is the solution and how is it implemented? |
| --- |
| **AWS**  All GSA use of AWS IAM requires MFA, which is a built-in feature of AWS. The MFA password or “token” is generated by a mobile device application per IA-2 (1). Hence, two different systems are involved – AWS IAM and the mobile device application. Further, each system is totally distinct from the system gaining access, which is the user’s client or web browser.  See <https://aws.amazon.com/iam/details/mfa/> and the Provisional Authorization for AWS GovCloud for more detail.  **cloud.gov**  cloud.gov uses GSA SecureAuth to provide MFA for both Client UAA and Operations UAA. See section 10.3 *(“cloud.gov”)* for a description of these two UAA servers.  **Client UAA:** Since the MFA token is generated by GSA SecureAuth itself, and is sent via government email, text, automated phone call, or mobile device application, at least two different systems are involved: cloud.gov, GSA SecureAuth, and the system transmitting the MFA password or “token”. Further, all of the systems are totally distinct from the system gaining access, which is the user’s client or web browser. For internal use of client UAA by the cloud.gov team (such as to log into cloud.gov components run as applications on the cloud.gov platform), the cloud.gov team discourages team use of the email option (preferring the text, phone, or mobile device application options).  **Operations UAA:**This is configured similar to Client UAA. GSA SecureAuth is configured to only provide MFA tokens over government text, automated phone call, or mobile device application (without the email option) for Operations UAA.  GSA Information Security is responsible for continuously assessing the strength of the GSA SecureAuth system in all respects.  **cloud.gov fallback identity provider**  The IDP requires MFA. The MFA password or “token” is generated by a mobile device application per IA-2 (1).  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, cloud.gov delegates authentication to customer enterprise identity systems. It is the responsibility of those systems to appropriately segment their MFA generation and provisioning from the systems that maintain their passwords. |

#### IA-2 (12) Control Enhancement (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

IA-2 (12) Additional FedRAMP Requirements and Guidance:

Guidance: Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12.

| IA-2 (12) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-2 (12) What is the solution and how is it implemented? |
| --- |
| **cloud.gov fallback identity provider**  The cloud.gov IDP does not accept PIV/CAC cards.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, cloud.gov delegates authentication to customer enterprise identity systems. It is the responsibility of those systems to appropriately accept and verify PIV cards.  For details about how cloud.gov integrates customer identity providers, see IA-2 (1). |

### IA-3 Device Identification and Authentication (M) (H)

The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.

| IA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter IA-3-1: VMs and services | |
| Parameter IA-3-2: remote connections | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-3 What is the solution and how is it implemented? |
| --- |
| All cloud.gov network access is configured as “deny all” on first instantiation, and then Cloud Operations configures it to permit limited exceptions based on the requirements for that specific VM. When Cloud Operations grants these exceptions to allow required VMs and services to communicate with each other over the network, they narrowly scope the exceptions with a focus on least functionality. (See CM-7 for further description of restrictions on network access.)  These “allow” exceptions are implemented using AWS Security Groups, which are configured to allow access only to specific ports from specific TCP/IP addresses assigned to the VMs and services that require access. Each VM has an IP address that uniquely identifies it.  The configuration for all security groups are stored in version-controlled manifests and are frequently audited, as described in the CM control statements.  Additionally, these are internal Cloud Foundry components that use unique certificates:   * Loggregator communicates with application containers using a connection secured with certificates (over HTTPS). * UAA communicates with other components using a connection secured with certificates (over HTTPS). * Consul communicates with other components using a connection secured with certificates (over HTTPS). (See SC-22 for details about Consul.) |

### IA-4 Identifier Management (L) (M)

The organization manages information system identifiers for users and devices by:

1. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers for [FedRAMP Assignment: at least two (2) years]; and
5. Disabling the identifier after [FedRAMP Assignment: ninety days for user identifiers (see additional requirements and guidance)]

IA-4e Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines the time period of inactivity for device identifiers.

Guidance: For DoD clouds, see DoD cloud website for specific DoD requirements that go above and beyond FedRAMP http://iase.disa.mil/cloud\_security/Pages/index.aspx.

| IA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter IA-4(a): System Owner | |
| Parameter IA-4(d): identifiers are never reused | |
| Parameter IA-4(e): disable the user identifier after ninety (90) days of inactivity for general user accounts and immediately for administrator level accounts | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Owner grants staff the Cloud Operations role, and the System Owner can delegate to Cloud Operations staff the ability to add and remove users from the Cloud Operations role. Similarly, Cloud Operations is responsible for authorizing all other internal users who need to use the system.  **cloud.gov fallback identity provider**  The IDP only provides identifiers (1) automatically upon request for federal government email addresses, or (2) by invitation from an existing cloud.gov user.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, cloud.gov delegates authentication to customer enterprise identity systems. It is the responsibility of the customer to provide all relevant authorizations, both “to” and “within” cloud.gov. |
| Part b | **AWS**  Cloud Operations creates a unique AWS account for each individual who is authorized to access AWS resources, based on the first part of their official GSA government email address. For example, the user “Alice.Smith” would correspond to “alice.smith@gsa.gov”.  **cloud.gov**  cloud.gov generates a universally unique identifier (UUID) for each individual SAML NameID provided by a trusted Identity Provider (IDP).  The SAML NameID is also called a “username”. GSA SecureAuth is an example of an IDP. For example, in the case of cloud.gov team members, GSA SecureAuth provides the SAML NameID (username), and cloud.gov generates a corresponding UUID to uniquely identify their cloud.gov account.  **cloud.gov fallback identity provider**  The IDP provides the SAML NameID (username), using the email address. |
| Part c | **AWS**  Identifiers are assigned and communicated to staff via email or Slack.  **cloud.gov**  Identifiers are automatically assigned upon logging in to any UAA server.  For example, when a GSA staff member first logs into cloud.gov as a tenant (using GSA SecureAuth), cloud.gov’s UAA server provisions a user account (with a unique identifier) for that staff member. |
| Part d | Identifiers are never reused. Each system generates a unique identifier that permanently identifies the individual associated with the identifier. |
| Part e | **AWS**  When a team member no longer requires access to cloud.gov resources, Cloud Operations immediately disables their AWS account as documented in the cloud.gov Off-boarding Checklist ( <https://github.com/18F/cg-product/blob/master/OffboardingChecklist.md> ). The identifier remains in any and all logs, including CloudTrail.  **cloud.gov**  While all authenticators are disabled, the identifier remains in the system as a UUID, to ensure the accuracy of any records or logs if the user returns to 18F. |

#### IA-4 (4) Control Enhancement (M) (H)

The organization manages individual identifiers by uniquely identifying each individual as [FedRAMP Assignment: contractors; foreign nationals].

| IA-4 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Parameter IA-4(4): contractors; foreign nationals | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-4 (4) What is the solution and how is it implemented? |
| --- |
| All accounts are always uniquely identifiable to a specific individual. Each individual can then be looked up in GSA Google Apps and the GSA Credentialing and Identity Management System (GCIMS) to determine their status as a contractor or foreign national.  **Customer Responsibility**  Customers are responsible for uniquely identifying the contractor and/or foreign national status of each user who has a role in their org or space (see Types of Users table).  For customers who do not use the cloud.gov identity provider, cloud.gov delegates the responsibility of customer identity management to their enterprise identity systems. |

### IA-5 Authenticator Management (L) (M)

The organization manages information system authenticators by:

1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
2. Establishing initial authenticator content for authenticators defined by the organization;
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
5. Changing default content of authenticators prior to information system installation;
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
7. Changing/refreshing authenticators [FedRAMP Assignment: to include sixty (60) days for passwords].
8. Protecting authenticator content from unauthorized disclosure and modification;
9. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
10. Changing authenticators for group/role accounts when membership to those accounts changes.

| IA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, System Owner, Information Security Officer | |
| Parameter IA-5(g): every sixty (60) days for passwords | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **AWS**  The System Owner verifies that internal staff have received their official GSA government email and GSA SecureAuth login (see below) before granting them access to the Cloud Operations role. Cloud Operations, along with the System Owner, have access to “write” abilities to the environment via AWS IAM. Cloud Operations subsequently grants “read-only” AWS IAM access to GSA Information Security, via the same verification method.  **cloud.gov**  All internal staff of 18F (as part of GSA) and GSA receive personal identity verification (PIV) cards from GSA, according to all relevant federal laws, regulations, and policies. The successful provisioning of a GSA PIV card results in internal staff being provisioned their initial GSA SecureAuth username, password, and second factor authenticator (government email address, text, automated phone call, or mobile device application token). GSA SecureAuth is used to authenticate to both the Client and Operations UAA Servers for all 18F and GSA staff.  **cloud.gov fallback identity provider**  The IDP verifies the identity of the email address holder by requiring them to click a confirmation link in their email.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, cloud.gov delegates customer identity verification to their enterprise identity systems. It is the responsibility of those systems to establish identity.  When those systems return identity assertions to cloud.gov, the assertions are encrypted and signed by the customer enterprise identity systems, which cloud.gov verifies as described in IA-8(4). |
| Part b | **AWS**  AWS generates an initial password that meets the requirements defined in part c of this control. The initial password must be changed by the user when they login to the system for the first time. When a password is changed by a user, the system enforces the requirements defined in part c of this control and prevents the user from using weak passwords or passwords that do not comply with 18F and GSA requirements.  **cloud.gov fallback identity provider**  The IDP requires the user to create an authenticator when they log into the system for the first time, which must comply with the requirements in part c.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, it is the responsibility of the customer enterprise identity system to establish authenticator content. |
| Part c | **AWS**  AWS password requirements settings:   * must not be the same as the previous password * must be at least 15 characters * must contain at least one symbol * must contain at least one number * must contain at least one uppercase letter * must contain at least one lowercase letter   **cloud.gov**  Internal users use GSA SecureAuth, which enforces password strength, in addition to the second-factor required for all authenticated sessions. The GSA IT Information Security policy is followed in all respects to password strength and distribution requirements. GSA requires a minimum length of 16 characters.  **cloud.gov fallback identity provider**  The IDP requires authenticators to have the same requirements as AWS but at least 20 characters.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, cloud.gov does not enforce authentication strength for customers, as it delegates authentication to customer enterprise identity systems. It is the responsibility of those systems to establish that authenticators have sufficient strength. |
| Part d | **AWS**  AWS IAM provisioning, if required, is accomplished through the on-boarding checklist: <https://github.com/18F/cg-product/blob/master/OnboardingChecklist.md>.  If AWS IAM accounts or keys are lost or compromised, Cloud Operations is responsible for disabling the lost or compromised credentials and issuing new ones. Revoking access is accomplished per the off-boarding checklist listed below.  **cloud.gov**  All policies and procedures in this regard are managed by GSA Information Security or the GSA SecureAuth system itself, and these policies and procedures are in compliance with all relevant provisions of the *GSA IT Information Security Policy.*  When staff leave, GSA disables their GSA SecureAuth access along with their government email address and any government mobile devices. A staffer who leaves 18F, but not GSA, still has GSA SecureAuth access and therefore access to UAA servers or other external services. As a result, 18F also always follows the off-boarding checklist, as written on the “Leaving 18F” page in the 18F handbook ( <https://handbook.18f.gov/leaving-18f/> ) and in the cloud.gov-specific off-boarding checklist ( <https://github.com/18F/cg-product/blob/master/OffboardingChecklist.md> ) to ensure all accounts are properly deactivated.  cloud.gov does not contain any default passwords that need to be changed during installation. All authenticator content within the environment is randomly generated, as described in the cloud.gov secrets policy ( <https://cloud.gov/docs/ops/secrets/> ). These authenticators (example: credentials to a cloud.gov managed database service such as RDS) are only provided within cloud.gov itself, as environmental variables. If these types of authenticators are compromised (as they cannot, by definition, be physically lost), the customer is responsible for re-deploying the application to which the service authenticator credentials were bound, therefore replacing the compromised credentials with new ones.  **cloud.gov fallback identity provider**  The IDP provides a reset password function for users that requires the user to click links sent to them by email. To reset their MFA token, we require the procedure described here: <https://cloud.gov/docs/getting-started/accounts/#if-you-can-t-access-your-token-codes>  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, cloud.gov delegates authentication to customer enterprise identity systems. It is the responsibility of those systems to distribute, replace, and revoke authenticators.  When those systems revoke authenticators, these authenticators can no longer be used to access cloud.gov as the customer system must authorize all cloud.gov users as described in IA-2. |
| Part e | **AWS**  AWS IAM is set to require that default passwords, or any password issued by an AWS IAM Administrator, need to be changed once the user receiving the password logs in for the first time.  **cloud.gov**  GSA SecureAuth is set to require that default passwords, or any password issued by an GSA SecureAuth Administrator, need to be changed once the user receiving the password logs in for the first time.  **cloud.gov fallback identity provider**  The IDP does not issue a default password. |
| Part f | **AWS**  AWS passwords expire after 60 days, and the user must set a new password before the expiration date. If the expiration date passes, the System Owner or Cloud Operations must manually reset the password. AWS also remembers the last 24 passwords set for any particular IAM user and prevents the re-use of those passwords. (By definition, at least one character needs to be changed in order for a new password to be accepted.)  **cloud.gov**  GSA SecureAuth passwords expire after 90 days, and the user must set a new password before the expiration date. If the expiration date passes, the user must request GSA SecureAuth administrators to manually reset the password. GSA SecureAuth also remembers the last 10 passwords set for any particular user and prevents their re-use. (By definition, at least one character needs to be changed in order for a new password to be accepted.)  **cloud.gov fallback identity provider**  Passwords expire after 90 days. The IDP prevents users from reusing the previous password.  **Customer Responsibility**  It is the responsibility of customer enterprise identity systems to establish authenticator maximum lifetime restrictions and reuse restrictions. |
| Part g | There are no additional conditions on authenticator change or refresh beyond what is above. |
| Part h | 18F policy requires the use of GSA-approved password managers as documented in the 18F Handbook ( <https://handbook.18f.gov/password-requirements/> ).  **cloud.gov fallback identity provider**  All content is encrypted at rest in Client UAA.  **Customer Responsibility**  Connections from cloud.gov to customer enterprise identity systems are protected with TLS to prevent unauthorized disclosure in transit. Otherwise, customers are responsible. |
| Part i | See above for information on encryption, both in transit and in rest, for passwords and multi-factor authenticators.  **Customer Responsibility**  Customers are wholly responsible for this control. |
| Part j | Part j is not applicable.  **AWS**  Not applicable. While users in AWS IAM may belong in groups to logically grouped sets of permissions, there are no group authenticators. Each authenticator is at the individual level.  **cloud.gov**  Not applicable. As described in IA-2 (5), cloud.gov does not support group authenticators. All authentication is at the individual level. |

#### IA-5 (1) Control Enhancement (L) (M)

The information system, for password-based authentication:

1. Enforces minimum password complexity of [FedRAMP Assignment: case sensitive, minimum of twelve (12) characters, and at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters];
2. Enforces at least the following number of changed characters when new passwords are created: [FedRAMP Assignment: at least one (1)];
3. Stores and transmits only cryptographically-protected passwords;
4. Enforces password minimum and maximum lifetime restrictions of [FedRAMP Assignment: one (1) day minimum, sixty (60) day maximum];
5. Prohibits password reuse for [FedRAMP Assignment: twenty-four (24)] generations; and
6. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

| IA-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, System Owner, Information Security Officer | |
| Parameter IA-5(1)(a): case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters | |
| Parameter IA-5(1)(b): at least one changed when new passwords are created | |
| Parameter IA-5(1)(d): one day minimum, sixty day maximum | |
| Parameter IA-5(1)(e): twenty-four generations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-5 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | See IA-5 part c, including password requirements for AWS, cloud.gov internal users (GSA SecureAuth), and cloud.gov fallback identity provider.  For this part of IA-5 (1) and subsequent parts, customer responsibility is the same as IA-5. |
| Part b | See IA-5 part f, including: for AWS and cloud.gov, password reuse is not permitted. By definition, at least one character needs to be changed in order for a new password to be accepted. |
| Part c | See IA-5 part i. |
| Part d | See IA-5 part f for password maximum restrictions. |
| Part e | See IA-5 part f for password reuse restrictions. |
| Part f | See IA-5 part e for requirements to change temporary passwords. |

#### IA-5 (2) Control Enhancement (M) (H)

The information system, for PKI-based authentication:

1. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
2. Enforces authorized access to the corresponding private key;
3. Maps the authenticated identity to the account of the individual or group; and
4. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

| IA-5 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-5 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov does not rely on PKI for individual authentication, but cloud.gov does use PKI to secure its communication with identity systems as described at <https://cloud.gov/docs/ops/federated-identity/> .  When adding a new identification system, Cloud Operations manually verifies the public key provided by the IDP by communicating with the agency staff via a method outside of cloud.gov itself.  Additionally, all communication between cloud.gov and identity systems are protected using TLS, which is configured to verify certificates are signed by an accepted trust anchor (i.e. a certificate authority). See the hyperlink above for additional details. |
| Part b | The private key used by cloud.gov to sign communications with identity systems is securely stored in an encrypted version-controlled repository which maintains an audit log of all access attempts. |
| Part c | As described in IA-5 (2), cloud.gov uses PKI to verify all SAML assertions are from trusted identity systems that have been added to a whitelist by Cloud Operations. |
| Part d | Not applicable. Being a completely virtualized system, there is no ability to accomplish this. |

#### IA-5 (3) Control Enhancement (M) (H)

The organization requires that the registration process to receive [FedRAMP Assignment: All hardware/biometric (multifactor authenticators] be conducted [FedRAMP Selection: in person] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].

| IA-5 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter IA-5(3)-1: PIV cards which enable issuance of GSA SecureAuth credentials and multifactor authenticators | |
| Parameter IA-5(3)-2: in person | |
| Parameter IA-5(3)-3: for internal users, USAccess Program; for external users, customer defined registration authority | |
| Parameter IA-5(3)-4: for internal users, GSA Office of Human Resources Management; for external users, customer defined personnel or roles | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-5 (3) What is the solution and how is it implemented? |
| --- |
| All GSA internal staff are issued a personal identity verification (PIV) card by GSA, which is the registration authority responsible for all PIV issuance and registration.  GSA policies require in-person identity proofing and verification of physical documentation in accordance with HSPD-12 standards.  The System Owner is responsible for verifying that GSA has issued a PIV credential, along with government email addresses and access to GSA SecureAuth, before authorizing Cloud Operations access to AWS or cloud.gov systems. See IA-5 part a for additional detail.  **Customer Responsibility**  As described in IA-5 (11), cloud.gov is not responsible for issuance or verification of MFA authenticators required by customer enterprise identity systems. |

#### IA-5 (4) Control Enhancement (M)

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [*Assignment: organization-defined requirements*].

IA-5(4) Additional FedRAMP Requirements and Guidance:

Guidance: If automated mechanisms which enforce password authenticator strength at creation are not used, automated mechanisms must be used to audit strength of created password authenticators.

| IA-5 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter IA-5(4): corporate password policies | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-5 (4) What is the solution and how is it implemented? |
| --- |
| As described in IA-5, AWS and cloud.gov’s integration with GSA SecureAuth require that password authenticators are strong by default, so no additional assurance is required.  **cloud.gov fallback identity provider**  The IDP automatically requires the password strength requirements (described in IA-5) during creation of a password.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, cloud.gov is not responsible for enforcing password strength, as it delegates authentication to customer enterprise identity systems. It is the responsibility of those systems to employ automated tools to determine if password authenticators are sufficiently strong. |

#### IA-5 (6) Control Enhancement (M) (H)

The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

| IA-5 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-5 (6) What is the solution and how is it implemented? |
| --- |
| **AWS**  AWS GovCloud has been assessed at the FIPS 199 High impact baseline, which is in excess of cloud.gov’s current FIPS 199 Moderate rating. AWS IAM is therefore sufficiently protected.  **cloud.gov**  cloud.gov protects any authenticators within the environment itself (see IA-5 part d), and therefore is sufficiently protected at the same categorization of cloud.gov itself. Any local storage of authenticators is also assessed at that same categorization (in terms of government laptops outside the scope of and boundary of this authorization, or in terms of local encryption in GSA-approved password manager applications on those laptops). |

#### IA-5 (7) Control Enhancement (M) (H)

The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

| IA-5 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-5 (7) What is the solution and how is it implemented? |
| --- |
| As described in CM-10, the cloud.gov system is developed in the open as required by the 18F open source policy (<https://github.com/18F/open-source-policy/blob/master/policy.md>). Due to this requirement, the cloud.gov team continuously reviews all changes to the system to ensure that no nonpublic information (which includes passwords and other authenticators) is embedded in any applications or scripts. This prevents cloud.gov from embedding authenticators in any of its systems.  See AC-22 for additional details on procedures that prevent nonpublic information from being added to cloud.gov public repositories. |

#### IA-5 (11) Control Enhancement (L) (M) (H)

The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].

| IA-5 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter IA-5(11): Not applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-5 (11) What is the solution and how is it implemented? |
| --- |
| **cloud.gov fallback identity provider**  This is not applicable to the IDP because it does not use hardware tokens.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, cloud.gov is not responsible for hardware tokens, as it delegates authentication to customer enterprise identity systems. It is the responsibility of those systems to implement support for hardware tokens, if applicable. |

### IA-6 Authenticator Feedback (L) (M) (H)

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

| IA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-6 What is the solution and how is it implemented? |
| --- |
| All systems obscure all input to password and other secret (one-time passwords, token) prompts by blanking all input when interacting with a command-line interface, and by displaying asterisks when using a web interface. |

### IA-7 Cryptographic Module Authentication (L) (M) (H)

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

| IA-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-7 What is the solution and how is it implemented? |
| --- |
| **AWS**  See the Provisional Authorization for AWS GovCloud.  **cloud.gov**  The System Owner and Cloud Operations are expressly prohibited from modifying any OpenSSL code running within the environment, unless given written and signed permission from the Authorizing Official. If cloud.gov, 18F, or GSA require a fork of OpenSSL, it will be listed and released along with other cloud.gov code repositories in GitHub.  While cloud.gov does not use any modifications to OpenSSL, we have set our UAA implementations to use 256-bit encryption keys, to order to strengthen the system. Per the notification requirement in 15 CFR 740.13, we notified the National Security Agency (NSA) and Commerce’s Bureau of Industry and Security (BIS) on April 28th, 2016 of this change, since the cloud.gov software is available and can be distributed globally.  As of the date of this document, they have not replied to our notification. On May 24th, 2016, the 18F Director of Infrastructure notified both NSA and BIS that cloud.gov moved forward with the change. The change commit was expressly approved by the 18F Director of Infrastructure ( <https://github.com/18F/cg-cf-release/pull/16> ).  If we receive a negative response at any time, Cloud Operations will revise our use of OpenSSL to meet the requirements of 15 CFR 740.1. |

### IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H)

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

| IA-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-8 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  It is the responsibility of the customer Application System Owner to uniquely identify non-organizational user identifiers which have access to their specific cloud.gov “Org” or “Space”. |

#### IA-8 (1) Control Enhancement (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

| IA-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-8 (1) What is the solution and how is it implemented? |
| --- |
| **cloud.gov fallback identity provider**  The IDP does not accept PIV credentials.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, cloud.gov delegates authentication to customer enterprise identity systems. It is the responsibility of those systems to verify Personal Identity Verification (PIV) credentials.  When those systems return assertions to cloud.gov based on cryptographic modules, the assertions are encrypted and signed by the agency single sign on systems, which cloud.gov verifies as described in IA-8(4). |

#### IA-8 (2) Control Enhancement (L) (M) (H)

The information system accepts only FICAM-approved third-party credentials.

| IA-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Not applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-8 (2) What is the solution and how is it implemented? |
| --- |
| GSA does not use any third-party credentials.  **cloud.gov fallback identity provider**  This is not applicable to the IDP because it does not use third-party credentials.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, cloud.gov delegates authentication to customer enterprise identity systems. If the customer uses third-party credentials with their system, it is their responsibility to assess FICAM compliance. |

#### IA-8 (3) Control Enhancement (L) (M) (H)

The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials.

| IA-8 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, System Owner | |
| Parameter IA-8(3): Not Applicable. cloud.gov delegates authentication to agency single sign on systems | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-8 (3) What is the solution and how is it implemented? |
| --- |
| GSA does not use any third-party credentials.  **cloud.gov authentication**  cloud.gov implements SAML 2.0 for integration with the cloud.gov fallback identity provider (IDP) and customer enterprise identity systems. SAML 2.0 is FICAM-approved.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, cloud.gov delegates authentication to customer enterprise identity systems. It is the responsibility of those systems to employ only FICAM-approved information system components to accept third-party credentials. |

#### IA-8 (4) Control Enhancement (L) (M) (H)

The information system conforms to FICAM-issued profiles.

| IA-8 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IA-8 (4) What is the solution and how is it implemented? |
| --- |
| Since cloud.gov integrates to GSA SecureAuth for internal users, it is the responsibility of GSA SecureAuth to conform to FICAM issued profiles.  **cloud.gov fallback identity provider**  This is not applicable to the IDP because it does not use third-party credentials.  **Customer Responsibility**  For customers who do not use the cloud.gov fallback identity provider, cloud.gov delegates authentication to customer enterprise identity systems. It is the responsibility of those systems to conform to FICAM issued profiles. |

## Incident Response (IR)

### IR-1 Incident Response Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
2. Reviews and updates the current:
   1. Incident response policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Incident response procedures [FedRAMP Assignment: at least annually].

| IR-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter IR-1(a): cloud.gov development and design team | |
| Parameter IR-1(b)(1): At least every 3 years | |
| Parameter IR-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| IR-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/IR-Policy.md> for the Incident Response procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### IR-2 Incident Response Training (L) (M)

The organization provides incident response training to information system users consistent with assigned roles and responsibilities in accordance with NIST SP 800-53 Rev 4:

1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| IR-2 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO) | |
| Parameter IR-2(a): 60 days | |
| Parameter IR-2(c): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The cloud.gov Program Manager organizes incident response training sessions, offered to the whole cloud.gov team at least annually, and requires that all Cloud Operations team members take the training. The training may be led by the Program Manager, a Cloud Operations team member, or another security specialist at 18F.  The cloud.gov team onboarding checklist (<https://github.com/18F/cg-product/blob/master/OnboardingChecklist.md>) also requires that all team members take incident response training within 60 days of joining the team.  This training is a meeting reviewing and explaining the cloud.gov IR Guide (<https://cloud.gov/docs/ops/security-ir/>) and discussing questions and examples. The team takes notes on the training, stored in a Google Doc in the cloud.gov team Google Drive folder. The team records attendance in that document.  If a cloud.gov team member has not completed cloud.gov trainings on deadline, the Program Manager schedules a training as soon as possible (at maximum during the next sprint [two-week planning increment]) so that person can complete the training as soon as possible. If they miss that training, the Program Manager removes their access to cloud.gov resources (following relevant items in the offboarding checklist at <https://github.com/18F/cg-product/blob/master/OffboardingChecklist.md> ) until they complete the training. |
| Part b | If the cloud.gov system changes in a radical way, the Program Manager adapts the incident response training to meet the needs of the new system. The Program Manager then requires Cloud Operations team members to take the training again. |
| Part c | The Program Manager requires all Cloud Operations team members to take the incident response training at least once a year. |

### IR-3 Incident Response Testing (M)

The organization tests the incident response capability for the information system [FedRAMP Assignment: at least annually] using [FedRAMP Assignment: see additional FedRAMP Requirements and Guidance] to determine the incident response effectiveness and documents the results.

IR-3 Additional FedRAMP Requirements and Guidance:

Requirements: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). For JAB authorization, the service provider provides test plans to the JAB/AO annually. Test plans are approved and accepted by the JAB/AO prior to the test commencing.

| IR-3 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO) | |
| Parameter IR-3-1: at least annually | |
| Parameter IR-3-2: tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-3 What is the solution and how is it implemented? |
| --- |
| The cloud.gov team, as directed by the Program Manager, creates test plans and exercises in accordance to NIST 800-61, and it presents these to the cloud.gov Authorizing Official for their approval.  cloud.gov tests its incident response capabilities with an annual table top exercise. The test takes the form of a teleconference (GSA Google Hangout) meeting where a security specialist (such as the Program Manager, a Cloud Operations team member, or another security specialist from 18F) guides the Cloud Operations team through a role-playing exercise with a simulated potential security incident. The team takes notes throughout the test, and afterward the team discusses the test and identifies weaknesses to fix with additional training or process improvements. The team files and tracks improvements with issues (cards) in a task tracking tool.  The team stores exercise notes in GSA Google Drive, in the 18F Team Folder. They follow a basic template in the folder, including the following sections: session leader names, participants from 18F Infrastructure and GSA Information Security, note-taker name, attendee names, exercise events/notes log, retro/feedback, and actionable items. |

#### IR-3 (2) Control Enhancement (M) (H)

The organization coordinates incident response testing with organizational elements responsible for related plans.

| IR-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-3 (2) What is the solution and how is it implemented? |
| --- |
| The cloud.gov team has conducted an incident response tabletop exercise to test our incident response plan, organized in coordination with 18F Infrastructure and GSA Information Security.  cloud.gov will coordinate all future annual exercises with 18F Infrastructure and GSA Information Security as well, and also evaluate if coordination is required with other organizational elements as incident response plans change. The exercise notes template (see IR-3) records this coordination. |

### IR-4 Incident Handling (L) (M) (H)

The organization:

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
2. Coordinates incident handling activities with contingency planning activities; and
3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

IR-4 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

| IR-4 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov implements automated processes to detect and analyze malicious activity within the platform, as described in SI-3 and other SI controls, including Snort for network-layer reporting. If these processes detect malicious activity, they automatically report the activity to the Cloud Operations team via PagerDuty. *Figure 10‑3 Monitoring and Alerting Data Flow Diagram* details the reporting system.  cloud.gov has an Incident Response Guide (<https://cloud.gov/docs/ops/security-ir/> ) that documents the procedures that staff should take in the case of an incident, as required by the 18F and GSA Incident Response Policy.  As part of that documented Incident Response process, the Cloud Operations team uses automated tools and manual tools to eradicate the threat and recover to a known state. Automated tools may include enforcing BOSH manifests and automatically replacing failed customer app instances. cloud.gov uses a service-oriented architecture that allows natural containment and separation.  If the system needs to be restored to a prior state, the team first reviews recent commits. If a defect is found in the configuration, the team initiates a GitHub rollback and a Concourse redeploy. This cycle will terminate the Virtual Machines and create new machines with known good configurations. Further details are included in SI controls. |
| Part b | cloud.gov incident response and contingency planning activities are coordinated due to overlapping subject areas. The Incident Response Guide and Contingency Plan ( <https://cloud.gov/docs/ops/contingency-plan/> ) include steps with cross-references that guide the team in following both plans as appropriate. For example, they direct that if a contingency situation is caused by a security incident, one Incident Commander should direct and delegate communications for the overall situation. |
| Part c | After the conclusion of each event response, the cloud.gov team schedules a retrospective (as documented at <https://cloud.gov/docs/ops/security-ir/#retrospective> ) and captures the output of the session in a team-only document. If appropriate, the team publishes a public version for customers as well.  As part of the retrospective discussion process, the team proposes, discusses and prioritizes ways to incrementally improve our systems, and to test these improvements. The team also discusses how to improve our incident response procedures, training, and exercises based on what we learned. This step is part of the postmortem process.  All cloud.gov team members have been cleared according to at least tier 1 non-sensitive federal security or an equivalent for contractors. |

#### IR-4 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to support the incident handling process.

| IR-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-4 (1) What is the solution and how is it implemented? |
| --- |
| The Cloud Operations team implements automated processes such as ClamAV and Tripwire to detect anomalies. When these processes detect an anomaly, they escalate an alert to Cloud Operations team members using PagerDuty.  PagerDuty has a built-in feature for tracking alert resolution status. PagerDuty automatically updates an alert to “resolved” if the problem condition is detected as cleared, or Cloud Operations can manually set the alert to “resolved”. The cloud.gov team also tracks activities throughout the incident response process in a private issue (ticket) that is only visible to the 18F team, with automatic timestamps for each update.  See SI controls for additional detail about anomaly detection and reporting. |

### IR-5 Incident Monitoring (L) (M) (H)

The organization tracks and documents information system security incidents.

| IR-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-5 What is the solution and how is it implemented? |
| --- |
| The overall cloud.gov incident response process is guided by our IR guide (<https://cloud.gov/docs/ops/security-ir/> ) which explains more details about how we track and document incidents. Summary of relevant information:  There are two ways incidents get reported to the team:   1. Automated: PagerDuty sends automated alerts from our monitoring system. (These are tracked with an automatic log within PagerDuty.) 2. Manual: A team member, customer, or other person reports a potential security incident to a team member.   In either case, the cloud.gov team member who first heard of the problem (who becomes the Incident Commander) then follows our IR guide. They send email reports to the GSA IT team and the 18F Infrastructure team, and they file an issue in the 18F Security Incidents GitHub repository, and they notify other cloud.gov team members. The issue tracker in the 18F Security Incidents GitHub repository serves as a centralized tracking tool for 18F team members. The IR Guide explains that throughout the incident process, the Incident Commander needs to track and update the progress of identifying and remediating the incident, with timestamps.  After an incident is resolved, the team does a retrospective about the incident and documents it in appropriate detail (including a timeline of events) in an internal document.  If the team decides that an appropriate action related to the incident is to notify customers, the team also posts information and updates to StatusPage (which helps track the incident for customers). |

### IR-6 Incident Reporting (L) (M) (H)

The organization:

1. Requires personnel to report suspected security incidents to the organizational incident response capability within [FedRAMP Assignment: US-CERT incident reporting timelines as specified in NIST SP800-61 (as amended)]; and
2. Reports security incident information to [Assignment: organization-defined authorities].

IR-6 Additional FedRAMP Requirements and Guidance

Requirement: Report security incident information according to FedRAMP Incident Communications Procedure.

| IR-6 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Cloud Operations | |
| Parameter IR-6(a): US-CERT incident reporting timelines as specified in NIST SP 800-61 | |
| Parameter IR-6(b): System Owner, Information Systems Security Officer (ISSO), incident response team | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | GSA requires all staff to report suspected security incidents to Infrastructure and GSA Information Security within the one hour of detecting a possible incident. This is documented in the cloud.gov incident response guide ( <https://cloud.gov/docs/ops/security-ir/> ) and in the *GSA IT Information Security Policy.* GSA Information Security evaluates the possible incident and handles reporting to US-CERT within the required reporting timelines. |
| Part b | All information pertaining to incidents is reported to 18F Infrastructure and GSA Information Security according to the cloud.gov incident response guide ( <https://cloud.gov/docs/ops/security-ir/> ) and according to the FedRAMP Incident Communications Procedure ( <https://www.fedramp.gov/templates/> ). |

#### IR-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to assist in the reporting of security incidents.

| IR-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-6 (1) What is the solution and how is it implemented? |
| --- |
| cloud.gov uses PagerDuty to automatically notify Cloud Operations staff in the case of a potential incident, based on automated alerts from cloud.gov’s several continuously-running automated security monitoring tools.  Further, cloud.gov automatically stores logs in Elasticsearch (a component of the ELK stack) and CloudWatch Logs, so that Cloud Operations and GSA Information Security can access relevant information when investigating a potential incident. AWS-level logs are automatically stored in CloudWatch Logs.  See 10.1 (Production Private Subnets) for an overview of Elasticsearch. |

### IR-7 Incident Response Assistance (L) (M) (H)

The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

| IR-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-7 What is the solution and how is it implemented? |
| --- |
| As described in the cloud.gov security incident response guide and contingency plan, Cloud Operations can notify customers about incidents and potential incidents using StatusPage ( <https://cloudgov.statuspage.io/> ), when this is appropriate for the incident. StatusPage allows customers to subscribe to updates by email or text message.  Customers can report potential incidents (and request support) via Slack or email, as documented at <https://cloud.gov/docs/help/> . The Security Incident Response guide explains to customers that they should email the cloud.gov support address if they encounter potential security problems (<https://cloud.gov/docs/ops/security-ir/> ). |

#### IR-7 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to increase the availability of incident response related information and support.

| IR-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-7 (1) What is the solution and how is it implemented? |
| --- |
| cloud.gov customers can subscribe to the cloud.gov-specific StatusPage ( <https://cloudgov.statuspage.io/> ) to automatically receive alerts about cloud.gov services.  The cloud.gov team uses StatusPage for multiple functions: an automated display of availability/status information for key services, and manual notices from the cloud.gov team about time-sensitive important information. These notices include outages and security incidents (when appropriate).  The cloud.gov team also uses proactive email notices to customers to communicate important information as necessary, which includes incident information when appropriate. |

#### IR-7 (2) Control Enhancement (M) (H)

The organization:

1. Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and
2. Identifies organizational incident response team members to the external providers.

| IR-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, Cloud Operations, ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-7 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | As part of 18F, the cloud.gov team has direct and cooperative relationships with the 18F Infrastructure team and the GSA Information Security team.  Within GSA Information Security, the cloud.gov team also works directly with its assigned ISSO, whose responsibility during incident response events facilitates cooperative relationships between cloud.gov’s incident response capability and external providers of information system protection capability.  GSA Information Security has direct relationships with other providers of federal incident response capability, inclusive of US-CERT. |
| Part b | The cloud.gov team coordinates with GSA Information Security primarily through our ISSO as POC for cross-organizational communication. |

### IR-8 Incident Response Plan (L) (M) (H)

The organization:

1. Develops an incident response plan that:
   1. Provides the organization with a roadmap for implementing its incident response capability;
   2. Describes the structure and organization of the incident response capability;
   3. Provides a high-level approach for how the incident response capability fits into the overall organization;
   4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   5. Defines reportable incidents;
   6. Provides metrics for measuring the incident response capability within the organization;
   7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   8. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
2. Distributes copies of the incident response plan to [FedRAMP Assignment: see additional FedRAMP Requirements and Guidance].

IR-8(b) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

1. Reviews the incident response plan [FedRAMP Assignment: at least annually];
2. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
3. Communicates incident response plan changes to [FedRAMP Assignment: see additional FedRAMP Requirements and Guidance].

IR-8(e) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

1. Protects the incident response plan from unauthorized disclosure and modification.

| IR-8 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO) | |
| Parameter IR-8(a)(8): FedRAMP JAB, System Owner | |
| Parameter IR-8(b) All cloud.gov employees and contractors, as well as key FedRAMP entities, and others deemed necessary by individual agencies/customers | |
| Parameter IR-8(c): at least annually | |
| Parameter IR-8(e): the cloud.gov team, including Cloud Operations, System Owner, and Program Manager, as well as GSA IT | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The cloud.gov team has developed an Incident Response Guide (<https://cloud.gov/docs/ops/security-ir/>) to implement incident response capabilities. Given the small size of the cloud.gov team, the structure of the incident response process is clear and concise; it assigns the first responder to the event the role of Incident Commander. (For this step, see <https://cloud.gov/docs/ops/security-ir/#initiate> - "In either case, the first participant on the cloud.gov team becomes the initial Incident Commander (IC) and carries out the next steps in the response.")  The Incident Response Guide provides clear guidance on what steps to take on each situation and how reporting should be handled. The Incident Response Guide empowers the Incident Commander to leverage as many resources from GSA and 18F as needed during the response process. The Incident Response Guide is continually reviewed and updated by the cloud.gov team and approved annually by the Authorizing Official. |
| Part b | The Incident Response Guide is distributed to the whole of the cloud.gov team, including Cloud Operations staff. When a new team member joins, their onboarding checklist (viewable publicly in template form at <https://github.com/18F/cg-product/blob/master/OnboardingChecklist.md> ) includes a checklist item for learning about cloud.gov’s Incident Response Policy and going through Incident Response Training within 60 days.  The Incident Response Guide is publicly available on the web as part of the cloud.gov documentation: <https://cloud.gov/docs/ops/security-ir/>  The Incident Response Checklist (which accompanies the Guide) is also publicly available: <https://cloud.gov/docs/ops/security-ir-checklist/> |
| Part c | The Incident Response Guide is continually reviewed and updated by the cloud.gov team. In addition, the cloud.gov team updates the IR Guide after it tests the guide, which happens at least annually, so it gets at least annual review and updates. |
| Part d | The Incident Response Guide is continually reviewed and updated by the cloud.gov team in response to system and organizational updates. In addition, the cloud.gov team updates the IR Guide after it tests the guide, which happens after any major system/organizational changes. |
| Part e | The cloud.gov team distributes changes to the Incident Response Guide to the whole cloud.gov team. The cloud.gov team works collaboratively over Slack and GitHub, with frequent meetings about product progress and changes, and changes to the Incident Response Guide are part of that collaborative process. This includes a biweekly sprint review meeting where the whole cloud.gov team presents and learns about all major completed work from the past two weeks. |
| Part f | The Incident Response Guide is stored in GitHub as a public open source file (in <https://github.com/18F/cg-site> ). The branch from which the document is generated is a protected branch forbidding the unauthorized deletion of revision history. Moreover, the cloud.gov team has both configured the repository and provided team policies to ensure strict controls on who has authority to approve changes to this guide. |

### IR-9 Information Spillage Response (M) (H)

The organization responds to information spills by:

1. Identifying the specific information involved in the information system contamination;
2. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;
3. Isolating the contaminated information system or system component;
4. Eradicating the information from the contaminated information system or component;
5. Identifying other information systems or system components that may have been subsequently contaminated; and
6. Performing other [Assignment: organization-defined actions].

| IR-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, System Owner, Information Systems Security Officer (ISSO) | |
| Parameter IR-9(b): Appropriate staff at the customer agency | |
| Parameter IR-9(f): Conduct a retrospective (postmortem) about the incident | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | As part of its ordinary operation, cloud.gov isolates all customer data, so that customers only have access to their own data.  If a cloud.gov team member notices a potential security incident related to information spillage, they must follow the cloud.gov Incident Response Process, which includes following the 18F Security Incident process ( <https://handbook.18f.gov/security-incidents/> ). The 18F process includes alerting GSA Information Security and 18F Infrastructure, and it includes specific instructions for reporting any potentially-sensitive information that may be involved (under “Reporting Other Incidents”, step 4).  **Customer Responsibility**  The Application System Owner is responsible for identifying the specific information involved in any information system contamination related to their application(s).  cloud.gov treats all information in customer orgs, spaces, and applications as equally sensitive; it has no ability to determine the sensitivity of customer data. |
| Part b | If cloud.gov is the cause of an information spill that affects customers, cloud.gov team members coordinate with 18F Infrastructure and GSA Information Security to communicate with affected customers. The specific person responsible for communicating with customers depends on the situation and is determined in collaboration between these teams; this may be the 18F Director of Infrastructure or the cloud.gov ISSO. This is covered in the Security Incident Response Guide in the “Remediate” stage, which happens after the incident responders have verified that the potential incident is a real incident.  **Customer Responsibility**  The Application System Owner is responsible for alerting the appropriate staff at their agency about their information spill. If appropriate for their procedure, they may also alert cloud.gov support to request cloud.gov-specific assistance with the spill, such as for technical advice or other coordination.  If cloud.gov customers request assistance from cloud.gov staff with an information spill, this is a security incident response process, so cloud.gov staff follow the Security Incident Response Guide. This guide includes alerting 18F Infrastructure and GSA Information Security, who coordinate with customer agency information security staff as appropriate. |
| Part c | cloud.gov team members (specifically Cloud Operations team members) handle isolating contaminated components, according to the cloud.gov Incident Response Guide. When this affects customers, they coordinate with the customers as described in part b.  **Customer Responsibility**  The Application System Owner is responsible for isolating their contaminated org, space, and application. |
| Part d | cloud.gov team members (specifically Cloud Operations team members) handle eradicating contaminated components, according to the cloud.gov Incident Response Guide. When this affects customers, they coordinate with the customers as described in part b.  **Customer Responsibility**  The Application System Owner is responsible for eradicating the information from the contaminated org, space, and application. |
| Part e | Cloud Operations coordinates with 18F Infrastructure, GSA Information Security, and any affected customers to identify any other affected components or systems.  **Customer Responsibility**  The Application System Owner is responsible for identifying other information systems or system components that may have been subsequently contaminated. |
| Part f | Whenever the cloud.gov team is involved in an incident response process, the last step (after the incident is resolved) is to conduct a retrospective (also called a postmortem) where the team discusses what they learned and identifies ways to prevent or mitigate the problem in the future.  **Customer Responsibility**  The Application System Owner is responsible for performing any other actions required by their agency or team process. |

#### IR-9 (1) Control Enhancement (M) (H)

The organization assigns [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills.

| IR-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, System Owner, Information Systems Security Officer (ISSO) | |
| Parameter IR-9(1): cloud.gov team, 18F Infrastructure, GSA Information Security | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-9 (1) What is the solution and how is it implemented? |
| --- |
| As described in the cloud.gov Incident Response Guide, the first cloud.gov team member who notices (or is notified of) a potential information spill is responsible for escalating the notification to 18F Infrastructure, GSA Information Security, and the rest of the cloud.gov team; these teams together are responsible for responding to information spills. As described in IR-9 part b, the specific person responsible for communicating with customers depends on the situation and is determined in collaboration between these teams; this may be the 18F Director of Infrastructure or the cloud.gov ISSO.  If a customer requests assistance from the cloud.gov team for handling an information spill, the first cloud.gov team member who is contacted (or notices the request) becomes the initial Incident Commander, who is responsible for appropriately escalating the request according to the cloud.gov Incident Response Guide, which includes notifying 18F Infrastructure and GSA Information Security. They then coordinate on the appropriate response to assist the customer.  **Customer Responsibility**  The Application System Owner is responsible for assigning responsibility for responding to information spills. |

#### IR-9 (2) Control Enhancement (M)

The organization provides information spillage response training [Assignment: organization- defined frequency].

| IR-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, System Owner, Information Systems Security Officer (ISSO) | |
| Parameter IR-9(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-9 (2) What is the solution and how is it implemented? |
| --- |
| See IR-2. The cloud.gov team provides security incident response training at least annually, so that it is prepared to handle information spills and assist customers upon request.  **Customer Responsibility**  The Application System Owner is responsible for ensuring that their team receives information spillage response training. |

#### IR-9 (3) Control Enhancement (M) (H)

The organization implements [Assignment: organization-defined procedures] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

| IR-9 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager | |
| Parameter IR-9(3): Incident Response Guide | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-9 (3) What is the solution and how is it implemented? |
| --- |
| The cloud.gov Incident Response Guide includes directions to identify the severity of an incident and respond appropriately. This procedure of identifying severity helps the team avoid unnecessary disruption.  **Customer Responsibility**  The Application System Owner is responsible for implementing procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions. |

#### IR-9 (4) Control Enhancement (M) (H)

The organization employs [Assignment: organization-defined security safeguards] for personnel exposed to information not within assigned access authorizations.

| IR-9 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager | |
| Parameter IR-9(4): (customer responsibility) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| IR-9 (4) What is the solution and how is it implemented? |
| --- |
| The cloud.gov Incident Response Guide, in the “Remediation” section, identifies notification to parties exposed to unauthorized information of their obligations for handling that information in the remediation steps to be recorded by the Incident Commander.  **Customer Responsibility**  The Application System Owner is responsible for this control for their applications. They may ask cloud.gov for assistance implementing it, such as if cloud.gov staff were exposed to information not within assigned access authorizations. |

## Maintenance (MA)

### MA-1 System Maintenance Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
2. Reviews and updates the current:
   1. System maintenance policy [FedRAMP Assignment: at least every three (3) years]; and
   2. System maintenance procedures [FedRAMP Assignment: at least annually].

| MA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owners | |
| Parameter MA-1(a): cloud.gov development and design team | |
| Parameter MA-1(b)(1): At least every three years | |
| Parameter MA-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| MA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/MA-Policy.md> for the System Maintenance procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### MA-2 Controlled Maintenance (L) (M) (H)

The organization:

1. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
2. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
3. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
4. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
5. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
6. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.

| MA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, Information Systems Security Officer (ISSO) | |
| Parameter MA-2(c): Not Applicable. Handled at the Infrastructure as a Service layer. | |
| Parameter MA-2(f): Not Applicable. Handled at the Infrastructure as a Service layer. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part c | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part d | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part e | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part f | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### MA-3 Maintenance Tools (M) (H)

The organization approves, controls, and monitors information system maintenance tools.

| MA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MA-3 What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

#### MA-3 (1) Control Enhancement (M) (H)

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

| MA-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MA-3 (1) What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

#### MA-3 (2) Control Enhancement (M) (H)

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

| MA-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MA-3 (2) What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

#### MA-3 (3) Control Enhancement (M) (H)

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

1. Verifying that there is no organizational information contained on the equipment;
2. Sanitizing or destroying the equipment;
3. Retaining the equipment within the facility; or
4. Obtaining an exemption from [FedRAMP Assignment: the information owner explicitly authorizes removal of the equipment from the facility].

| MA-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, Information Systems Security Officer (ISSO) | |
| Parameter MA-3(3)(d): Not Applicable. Handled at the Infrastructure as a Service layer | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MA-3 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part c | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part d | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### MA-4 Remote Maintenance (L) (M) (H)

The organization:

1. Approves and monitors nonlocal maintenance and diagnostic activities;
2. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
3. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
4. Maintains records for nonlocal maintenance and diagnostic activities; and
5. Terminates session and network connections when nonlocal maintenance is completed.

| MA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part c | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part d | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part e | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

#### MA-4 (2) Control Enhancement (M) (H)

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

| MA-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MA-4 (2) What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### MA-5 Maintenance Personnel (L) (M) (H)

The organization:

1. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
2. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
3. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

| MA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part c | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

#### MA-5 (1) Control Enhancement (L) (M)

The organization:

1. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
   1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
   2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
2. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

MA-5 (1) Additional FedRAMP Requirements and Guidance:

Requirement: Only MA-5 (1) (a) (1) is required by FedRAMP

| MA-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MA-5 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### MA-6 Timely Maintenance (M) (H)

The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.

| MA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter MA-6(1): Not Applicable | |
| Parameter MA-6(2): Not Applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MA-6 What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

## Media Protection (MP)

### MP-1 Media Protection Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
2. Reviews and updates the current:
   1. Media protection policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Media protection procedures [FedRAMP Assignment: at least annually].

| MP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter MP-1(a): cloud.gov development and design team | |
| Parameter MP-1(b)(1): At least every three years | |
| Parameter MP-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| MP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/MP-Policy.md> for the Media Protection procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### MP-2 Media Access (L) (M)

The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

| MP-2 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter MP-2-1: Not applicable | |
| Parameter MP-2-2: Not applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MP-2 What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### MP-3 Media Labeling (M) (H)

The organization:

1. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
2. Exempts [FedRAMP Assignment: no removable media types] from marking as long as the media remain within [Assignment: organization-defined controlled areas].

MP-3(b) Additional FedRAMP Requirements and Guidance:

Guidance: Second parameter in MP-3(b)-2 is not applicable.

| MP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Not Applicable | |
| Parameter MP-3(b)-1: no removable media types | |
| Parameter MP-3(b)-2: Not Applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MP-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### MP-4 Media Storage (M) (H)

The organization:

1. Physically controls and securely stores [FedRAMP Assignment: [all types of digital and non-digital media with sensitive information]] within [FedRAMP Assignment: see additional FedRAMP requirements and guidance]; and

MP-4a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines controlled areas within facilities where the information and information system reside.

1. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

| MP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, Information Systems Security Officer (ISSO) | |
| Parameter MP-4(a)-1: all types of digital and non-digital media with sensitive information | |
| Parameter MP-4(a)-2: Not applicable. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MP-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### MP-5 Media Transport (M) (H)

The organization:

1. Protects and controls [FedRAMP Assignment: all media with sensitive information] during transport outside of controlled areas using [FedRAMP Assignment: for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secured in locked container];

MP-5a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB/AO.

1. Maintains accountability for information system media during transport outside of controlled areas;
2. Documents activities associated with the transport of information system media; and
3. Restricts the activities associated with transport of information system media to authorized personnel.

| MP-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, System Owner, Cloud Operations | |
| Parameter MP-5(a)-1: Not applicable | |
| Parameter MP-5(a)-2: Not applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MP-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part c | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part d | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

#### MP-5 (4) Control Enhancement (M) (H)

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

| MP-5 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MP-5 (4) What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### MP-6 Media Sanitization and Disposal (L) (M)

The organization:

1. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and
2. Employs sanitization mechanisms with strength and integrity commensurate with the classification or classification of the information.

| MP-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter MP-6(a)-1: Not applicable | |
| Parameter MP-6(a)-2: Not applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MP-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

#### MP-6 (2) Control Enhancement (M)

The organization tests sanitization equipment and procedures [FedRAMP Assignment: at least annually] to verify that the intended sanitization is being achieved.

MP-6(2) Additional FedRAMP Requirements and Guidance:

Guidance: Equipment and procedures may be tested or evaluated for effectiveness.

| MP-6 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter MP-6(2): Not applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MP-6 (2) What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### MP-7 Media Use (L) (M) (H)

The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards].

| MP-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter MP-7-1: Not applicable | |
| Parameter MP-7-2: Not applicable | |
| Parameter MP-7-3: Not applicable | |
| Parameter MP-7-4: Not applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MP-7 What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

#### MP-7 (1) Control Enhancement (M) (H)

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

| MP-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| MP-7 (1) is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

## Physical and Environmental Protection (PE)

### PE-1 Physical and Environmental Protection Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
2. Reviews and updates the current:
   1. Physical and environmental protection policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Physical and environmental protection procedures [FedRAMP Assignment: at least annually].

| PE-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter PE-1(a): cloud.gov development and design team | |
| Parameter PE-1(b)(1): At least every three years | |
| Parameter PE-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| PE-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See https://github.com/18F/compliance-docs/blob/master/PE-Policy.md for the Physical and Environmental Protection procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### PE-2 Physical Access Authorizations (L) (M)

The organization:

1. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
2. Issues authorization credentials for facility access;
3. Reviews the access list detailing authorized facility access by individuals [FedRAMP Assignment: at least annually]; and
4. Removes individuals from the facility access list when access is no longer required.

| PE-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Parameter PE-2(c): (Inherited from AWS) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part c | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part d | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-3 Physical Access Control (L) (M) (H)

The organization:

1. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by:
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress/egress to the facility using [FedRAMP Assignment: CSP defined physical access control systems/devices AND guards];
2. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points];
3. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;
4. Escorts visitors and monitors visitor activity [FedRAMP Assignment: in all circumstances within restricted access area where the information system resides];
5. Secures keys, combinations, and other physical access devices;
6. Inventories [Assignment: organization-defined physical access devices] every [FedRAMP Assignment: at least annually]; and
7. Changes combinations and keys [FedRAMP Assignment: at least annually] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

| PE-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Parameter PE-3(a): (Inherited from AWS) | |
| Parameter PE-3(a)(2): (Inherited from AWS) | |
| Parameter PE-3(b): (Inherited from AWS) | |
| Parameter PE-3(c): (Inherited from AWS) | |
| Parameter PE-3(d): (Inherited from AWS) | |
| Parameter PE-3(f)-1: (Inherited from AWS) | |
| Parameter PE-3(f)-2: (Inherited from AWS) | |
| Parameter PE-3(g): (Inherited from AWS) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part c | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part d | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part e | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part f | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part g | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-4 Access Control for Transmission Medium (M) (H)

The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].

| PE-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Parameter PE-4-1: (Inherited from AWS) | |
| Parameter PE-4-2: (Inherited from AWS) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-4 What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-5 Access Control for Output Devices (M) (H)

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

| PE-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-5 What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-6 Monitoring Physical Access (L) (M) (H)

The organization:

1. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
2. Reviews physical access logs [FedRAMP Assignment: at least monthly] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and
3. Coordinates results of reviews and investigations with the organization’s incident response capability.

| PE-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Parameter PE-6(b)-1: (Inherited from AWS) | |
| Parameter PE-6(b)-2: (Inherited from AWS) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part c | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

#### PE-6 (1) Control Enhancement (M) (H)

The organization monitors physical intrusion alarms and surveillance equipment.

| PE-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-6 (1) What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-8 Visitor Access Records (L) (M) (H)

The organization:

1. Maintains visitor access records to the facility where the information system resides for [FedRAMP Assignment: for a minimum of one (1) year]; and
2. Reviews visitor access records [FedRAMP Assignment: at least monthly]

| PE-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Parameter PE-8(a): for a minimum of one year | |
| Parameter PE-8(b): at least monthly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-9 Power Equipment and Cabling (M) (H)

The organization protects power equipment and power cabling for the information system from damage and destruction.

| PE-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-9 What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-10 Emergency Shutoff (M) (H)

The organization:

1. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
2. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and
3. Protects emergency power shutoff capability from unauthorized activation.

| PE-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Parameter PE-10(b): (Inherited from AWS) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part c | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-11 Emergency Power (M) (H)

The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss.

| PE-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Parameter PE-11: (Inherited from AWS) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-11 What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-12 Emergency Lighting (L) (M) (H)

The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

| PE-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-12 What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-13 Fire Protection (L) (M) (H)

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

| PE-13 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-13 What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

#### PE-13 (2) Control Enhancement (M) (H)

The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders].

| PE-13 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Parameter PE-13(2)-1: (Inherited from AWS) | |
| Parameter PE-13(2)-2: (Inherited from AWS) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-13 (2) What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

#### PE-13 (3) Control Enhancement (M) (H)

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

| PE-13 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-13 (3) What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-14 Temperature and Humidity Controls (L) (M) (H)

The organization:

1. Maintains temperature and humidity levels within the facility where the information system resides at [FedRAMP Assignment: consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled "Thermal Guidelines for Data Processing Environments]; and

PE-14 (a) Additional FedRAMP Requirements and Guidance:   
Requirement: The service provider measures temperature at server inlets and humidity levels by dew point.

1. Monitors temperature and humidity levels [FedRAMP Assignment: continuously].

| PE-14 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Parameter PE-14(a): (Inherited from AWS) | |
| Parameter PE-14(b): (Inherited from AWS) | |
| Parameter PE-14(b) Additional: (Inherited from AWS) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

#### PE-14 (2) Control Enhancement (M) (H)

The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

| PE-14 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-14 (2) What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-15 Water Damage Protection (L) (M) (H)

The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

| PE-15 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-15 What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-16 Delivery and Removal (L) (M) (H)

The organization authorizes, monitors, and controls [FedRAMP Assignment: all information system components] entering and exiting the facility and maintains records of those items.

| PE-16 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Parameter PE-16: (Inherited from AWS) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-16 What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

### PE-17 Alternate Work Site (M) (H)

The organization:

1. Employs [Assignment: organization-defined security controls] at alternate work sites;
2. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
3. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

| PE-17 | Control Summary Information |
| --- | --- |
| Responsible Role: Infrastructure as a Service provider | |
| Parameter PE-17(a): (Inherited from AWS) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PE-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part b | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |
| Part c | cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control. |

## Planning (PL)

### PL-1 Security Planning Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
2. Reviews and updates the current:
   1. Security planning policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Security planning procedures [FedRAMP Assignment: at least annually].

| PL-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM), Program Manager | |
| Parameter PL-1(a): cloud.gov development and design team | |
| Parameter PL-1(b)(1): At least every three years | |
| Parameter PL-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| PL-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/PL-Policy.md> for the Security Planning procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### PL-2 System Security Plan (L) (M) (H)

The organization:

1. Develops a security plan for the information system that:
   1. Is consistent with the organization’s enterprise architecture;
   2. Explicitly defines the authorization boundary for the system;
   3. Describes the operational context of the information system in terms of missions and business processes;
   4. Provides the security categorization of the information system including supporting rationale;
   5. Describes the operational environment for the information system and relationships with or connections to other information;
   6. Provides an overview of the security requirements for the system;
   7. Identifies any relevant overlays, if applicable;
   8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
   9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
2. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];
3. Reviews the security plan for the information system [FedRAMP Assignment: at least annually];
4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
5. Protects the security plan from unauthorized disclosure and modification.

| PL-2 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO) | |
| Parameter PL-2(b): Distribute to System Owner, ISSO, ISSM, AO | |
| Parameter PL-2(c): Are least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PL-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Using the most current FedRAMP SSP template, 18F developed a system security plan which includes the cloud.gov PaaS and encompasses the cloud.gov applications. The security plan is developed in accordance with NIST Special Publication 800-18 R1 *Guide of Developing Federal Information System Security Plans,* as well asFedRAMP guidance. The System Security Plan:   * Is consistent with 18F enterprise cloud.gov architecture; * Explicitly defines the authorization boundary for cloud.gov PaaS; * Describes the operational context of cloud.gov PaaS in terms of missions and business processes; * Provides the security category and impact level of cloud.gov including supporting rationale; * Describes the operational network for cloud.gov; * Describes relationships with or connections to other information systems; * Provides an overview of the security requirements for cloud.gov; and * Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions. |
| Part b | 18F distributes copies of the cloud.gov SSP and communicates subsequent changes to the plan to the cloud.gov System Owner, ISSO, ISSM, AO and other designated members within the 18F staff and agency. |
| Part c | The ISSO, in conjunction with key 18F management officials, reviews the cloud.gov SSP at least annually or whenever there is a significant change to the information system. |
| Part d | The ISSO updates the cloud.gov SSP to address changes to the platform and its network of operation or problems identified during plan implementation or security control assessments, and thereafter whenever a significant change occurs. |
| Part e | The ISSO protects the security plan from unauthorized modification by maintaining it as a write-access-controlled Google Doc and alternatively in a version-controlled documentation repository ( <https://github.com/18F/cg-compliance> ) that can only be modified by designated members from 18F and the agency.  The cloud.gov team intentionally makes most of the system security plan publicly available as open source documents in 18F repositories (including <https://github.com/18F/cg-compliance> and <https://github.com/18F/compliance-docs> ). We follow 18F’s Open Source Policy ( <https://github.com/18F/open-source-policy/blob/master/policy.md> ): our non-sensitive work should be public and open source whenever possible. The cloud.gov team does not share sensitive information (such as PII that may be in the SSP) publicly, and follows 18F guidance around this point: <https://github.com/18F/open-source-policy/blob/master/practice.md#protecting-sensitive-information> |

#### PL-2 (3) Control Enhancement (M) (H)

The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.

| PL-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO) | |
| Parameter PL-2(3): 3PAO, auditors | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PL-2 (3) What is the solution and how is it implemented? |
| --- |
| The cloud.gov Cloud Operations team plans and coordinates security-related activities affecting the platform with the Authorizing Official, System Owner, ISSM, and ISSO before conducting such activities in order to reduce the impact on other entities. |

### PL-4 Rules of Behavior (L) (M)

The organization:

1. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
2. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
3. Reviews and updates the rules of behavior [FedRAMP Assignment: at least every three (3) years]; and
4. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

| PL-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager | |
| Parameter PL-4(c): at least every three years | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PL-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All 18F staff members (including Cloud Operations staff) adhere to the GSA Information Technology (IT) General Rules of Behavior CIO 2015.1A CHGE 1 May 3, 2016 which is readily available on the GSA InSite web portal for individuals requiring access to the information system (and available upon request to other agencies and auditors). This lists the rules that describe their responsibilities and expected behavior with regard to information and information system usage.  cloud.gov documentation also provides a public list of Rules of Behavior for all cloud.gov account holders, available under “Use your account responsibly” on this page: <https://cloud.gov/docs/getting-started/accounts/> |
| Part b | All 18F staff members are required to sign an acknowledgment indicating that they have read, understand, and agree to abide by the GSA Rules of Behavior, before authorizing access to information and the information system.  When logging into the cloud.gov system, all cloud.gov account holders (internal and external users) are required to agree to the cloud.gov account holder Rules of Behavior. The website (as seen at <https://login.fr.cloud.gov/login> ) provides a warning with a “Read more details” link, and the detailed description of requirements includes a link to the rules at <https://cloud.gov/docs/getting-started/accounts/> ). This is a public page that anyone can view. Users must click “Agree and Continue” before they can log in. |
| Part c | All reviews and updates to the GSA Rules of Behavior are handled by GSA’s security policy team, with expected updates to the Rules of Behavior at least every three years. |
| Part d | GSA requires individuals who have signed a previous version of the GSA Rules of Behavior to read and resign when the rules of behavior are revised/updated. |

#### PL-4 (1) Control Enhancement (M) (H)

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

| PL-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PL-4 (1) What is the solution and how is it implemented? |
| --- |
| All staff adheres to the GSA Information Technology (IT) general *Rules of Behavior CIO 2015.1A CHGE 1 May 3, 2016* which is readily available on the GSA InSite web portal for individuals requiring access to the information system. This includes the rules that describe their responsibilities and expected behavior with regard social media under *GSA Order CIO 2106.1, GSA Social Media Policy*, which is also readily available on the GSA InSite web portal. This document in turn references the GSA Social Media Guide which provides specific detail on policies with examples to guide understanding. |

### PL-8 Information Security Architecture (M) (H)

The organization:

1. Develops an information security architecture for the information system that:
   1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
   2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
   3. Describes any information security assumptions about, and dependencies on, external services;
2. Reviews and updates the information security architecture [FedRAMP Assignment: at least annually or when a significant change occurs] to reflect updates in the enterprise architecture; and

PL-8 (b) Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F, on Page F-7.

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 Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter PL-8(b): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PL-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The system implements a centralized security stack that can support multiple applications; ensuring adherence to NIST 800-53 controls and FISMA, as well as 18F and GSA Information Technology (IT) Security Policies. Information security architecture is integrated into the information system by addressing information system requirements throughout the SDLC process. The FedRAMP JAB provides feedback to the Cloud Operations team on the security architecture and the Cloud Operations team receives regular guidance from the JAB board.    cloud.gov uses industry best practices and applies hardening security benchmarks to all virtual machine instances. For perimeter protection, each subnet is assigned individual elastic network interface (ENI), so security groups can be applied to each of the interfaces; firewall rules are applied for isolated traffic between subnets. This adds an additional layer of protection.  The determining factors of Confidentiality, Integrity, and Availability of the cloud.gov system are its FIPS 199 information types, which are listed in Section 2 of its SSP. The resulting Security Categorization, FIPS 199 Moderate Impact, governs the cloud.gov security architecture, which NIST SP 800-27A defines as “A description of security principles and an overall approach for architecture complying with the principles that drive the system design.” The information security architectural approach is documented in the cloud.gov System Security Plan, which describes implementation of said principles.  The cloud.gov platform leverages IaaS via Amazon Web Services, which received a FedRAMP ATO in June 21, 2016. This allows the cloud.gov platform to inherit some security controls such as physical security and share responsibility of other controls such as media protection. For web applications, the Cloud Operations team ensures that a web vulnerability scanner (OWASP Zap) is run on a monthly basis. 18F web applications use industry best practices and federal hardening guidelines for web servers and application services like Java.  The SSP references an attached ***Services Table*** in describing control AC-20, “Use of External Information Systems”. The attachment comprehensively lists external services incorporated into cloud.gov operations, as well as information about the kinds of information exchanged with them and assumptions about the security and sensitivity of that information. |
| Part b | The cloud.gov ISSO, cloud.gov System Owner, and FedRAMP JAB review applicable security architectures prior to major implementations or security assessments. The cloud.gov ISSO(s) reviews and updates the information security architecture within the System Security Plan on an annual basis or when a significant change takes place to reflect updates in the enterprise architecture. Due to the dynamic and elastic nature of cloud computing, the operations team monitors real-time updates of its information security architecture using the AWS Management Console and other management tools. |
| Part c | The cloud.gov operations team follows the risk management framework (RMF) which includes conducting annual risk assessments for its information systems and infrastructure. Any changes are then updated in the SSP, plan of actions and milestones (POAM), and security assessment report (SAR).  All changes to the cloud.gov platform are routed through the 18F Change Control process using the GitHub ticketing and tracking system which monitors changes including, but not limited to, ensuring that information security architecture changes are appropriately reflected in updates to the SSP, Cloud Operations team documentation and other security architecture-related documentation.  The cloud.gov Program Manager ensures that planned aspects of the cloud.gov security architecture are reflected in organization procurements/acquisitions and captured within the appropriate controls of this System Security Plan (SSP). Planned architectural changes, once approved, are incorporated into the annual SSP update cycle. |

## Personnel Security (PS)

### PS-1 Personnel Security Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
2. Reviews and updates the current:
   1. Personnel security policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Personnel security procedures [FedRAMP Assignment: at least annually].

| PS-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter PS-1(a): cloud.gov development and design team | |
| Parameter PS-1(b)(1): At least every three years | |
| Parameter PS-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| PS-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See https://github.com/18F/compliance-docs/blob/master/PS-Policy.md for the Personnel Security procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### PS-2 Position Categorization (L) (M)

The organization:

1. Assigns a risk designation to all positions;
2. Establishes screening criteria for individuals filling those positions; and
3. Reviews and revises position risk designations [FedRAMP Assignment: at least every three (3) years].

| PS-2 | Control Summary Information |
| --- | --- |
| Responsible Role: GSA Office of Human Resources Management, 18F Talent, 18F Supervisors | |
| Parameter PS-2(c): at least every three years | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PS-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Position risk designation is assigned by the GSA Office of Human Resources Management (OHRM), 18F Talent, and 18F Supervisors. |
| Part b | Since GSA is a federal agency, we follow the risk designation methodology prescribed in the Office of Personnel Management (OPM) *Federal Investigations Notice, No. 10-06* ( <https://www.opm.gov/investigations/background-investigations/federal-investigations-notices/2010/fin10-06.pdf> ): we use the Position Designation Automated Tool available via the OPM website ( <https://www.opm.gov/investigations/> ).  This tool ( <https://www.opm.gov/investigations/background-investigations/position-designation-tool/> ) is an interactive way to apply the OPM Position Designation System to assess the duties and responsibilities of a position. |
| Part c | Risk designations are re-categorized whenever:   * Responsibilities change * The impact level of the system or the information in it changes * Or at least once every three years |

### PS-3 Personnel Screening (L) (M) (H)

The organization:

1. Screens individuals prior to authorizing access to the information system; and
2. Rescreens individuals according to [FedRAMP Assignment: For national security clearances; a reinvestigation is required during the fifth (5th) year for top secret security clearance, the tenth (10th) year for secret security clearance, and fifteenth (15th) year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the fifth (5th) year. There is no reinvestigation for other moderate risk positions or any low risk positions].

| PS-3 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter PS-3(b): For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PS-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Personnel screening is provided by the Office of Personnel Management (OPM). |
| Part b | See above. |

#### PS-3 (3) Control Enhancement (M) (H)

The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

1. Have valid access authorizations that are demonstrated by assigned official government duties; and
2. Satisfy [FedRAMP Assignment: personnel screening criteria – as required by specific information].

| PS-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter PS-3 (3)(b): personnel screening criteria – as required by specific information | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PS-3 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov does not contain any information requiring special protection. |
| Part b | cloud.gov does not contain any information requiring special protection. |

### PS-4 Personnel Termination (L) (M)

The organization, upon termination of individual employment:

1. Disables information system access within [FedRAMP Assignment: same day];
2. Terminates/revokes any authenticators/credentials associated with the individual;
3. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics];
4. Retrieves all security-related organizational information system-related property;
5. Retains access to organizational information and information systems formerly controlled by terminated individual; and
6. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

| PS-4 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter PS-4(a): same day | |
| Parameter PS-4(c): agency security policies | |
| Parameter PS-4(f)-1: System Owner, Cloud Operations | |
| Parameter PS-4(f)-2: 24 hours | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PS-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Disabling, termination and conducting of exit interviews are initiated and facilitated by the supervisor or contracting official of an individual. Retrieval of all information system-related property which includes HDPS-12 cards, authentication tokens, mobile devices, laptops, etc. is a common control provided by GSA. More information can be found in the *GSA IT Security Procedural Guide 03-23, Termination and Transfer*. cloud.gov disables access to accounts within the same day of termination. |
| Part b | cloud.gov revokes all access associated to the individual the same day of termination. |
| Part c | Disabling, termination and conducting of exit interviews are initiated and facilitated by the supervisor or contracting official of an individual. Retrieval of all information system-related property which includes HDPS-12 cards, authentication tokens, mobile devices, laptops, etc. is a common control provided by GSA. More information can be found in the *GSA IT Security Procedural Guide 03-23, Termination and Transfer*. cloud.gov disables access to accounts within the same day of termination. |
| Part d | Disabling, termination and conducting of exit interviews are initiated and facilitated by the supervisor or contracting official of an individual. Retrieval of all information system-related property which includes HDPS-12 cards, authentication tokens, mobile devices, laptops, etc. is a common control provided by GSA. More information can be found in the *GSA IT Security Procedural Guide 03-23, Termination and Transfer*. cloud.gov disables access to accounts within the same day of termination. |
| Part e | Disabling, termination and conducting of exit interviews are initiated and facilitated by the supervisor or contracting official of an individual. Retrieval of all information system-related property which includes HDPS-12 cards, authentication tokens, mobile devices, laptops, etc. is a common control provided by GSA. More information can be found in the *GSA IT Security Procedural Guide 03-23, Termination and Transfer*. cloud.gov disables access to accounts within the same day of termination. |
| Part f | Disabling, termination and conducting of exit interviews are initiated and facilitated by the supervisor or contracting official of an individual. Retrieval of all information system-related property which includes HDPS-12 cards, authentication tokens, mobile devices, laptops, etc. is a common control provided by GSA. More information can be found in the *GSA IT Security Procedural Guide 03-23, Termination and Transfer*. cloud.gov disables access to accounts within the same day of termination. |

### PS-5 Personnel Transfer (L) (M)

The organization:

1. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
2. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];
3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4. Notifies [Assignment: organization-defined personnel or roles] within [FedRAMP Assignment: within five days of the formal transfer action (DoD 24 hours)].

| PS-5 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter PS-5(b)-1: initiates transfers or re-assignment | |
| Parameter PS-5(b)-2: within the same day | |
| Parameter PS-5(d)-1: System Owner, Program Manager | |
| Parameter PS-5(d)-2: within five days of the formal transfer action | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PS-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Review of ongoing operational need for current logical and physical access by individuals are initiated and facilitated by the System Owner and Program Manager. Retrieval of all information system-related property which includes HDPS-12 cards, authentication tokens, mobile devices, laptops, etc. is a common control provided by GSA. cloud.gov revokes privileged access if an individual is reassigned or transferred outside of the team. |
| Part b | The cloud.gov System Owner or Program Manager initiates the revoking process within the same day of an individual being transferred outside of the team. |
| Part c | The cloud.gov System Owner or Program Manager modifies permissions granted to individuals to correspond any changes in the individual requirements. |
| Part d | 18F notifies the cloud.gov System Owner or Program Manager within 5 days of a formal transfer action. |

### PS-6 Access Agreements (L) (M)

The organization:

1. Develops and documents access agreements for organizational information systems;
2. Reviews and updates the access agreements [FedRAMP Assignment: at least annually]; and
3. Ensures that individuals requiring access to organizational information and information systems:
   1. Sign appropriate access agreements prior to being granted access; and
   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [FedRAMP Assignment: at least annually].

| PS-6 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter PS-6(b): At least annually | |
| Parameter PS-6(c)(2) At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PS-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All cloud.gov users click through and agree to an access agreement every time they need a new authorized session to cloud.gov through the browser. See AC-8 for details about this access agreement.  **Shared Responsibility**  Since cloud.gov is provided by a federal agency to other agencies, 18F/GSA signs standard US Treasury forms (7600A and 7600B) to create inter-agency agreements (IAAs) that allow other agencies to access and use cloud.gov. The 18F Agreements team develops agreement text with the GSA Office of General Counsel (OGC) to ensure the boilerplate of all cloud.gov access agreements meet all legal, regulatory, policy, and Executive Order requirements.  All agreements are signed by both the Requesting Agency (the cloud.gov customer) and the Service Agency (18F/GSA), and a copy is distributed to both parties. All documentation making up the agreement is then stored in GSA's Google Drive for Government account. |
| Part b | The System Owner reviews all access agreements at least yearly, or upon request from 18F Agreements, GSA Information Security, or OGC.  **Shared Responsibility**  18F Agreements and OGC track, review, approve, and make all changes to cloud.gov agreements, either upon receiving a request for a modification (whether requested from cloud.gov or the Requesting Agency), identifying the need for additional funds, or near the end of the period of performance (not to exceed one year from signing). |
| Part c | **Shared Responsibility**  18F/GSA requires that all agencies have an active, signed, and fully-funded agreement to maintain access and use of the system. |

### PS-7 Third-Party Personnel Security (L) (M)

The organization:

1. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
2. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
3. Documents personnel security requirements;
4. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [FedRAMP Assignment: same day]; and
5. Monitors provider compliance.

| PS-7 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter PS-7(d)-1 n/a | |
| Parameter PS-7(d)-2 n/a | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PS-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | 18F does not currently use third-party personnel. However, overall GSA enforces the same requirements on contractors that it does on staff. See the *GSA IT Security Policy* for more information. |
| Part b | See the *GSA IT Security Policy* for more information. |
| Part c | See the *GSA IT Security Policy* for more information. |
| Part d | 18F does not employ any third-party personnel to work on cloud.gov directly. If 18F issues new contracts in the future, those contracts will use the FedRAMP assignment of "same day" for any personnel change notifications. |
| Part e | Not applicable. |

### PS-8 Personnel Sanctions (L) (M)

The organization:

1. Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
2. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

| PS-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Authorizing Official, System Owner, 18F supervisors, and GSA Office of Human Resources Management (if applicable), GSA Office of General Counsel (if applicable) | |
| Parameter PS-8(b)-1 the GSA Information Security team, and the individual's direct supervisor | |
| Parameter PS-8(b)-2 within 24 hours | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| PS-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | PS-1's procedures outlines the formal sanctions process whenever a failure to comply with information security policies and procedures is detected. See PS-1 and the *Personnel Security Policy* procedures for the implementation. |
| Part b | The GSA Information Technology Security Policy empowers the GSA Office of Human Resources Management (OHRM) to ensure "consistent and appropriate sanctions for personnel violating management, operation, or technical information security controls."  Since cloud.gov is a system provided by a Federal agency, only OHRM and the individual's direct supervisor can issue formal and final sanctions. The Authorizing Official for the system can only make recommendations on sanctions and actions. However, the Authorizing Official can make final determinations if the individual in question is allowed to access the system after an incident is detected.  See PS-1 and the 18F *Personnel Security Policy* procedures for the implementation. |

## Risk Assessment (RA)

### RA-1 Risk Assessment Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
2. Reviews and updates the current:
   1. Risk assessment policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Risk assessment procedures [FedRAMP Assignment: at least annually].

| RA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter RA-1(a): cloud.gov development and design team | |
| Parameter RA-1(b)(1): At least every three years | |
| Parameter RA-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| RA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/RA-Policy.md> for the Risk Assessment procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### RA-2 Security Categorization (L) (M) (H)

The organization:

1. Categorizes information and the information system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
3. Ensures the security categorization decision is reviewed and approved by the AO or authorizing official designated representative.

| RA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Authorizing Official | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| RA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The cloud.gov System Owner categorized the cloud.gov information and information system in accordance with FIPS 199 “Standards for Security Categorization of Federal Information and Information System” and NIST SP 800-60 “Guide for Mapping Types of Information and Information Systems to Security Categories,” Volume II, Appendix C.3:  C.3.5 Information & Technology Management  (C.3.5.1) System Development  (C.3.5.2) Lifecycle/Change  (C.3.5.3) System Maintenance  (C.3.5.4) IT Infrastructure  SSP Section 2.1, *Table 2‑2 Sensitivity Categorization of Information Types* and Section 2.2, *Table 2‑3 Security Impact Level* demonstrate the risk assessment conducted.  The security category for cloud.gov has been selected as Moderate based on the high-water mark of the security categorization of the internal information types provided by cloud.gov. |
| Part b | The cloud.gov System Owner documented the security categorization results in Section 2 of this SSP (Refer to Section 2.1, Table 2-2 and Section 2.2, Table 2.3), based on *NIST SP 800-60, Volume II, Appendix C.3*. |
| Part c | The cloud.gov Authorizing Official reviewed and approved the categorization on March 1, 2016. The FedRAMP JAB reviews this information as part of the risk-based decision on whether or not to grant a P-ATO. |

### RA-3 Risk Assessment (L) (M)

The organization:

1. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
2. Documents risk assessment results in [Selection: security plan; risk assessment report; [FedRAMP Assignment: security assessment report]];
3. Reviews risk assessment results [FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs];
4. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and
5. Updates the risk assessment [FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

RA-3 Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F

RA-3 (d) Requirement: Include the Authorizing Official; for JAB authorizations to include FedRAMP.

| RA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO), Program Manager | |
| Parameter RA-3(b): as part of the 3PAO SAR Report, and within the SSP as appropriate incorporating the 3PAO assessment determinations | |
| Parameter RA-3(c): at least every 3 years, or when significant changes occur which could impact risk level | |
| Parameter RA-3(d): the Authorizing Official, System Owner, ISSO, ISSM, FedRAMP PMO | |
| Parameter RA-3(e): at least every three years or when a significant change occurs | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| RA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov uses an accredited 3PAO to perform annual risk assessments of the platform security controls in accordance with the 18F’s continuous monitoring strategy as well as FedRAMP's requirements.  This includes a Security Assessment Report that identifies risks and threats both at a company and at a business process level. |
| Part b | The accredited 3PAO documents its risk assessment results in a Security Assessment Report (SAR). The cloud.gov team uses the report to update the cloud.gov Plan of Actions and Milestones (POAM) with the risk assessment results, along with updating the SSP as appropriate. This POAM is part of 18F’s continuous monitoring strategy for FedRAMP. |
| Part c | The 3PAO reviews the SAR as part of the annual 3PAO review, or whenever significant changes to the cloud.gov system or its environment of operation (including the identification of new threats and vulnerabilities or other conditions) occur that may impact the risk and security state of cloud.gov.  The cloud.gov Program Manager reviews the cloud.gov risk assessment when received from the 3PAO. |
| Part d | The cloud.gov Program Manager disseminates cloud.gov risk assessment results to the Authorizing Official, Systems Owner, Information Systems Security Officer (ISSO) and the FedRAMP JAB for review. |
| Part e | The 3PAO updates the SAR as part of the annual 3PAO review, or whenever significant changes to the cloud.gov system or its environment of operation (including the identification of new threats and vulnerabilities or other conditions) occur that may impact the risk and security state of cloud.gov.  The cloud.gov Program Manager updates the associated POAMs (or delegates this to a cloud.gov team member), as appropriate. |

### RA-5 Vulnerability Scanning (L) (M) (H)

The organization:

1. Scans for vulnerabilities in the information system and hosted applications [FedRAMP Assignment: monthly operating system/infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

RA-5 (a) Additional FedRAMP Requirements and Guidance:

Requirement: An accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.

1. Employs vulnerability scanning tools and techniques that promote 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 and making transparent, checklists and test procedures; and
   3. Measuring vulnerability impact;
2. Analyzes vulnerability scan reports and results from security control assessments
3. Remediates legitimate vulnerabilities; [FedRAMP Assignment: high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate risk vulnerabilities mitigated within ninety (90) days from date of discovery], in accordance with an organizational assessment of risk; and
4. 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-5 (e) Additional FedRAMP Requirements and Guidance:

Requirement: To include the Risk Executive; for JAB authorizations to include FedRAMP ISSOs.

| RA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, System Owner, Information Systems Security Officer (ISSO) | |
| Parameter RA-5(a): Monthly operating system; monthly web applications; annual penetration test and scans of all components performed by a 3PAO and GSA Information Security | |
| Parameter RA-5(d): High-risk vulnerabilities mitigated within 30 days; Moderate risk vulnerabilities mitigated within 90 days, Low findings mitigated within 180 days | |
| Parameter RA-5(e): include the System Owners, Cloud Operations, ISSM, ISSO, and the Authorizing Official; for JAB authorizations to include FedRAMP | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| RA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All scanning operations are conducted in collaboration with GSA Information Security teams.  **AWS** GSA Information Security runs weekly authenticated Nessus vulnerability scans from within the Virtual Private Clouds (VPCs).  Scans are supported by Cloud Operations, who ensure that all relevant components are identified for vulnerability scanning. The Nessus Agent is installed on all relevant components.    Cloud Operations and GSA Information Security work together to configure the scans, and to install relevant Nessus plug-ins appropriate for cloud.gov. Scans include but may not be limited to network discovery, OS vulnerabilities, application vulnerabilities, malware, and backdoors.  An authenticated Nessus scan is also run when a new baseline for EC2 hosts is built. Nessus assesses relevant Center for Internet Security (CIS) benchmark compliance checks, which include but may not be limited to long-term support versions of Ubuntu at the Level 1 benchmark. Cloud Operations team is responsible for ensuring scans completely successfully before rolling a new baseline into production.  **cloud.gov**  All vulnerability scanning and code analysis (whether static or dynamic) is coordinated with GSA Information Security. Cloud Operations is responsible for ensuring all scanning and analysis tooling runs successfully.  **Code scanning:** All 18F or GSA originated code is statically analyzed for test coverage, complexity, duplication, and security before being introduced into the production environment. Code Climate ( <https://codeclimate.com/> ) is the default scanner, but other scanning tools may be deployed in addition to Code Climate, at the discretion of Cloud Operations, the System Owner, or the Authorizing Official.  **Web application scanning:** Components of the cloud.gov system that are run as web applications on the platform by the cloud.gov team (for example login.fr.cloud.gov and dashboard.fr.cloud.gov) receive the following web application scanning:   * OWASP ZAP (Zed Attack Proxy) ( <https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project> ):   + Once a month, the Cloud Operations team manually runs an authenticated OWASP ZAP scan on these web application components and reviews the results. * External-facing web application components receive additional vulnerability scanning, at least monthly, via HP WebInspect. The automation of this task, and the distribution of any relevant results, is the responsibility of the GSA Information Security team, and is provided via their infrastructure outside the cloud.gov authorization boundary.   **Scan automation:** Throughout the development and deployment lifecycle, Cloud Operations uses Concourse to facilitate scheduling, running, and automation of all security tooling. The Concourse system ensures that security scanning tools are run against the entire system at regular intervals and that tests are successful before code and configuration is moved through the Staging VPC into the Production VPC.  **3PAO:** cloud.gov’s 3PAO scans operating systems/infrastructure, web applications, and databases once annually to provide an independent review of any system vulnerabilities. The 3PAO uses Nessus, Acunetix WVS, AppDetectivePro, Skipfish, Burp Suite Pro, and other tools that may be packaged with Kali Linux to assess cloud.gov.  **Additional tools:** Other tools, or specific configurations of the above tools, may be added or changed with collaboration and consent from Cloud Operations, the System Owner, GSA Information Security, and the Authorizing Official.  **Customer Responsibility**  cloud.gov is not responsible for scanning for vulnerabilities in customer applications. Application System Owners are responsible for all parts of RA-5 for their applications. |
| Part b | Wherever possible, tools consume and output data facilitate interoperability, comparisons, and central management of results. For example, vulnerabilities are rated on the Common Vulnerability Scoring System (CVSS) where appropriate. Matches with Common Vulnerability Enumerations (CVE) are detected.  GSA Information Security uses data collected by the GSA enterprise Tenable Security Center (TSC) to output reports in CyberScope format to meet GSA’s NIST, DHS, and OMB reporting requirements.  Code Climate is integrated into GitHub by design. OWASP ZAP outputs scan data in an open XML format. |
| Part c | Scan results and logs are kept for at least 60 days (with a monthly export kept indefinitely in Google Drive) for comparison to previous reports. Nessus reports are reviewed at least weekly and appropriate actions are taken by Cloud Operations to resolve any vulnerabilities. Any negative Code Climate reports on GitHub pull requests must be analyzed and resolved before the team can merge the pull request.  Any vulnerabilities that cannot be resolved immediately are tracked in the cloud.gov Plan of Action and Milestones (POAM). The POAM, vulnerability reports, and code analysis results are available to GSA Information Security on-demand via internal GSA file-sharing systems outside the boundary and scope of cloud.gov. |
| Part d | If possible, cloud.gov vulnerabilities are remediated immediately by Cloud Operations or the cloud.gov development and design team. Otherwise, cloud.gov teams attempt to remediate findings as soon as possible. The *GSA IT Security Policy* mandates that Critical and High risk findings be addressed within 30 days. Moderate risk findings are mandated to be addressed within 90 days. As required by FedRAMP, Low risk findings are addressed within 180 days.  If remediations will adversely impact functionality, performance, or availability, the cloud.gov ISSO, ISSM, Cloud Operations, GSA Information Security, and the System Owner will collaborate on implementing any compensating controls. The cross-functional team will then present any materials or justifications to the Authorizing Official (AO) for a risk-based decision. The AO will decide whether to accept the risk and will put any decisions in writing to the team. |
| Part e | All assessments and reports are available to all internal roles listed in *Table 9‑1 Personnel Roles and Privileges*, and to engineering teams across 18F and the Technology Transformation Services. |

#### RA-5 (1) Control Enhancement (M) (H)

The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities to be scanned.

| RA-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, GSA Information Security | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| RA-5 (1) What is the solution and how is it implemented? |
| --- |
| Due to the entire information system being virtualized in AWS, Cloud Operations and GSA Information Security always have an up-to-date and complete inventory of all components that make up cloud.gov. The AWS Management Console automatically keeps a list of all active components and service in AWS.  Cloud Operations configures the cloud.gov BOSH release to include the appropriate agents for each scanning/monitoring tool (including Tripwire, Snort, Nessus, and ClamAV), so that the agents automatically get deployed onto every host. See diagram 10-4.3 (*Monitoring and Alerting Data Flow*) for an illustration of the components in all EC2 instances. |

#### RA-5 (2) Control Enhancement (M) (H)

The organization updates the information system vulnerabilities scanned [Selection (one or more): [FedRAMP Assignment: prior to a new scan]].

| RA-5 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, GSA Information Security | |
| Parameter RA-5(2): prior to a new scan | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| RA-5 (2) What is the solution and how is it implemented? |
| --- |
| All GSA Information Security and 18F security tooling is setup to automatically download updated lists of vulnerabilities and signatures before every scan, whether from NIST’s National Vulnerability Database or their own private feeds. In the cases where customized signatures or plug-ins are available (ex: Code Climate, Nessus, Snort, etc.), these are kept updated on an ongoing basis. |

#### RA-5 (3) Control Enhancement (M) (H)

The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

| RA-5 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, GSA Information Security | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| RA-5 (3) What is the solution and how is it implemented? |
| --- |
| All GSA Information Security and 18F security tooling is setup to report on all components that underwent scanning (either by IP address, host name, or code repository as appropriate) and to also log which vulnerabilities were checked for, or which custom signatures or plug-ins were active during the scan. |

#### RA-5 (5) Control Enhancement (M) (H)

The organization includes privileged access authorization to [FedRAMP Assignment: operating systems, databases, web applications] for selected [FedRAMP Assignment: all scans].

| RA-5 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, GSA Information Security, 3PAO | |
| Parameter RA-5(5)-1: operating systems, web applications | |
| Parameter RA-5(5)-2: all scans that require privileged access | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| RA-5 (5) What is the solution and how is it implemented? |
| --- |
| Nessus is granted privileged access to the cloud.gov EC2 host baseline to allow for complete scanning, before it is deployed across the Production VPC. Nessus Agents are then deployed for continuous reporting to Nessus Manager.  OWASP ZAP, HP WebInspect, and Burp Suite Pro (or similar tools used by the 3PAO for application scanning) are provided with authentication credentials when required to complete any application level scanning. This depends on the component being scanned; they get the least necessary credentials to appropriately scan the system. For example, scanning the public cloud.gov website does not require authentication, but scanning the internal metrics web application does require authentication. |

#### RA-5 (6) Control Enhancement (M) (H)

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

RA-5(6) Additional FedRAMP Requirements and Guidance:

Guidance: Include in Continuous Monitoring ISSO digest/report to JAB/AO.

| RA-5 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, GSA Information Security, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| RA-5 (6) What is the solution and how is it implemented? |
| --- |
| GSA’s Tenable Security Center (TSC) automatically keeps vulnerability scan data and can provide reports for a server over time to compare the results of vulnerability scans and determine trends in information system vulnerabilities. GSA’s Tenable Security Center is used to identify and prevent regressions. Repeated findings are annotated with the first discovered dates. The cloud.gov ISSO is responsible for monitoring TSC along with the rest of the GSA Information Security team.  All 18F security tooling is set up to keep results and reports indefinitely.  The cloud.gov team sends a monthly Continuous Monitoring report to the FedRAMP JAB with a summary of vulnerability scans, which can be compared over time. |

#### RA-5 (8) Control Enhancement (L) (M) (H)

The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

RA-5(8) Additional FedRAMP Requirements and Guidance:

Requirement: This enhancement is required for all high vulnerability scan findings.

Guidance: While scanning tools may label findings as high or critical, the intent of the control is based around NIST's definition of high vulnerability.

| RA-5 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Officer (ISSO) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| RA-5 (8) What is the solution and how is it implemented? |
| --- |
| When any newly identified vulnerability is discovered (including high-severity vulnerabilities), the Cloud Operations and GSA Information Security teams review the audit logs stored in CloudTrail to identify if the vulnerability was exploited.  If any sign of exploit is detected, the team follows the procedures outlined in the system-specific Security Incident Response guide ( <https://cloud.gov/docs/ops/security-ir/> ). |

## System and Services Acquisition (SA)

### SA-1 System and Services Acquisition Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
2. Reviews and updates the current:
   1. System and services acquisition policy [FedRAMP Assignment: at least every three (3) years]; and
   2. System and services acquisition procedures [FedRAMP Assignment: at least annually].

| SA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter SA-1(a): cloud.gov development and design team | |
| Parameter SA-1(b)(1): At least every three years | |
| Parameter SA-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/SA-Policy.md> for the System and Services Acquisition procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### SA-2 Allocation of Resources (L) (M) (H)

The organization:

1. Determines information security requirements for the information system or information system service in mission/business process planning;
2. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
3. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

| SA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, Contracting Officer | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The cloud.gov program uses two-week planning sprints. Before each sprint, work is prioritized, inclusive of security needs. |
| Part b | 18F is part of the Technology Transformation Services (TTS) within GSA; cloud.gov and 18F coordinate with TTS and GSA leadership to appropriately plan for cloud.gov’s budget and staffing needs.  cloud.gov has also been filed and registered as a major IT investment through the Electronic Capital Planning Investment Control (eCPIC) process with the Office of Management and Budget. |
| Part c | cloud.gov is a major investment. As such, it is required to file reports on spending/budget with OMB. These reports include a breakout of spending on cloud.gov’s security analysis. |

### SA-3 System Development Life Cycle (L) (M) (H)

The organization:

1. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;
2. Defines and documents information security roles and responsibilities throughout the system development life cycle;
3. Identifies individuals having information security roles and responsibilities; and
4. Integrates the organizational information security risk management process into system development life cycle activities.

| SA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, System Owner, Program Manager | |
| Parameter SA-3(a) Scrumban process | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | 18F practices a Scrumban process when developing new features or fixing existing issues, including security fixes and enhancements for cloud.gov. Each feature or issue is assigned to a card in the system, where it goes through a process of being identified, prioritized, explored, delivered, and finally demonstrated. Each card is reviewed by the team as a whole throughout its lifecycle to identify any security risks or concerns, which are recorded on the card as "acceptance criteria" that must be addressed before development is complete.    Once development is complete, a team member submits the code to the version control system as a "pull request", where at least one other team member further reviews it before merging it into the code base. New features are deployed into our staging area where they undergo further security review and stakeholder acceptance testing, as well as automated acceptance tests. |
| Part b | The System Owner is responsible for ensuring appropriate staffing for security needs. The Cloud Operations team implements, configures, and maintains security controls.  GSA Information Security supports and monitors the cloud.gov team, including the ISSO who serves as a liaison between GSA Information Security and the cloud.gov team.  The cloud.gov 3PAO provides third-party verification and assessment of cloud.gov security.  See *Table 9‑1 Personnel Roles and Privileges*for more details. |
| Part c | As part of cloud.gov account management and access control, each service has a list of privileged accounts with the identities of the cloud.gov team members who have those privileges. See AC and IA control families for more details. |
| Part d | As part of 18F and GSA, the cloud.gov team complies with all GSA IT security policies and procedures. The team integrates the security risk management processes identified in the GSA IT Security Procedural Guide: Managing Enterprise Risk, Security Assessment and Authorization, Planning and Risk Assessment (CIO-IT Security-06-30).  See <https://github.com/18F/compliance-docs> for 18F security policies. |

### SA-4 Acquisitions Process (L) (M) (H)

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

1. Security functional requirements;
2. Security strength requirements;
3. Security assurance requirements;
4. Security-related documentation requirements;
5. Requirements for protecting security-related documentation;
6. Description of the information system development environment and environment in which the system is intended to operate; and
7. Acceptance criteria.

Additional FedRAMP Requirements and Guidance:

Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred.   
See <http://www.niap-ccevs.org/vpl> or <http://www.commoncriteriaportal.org/products.html>.

| SA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, System Owner, Contracting Officer | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | System and Services Acquisition Policy is included in *CIO P 2100.1 - GSA IT Security Policy, Chapter 5. Policy on Technical Controls*. It states, "GSA system program managers and contracting officers shall ensure that the appropriate security requirements of this order are included in task orders and contracts for all IT systems designed, developed, implemented, and operated by a contractor on behalf of the government, including systems operating in a Cloud Computing environment including but not limited to Software as a Service (SaaS)."  GSA Information Security also defined agency-wide system and services acquisition procedures in *IT Security Procedural Guide: Security Language for IT Acquisition Efforts (CIO-IT Security-09-48).* |
| Part b | GSA IT specifies security strength requirements for all GSA systems. See documents referenced in part a for details. |
| Part c | GSA IT specifies security assurance requirements for all GSA systems. See documents referenced in part a for details. |
| Part d | GSA IT specifies security-related documentation requirements for all GSA systems. See documents referenced in part a for details. |
| Part e | GSA IT specifies requirements for protecting security-related documentation for all GSA systems. See documents referenced in part a for details. |
| Part f | GSA IT specifies acceptable development and operation environments for all GSA systems. See documents referenced in part a for details. |
| Part g | GSA IT specifies security-related acceptance criteria for all GSA systems. See documents referenced in part a for details. |

#### SA-4 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

| SA-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-4 (1) What is the solution and how is it implemented? |
| --- |
| As described in SA-4, GSA IT provides policies and procedures that specify security-related requirements for the developers of information systems at GSA, including requiring developers to provide descriptions of the functional properties of the security controls to be employed. |

#### SA-4 (2) Control Enhancement (L) (M)

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [FedRAMP Selection (one or more): to include security-relevant external system interfaces, and high-level design]; [Assignment: organization-defined design/implementation information] at [Assignment: organization-defined level of detail].

| SA-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SA-4-1: security-relevant external system interfaces and high-level design | |
| Parameter SA-4-2: purpose and acceptance criteria | |
| Parameter SA-4-3: technical and operational level of detail | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-4 (2) What is the solution and how is it implemented? |
| --- |
| As described in SA-4, GSA IT provides policies and procedures that require developers of information systems to provide design and implementation information for security controls. |

#### SA-4 (8) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [FedRAMP Assignment: at least the minimum requirement as defined in control CA-7].

SA-4 (8) Additional FedRAMP Requirements and Guidance:

Guidance: CSP must use the same security standards regardless of where the system component or information system service is acquired.

| SA-4 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO) | |
| Parameter SA-4(8): at least the minimum requirement as defined in control CA-7 | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-4 (8) What is the solution and how is it implemented? |
| --- |
| Given cloud.gov’s current architecture, this is only applicable for AWS GovCloud. Please see the Provisional Authorization for AWS GovCloud for details. |

#### SA-4 (9) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

| SA-4 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-4 (9) What is the solution and how is it implemented? |
| --- |
| The cloud.gov program utilizes agile development processes. Changes are made early, often, and iteratively. Functions, ports, and protocols are part of this process. In the cloud.gov program, all such configuration is captured in version control and deployed in a fully automated process.  We use our Configuration Management procedures to identify these changes early in the system development life cycle, using our Feature Lifecycle procedure with Sketching and Security Impact Analysis steps before implementation: <https://github.com/18F/cg-product/blob/master/FeatureLifecycle.md> |

#### SA-4 (10) Control Enhancement (M) (H)

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

| SA-4 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-4 (10) What is the solution and how is it implemented? |
| --- |
| cloud.gov itself does not accept personal identity verification (PIV) cards.  **Customer Responsibility**  Customers may configure an enterprise identity provider that directly accepts PIV cards, either as a primary authenticator or a multi-factor authenticator (MFA). |

### SA-5 Information System Documentation (L) (M)

The organization:

1. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
2. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;
3. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response;
4. Protects documentation as required, in accordance with the risk management strategy; and
5. Distributes documentation to [Assignment: organization-defined personnel or roles)].

| SA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SA-5(c): Not applicable | |
| Parameter SA-5(e): all internal and external roles | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Cloud Operations always obtains complete documentation, including administrator documentation, for any technology that is used within cloud.gov. The maintenance of administrator documentation, in the form of version-controlled changes in a code repository or our documentation repository, is an assumed requirement for all changes. |
| Part b | Cloud Operations always obtains complete documentation, including user documentation, for any technology that is used within cloud.gov. The maintenance of user-facing documentation, in the form of version-controlled changes in a code repository or our documentation repository, is an assumed requirement for all changes. |
| Part c | Not applicable. Undocumented technology is not used for cloud.gov. |
| Part d | Currently, cloud.gov only uses technology whose documentation can be shared publicly. |
| Part e | 18F values transparency and collaboration. All documentation for technologies used by cloud.gov is either linked to directly from <https://cloud.gov/docs/> , or is shared broadly within GSA via Google Apps for Government. |

### SA-8 Security Engineering Principles (M) (H)

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

| SA-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-8 What is the solution and how is it implemented? |
| --- |
| cloud.gov applies security best practices, including but not limited to:   * Representing the entire system as “code”, so all changes and side effects can be quickly identified * Deploying the system via automated scripts and pipelines, ensuring no mistakes are made in instantiation * Minimizing the network surface area, applying security controls, isolating applications and data in containers, and encrypting connections. * Implementing role-based access controls, applying and enforcing permissions to isolate user to their space. Baseline configurations settings are reviewed on a continual basis to comply with federal mandates and compliance standards. * Documenting changes to the baseline configuration in GitHub for review. Part of this process includes a thorough security analysis of the proposed change prior to the configuration change being implemented on the operational system. * Deploying with every application a standard set of tools for security and monitoring of each application to identify security issues.   For more details please refer to the *18F Configuration Management Policy* and security controls CM-2, CM-3, and CM-6. |

### SA-9 External Information System Services (L) (M) (H)

The organization:

1. Requires that providers of external information system services comply with organizational information security requirements and employ [FedRAMP Assignment: FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
3. Employs [FedRAMP Assignment: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored] to monitor security control compliance by external service providers on an ongoing basis.

Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Continuous Monitoring Strategy Guide  
[https://www.FedRAMP.gov/resources/documents](https://www.fedramp.gov/resources/documents)

| SA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Authorizing Official, System Owner, GSA Information Security | |
| Parameter SA-9(a) FedRAMP Security Controls Baseline(s) | |
| Parameter SA-9(c): FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The Authorizing Official is ultimately accountable for ensuring oversight and compliance in the use of external information systems, and reviews the addition of any external information system with the System Owner and GSA Information Security. The Authorizing Official also accepts the risk of operating any external information system that has not been assessed to a FedRAMP Security Controls Baseline. |
| Part b | The Authorizing Official, System Owner, and GSA Information Security work together to ensure external information systems meet this control where applicable. See the *GSA IT Standards Profile* and the *GSA IT Information Security Policy* for additional information. |
| Part c | 18F uses its own monitoring program, or FedRAMP Continuous Monitoring program for external services. |

#### SA-9 (1) Control Enhancement (M) (H)

The organization:

1. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and
2. Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].

| SA-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Authorizing Official, System Owner, and GSA Information Security | |
| Parameter SA-9(1)(b): *see Additional Requirement and Guidance* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-9 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | 18F always conducts risk assessments for all technologies and services. See the risk assessment (RA) control family for details. |
| Part b | The cloud.gov System Owner must approve the acquisition or outsourcing of information security services for cloud.gov. |

#### SA-9 (2) Control Enhancement (M) (H)

The organization requires providers of [FedRAMP Assignment: All external systems where Federal information is processed or stored] to identify the functions, ports, protocols, and other services required for the use of such services.

| SA-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: System Owner, Information Systems Security Officer (ISSO) | |
| Parameter SA-9(2): All external systems where Federal information is processed or stored | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-9 (2) What is the solution and how is it implemented? |
| --- |
| See SA-5. Documentation on functions, ports, protocols, and other required services is obtained where applicable. |

#### SA-9 (4) Control Enhancement (M) (H)

The organization employs [Assignment: organization-defined security safeguards] to ensure that the interests of [FedRAMP Assignment: All external systems where Federal information is processed or stored] are consistent with and reflect organizational interests.

| SA-9 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SA-9(4)-1: risk assessments | |
| Parameter SA-9(4)-2: All external systems where Federal information is processed or stored | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-9 (4) What is the solution and how is it implemented? |
| --- |
| 18F always conducts risk assessments for all technologies and services. See the risk assessment (RA) control family for details. |

#### SA-9 (5) Control Enhancement (M) (H)

The organization restricts the location of [FedRAMP Selection: information processing, information data, AND information services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].

Additional FedRAMP Requirements and Guidance

Guidance: System services refer to FTP, Telnet, and TFTP, etc.

| SA-9 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SA-9(5)-1: information processing, information data, and information services | |
| Parameter SA-9(5)-2: to the internal cloud.gov platform hosted within GovCloud, and in some cases to defined supporting systems | |
| Parameter SA-9(5)-3: FedRAMP-defined conditions | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-9 (5) What is the solution and how is it implemented? |
| --- |
| See the Attachment *Services Table* for the list of services that cloud.gov can use for information processing, information data, and information services. Before adding services to the system, the cloud.gov System Owner must approve, and initiate the Significant Change Request process if necessary. |

### SA-10 Developer Configuration Management (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

1. Perform configuration management during system, component, or service [FedRAMP Selection: development, implementation, AND operation];
2. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];
3. Implement only organization-approved changes to the system, component, or service;
4. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
5. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

SA-10 (e) Additional FedRAMP Requirements and Guidance:

Requirement: For JAB authorizations, track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP ISSOs.

| SA-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SA-10(a): development, implementation, AND operation | |
| Parameter SA-10(b): all AWS and cloud.gov components | |
| Parameter SA-10(e): System Owner, Cloud Operations, Information Systems Security Officer (ISSO), GSA Information Security | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | All configuration management (CM) on cloud.gov and AWS is performed by developers, so all controls related to CM can be found in the CM policies, procedures, and control family documentation. See CM-1 and onwards for details. |
| Part b | As described in part a, documenting, managing, and controlling the integrity of changes is covered in the CM controls. |
| Part c | The process for implementing only organization-approved changes to the system is documented in the CM controls. |
| Part d | The process for documenting approved changes and the potential security impacts of such changes is documented in the CM controls. |
| Part e | As described in CM, RA, and SI, cloud.gov tracks security flaws and flaw resolution within the system, including Continuous Monitoring reporting to the JAB. |

#### SA-10 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

| SA-10 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-10 (1) What is the solution and how is it implemented? |
| --- |
| Deployment artifacts are stored in AWS S3 and distributed by BOSH via the “blobstore”. SHA-1 hashes are checked to verify file integrity throughout the deployment process. |

### SA-11 Developer Security Testing and Evaluation (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

1. Create and implement a security assessment plan;
2. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage];
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
4. Implement a verifiable flaw remediation process; and
5. Correct flaws identified during security testing/evaluation.

| SA-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, 3PAO, Information Systems Security Officer (ISSO) | |
| Parameter SA-11(b)-1: unit and integration testing | |
| Parameter SA-11(b)-2: each deployment | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | A security assessment plan is created by the FedRAMP Accredited Third Party Assessment Organization (3PAO). It is used for annual assessments conducted by the 3PAO for continuous monitoring of cloud.gov. |
| Part b | cloud.gov performs unit and integration testing on the system upon each deployment. |
| Part c | Security testing is done automatically and tracked using tools like Nessus, OWASP ZAP and Concourse. |
| Part d | Remediations are made by implementing changes to the configuration on configuration management, redeploying and testing. |
| Part e | Flaws identified by automated tools are remediated or marked as false as soon as possible. |

#### SA-11 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

SA-11 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

| SA-11 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-11 (1) What is the solution and how is it implemented? |
| --- |
| For code developed by 18F, Cloud Operations ensures Code Climate, at minimum, is actively monitoring each code repository master branch, and performs a new scan of the code whenever the branch is changed.  The result of each scan is automatically documented within the Code Climate service itself. Cloud Operations and any other relevant internal teams are also automatically notified of any vulnerabilities.  GitHub provides automated scanning for vulnerabilities in JavaScript and Ruby code dependencies, which alerts Cloud Operations with GitHub notifications when it identifies vulnerabilities: <https://github.com/blog/2470-introducing-security-alerts-on-github>  Where additional scanning for known vulnerabilities on code dependencies is relevant, Cloud Operations is also working on ensuring additional automated scanning tools will run, for example on Python and Go dependencies. |

#### SA-11 (2) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

| SA-11 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-11 (2) What is the solution and how is it implemented? |
| --- |
| 18F always conducts risk assessments for all technologies and services. See the risk assessment (RA) control family for details. |

#### SA-11 (8) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

| SA-11 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SA-11 (8) What is the solution and how is it implemented? |
| --- |
| cloud.gov commonly incorporates open source code where the author cannot be held responsible for dynamic scanning. In such cases, 18F takes on responsibility for dynamic scanning. Nessus is the primary tool used for performing dynamic analysis. See RA-5 and the entire SI family for details. |

## System and Communications Protection (SC)

### SC-1 System and Communications Protection Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
2. Reviews and updates the current:
   1. System and communications protection policy [FedRAMP Assignment: at least every three (3) years]; and
   2. System and communications protection procedures [FedRAMP Assignment: at least annually].

| SC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter SC-1(a): cloud.gov development and design team | |
| Parameter SC-1(b)(1): At least every three years | |
| Parameter SC-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/SC-Policy.md> for the System and Communications Protection procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### SC-2 Application Partitioning (M) (H)

The information system separates user functionality (including user interface services) from information system management functionality.

| SC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-2 What is the solution and how is it implemented? |
| --- |
| Cloud Foundry is the core set of components in the cloud.gov Platform as a Service, based on the Cloud Foundry open source project. User functionality is made available through the cloud.gov web user interface (“Dashboard”) and Cloud Foundry command-line interface (CF CLI). Both the Dashboard and CF CLI make use of the Cloud Foundry API. Users are permitted to write applications which directly manipulate the Cloud Foundry API when needed.  Privileged cloud.gov team roles (such as System Owner and Cloud Operations) have privileged Cloud Foundry API access, granted via User Account and Authentication (UAA) Server group membership. The Cloud Foundry API provides management functionality only to privileged team members.  The cloud.gov team manages information system functionality surrounding and supporting the Cloud Foundry components via AWS, GitHub, and Concourse. Users are unable to manipulate these facilities. |

### SC-4 Information in Shared Resources (M) (H)

The information system prevents unauthorized and unintended information transfer via shared system resources.

| SC-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-4 What is the solution and how is it implemented? |
| --- |
| **AWS Components**   * cloud.gov utilizes the AWS S3 service to store non-public information. S3 information transfer controls include: * S3 provides both bucket and object-level access controls, with defaults that only permit authenticated access by the bucket or object creator. * If a bucket creator wants to grant data access to a user, they have two options:   + Grant access to a specific user. This access is granted with the authentication process documented at <https://docs.aws.amazon.com/AmazonS3/latest/dev/RESTAuthentication.html>   + Grant anonymous access. * An authenticated user can read an object only if the user has been granted Read permissions in an Access Control List (ACL) at the object level. * An authenticated user can list the keys and create or overwrite objects in a bucket only if the user has been granted Read and Write permissions in an ACL at the bucket level. * Bucket- and object-level ACLs are independent; an object does not inherit ACLs from its bucket. * Permissions to read or modify the bucket or object ACLs are themselves controlled by ACLs that default to creator-only access.   **Cloud Foundry Components**  cloud.gov uses Cloud Foundry components to protect users and shared resources from security threats by minimizing network surface area, applying security controls, isolating customer applications and data in containers, encrypting connections. Cloud.gov generates customer-specific least-privilege credentials which are restricted to reading and writing only data in shared resources belonging to that customer.  **Customer Responsibility**  Amazon S3 is accessible via TLS endpoints. The encrypted endpoints are accessible from both the Internet and from within Amazon EC2, ensuring that data are transferred securely both within the AWS GovCloud environment and to and from sources outside of the AWS GovCloud environment. The customer is responsible for managing access to customer application data, and is advised not to shared cloud.gov-generated customer-specific credentials for S3 with others. Customers can opt to provision an explicitly unrestricted, public S3 bucket when public access to the data is warranted. |

### SC-5 Denial of Service Protection (L) (M) (H)

The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].

| SC-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-5-1: volume and protocol attacks | |
| Parameter: SC-5-2: VPC firewall rules, elastic capacity | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-5 What is the solution and how is it implemented? |
| --- |
| cloud.gov uses AWS's IaaS services with well-formed Virtual Private Cloud (VPC) firewall rules to reduce the attack surface of hosted components, while service resiliency is maintained by utilizing AWS Availability Zones and Elastic Load Balancing services.  Cloud Foundry's security components limit the effects of an attack at the application layer. It limits DoS attacks on this layer with well-formed application security groups, which control the traffic flowing to and from hosted applications. Only traffic explicitly directed at a given application’s whitelisted routes and ports will reach the application. |

### SC-6 Resource Availability (M) (H)

The information system protects the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more); priority; quota; [Assignment: organization-defined security safeguards]].

| SC-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-6-1: volatile and non-volatile storage, bandwidth, and availability of applications | |
| Parameter SC-6-2: quota | |
| Parameter SC-6-3: AWS features such as Elastic Load Balancing and auto scaling technologies, along with monitoring via New Relic, CloudWatch, CloudWatch Logs, and ELK to alert on availability concerns | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-6 What is the solution and how is it implemented? |
| --- |
| cloud.gov protects the availability of resources by allocating volatile and non-volatile storage, bandwidth, and availability by using automated AWS features such as Elastic Load Balancing technology at the infrastructure layer and CF's application lifecycle management components, Cloud Controller, at the application layers.  cloud.gov sets explicit resource limits on hosted applications which prevent an attack on one hosted application from causing resource starvation for other applications and the platform in general.  cloud.gov has resource monitoring tools that alert the team if overall platform resources are reaching their limits: CF's built-in health monitoring system, New Relic, CloudWatch, CloudWatch Logs, and ELK, which combined provide real-time alerts and visibility into critical systems and applications. When needed, additional resources can be provisioned for the platform’s use without interrupting operations |

### SC-7 Boundary Protection (L) (M) (H)

The information system:

1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
2. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
3. 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: Cloud Operations | |
| Parameter SC-7(b): logically | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Cloud Operations team members monitor and control communications at the external boundary of the system and at key internal boundaries within the system.  **AWS Boundary Protection**   * Secure Network Architecture   + 18F utilizes the AWS-provided virtual network devices, including firewall and other boundary devices, to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services.   + AWS Virtual Private Cloud (VPC) is used to logically isolate the resources supporting the application in a virtual network. VPC is in effect a perimeter firewall.   + ACLs, or traffic flow policies, are established on each managed interface, which manage and enforce the flow of traffic. * Internet Gateways   + AWS has strategically placed a limited number of access points to the cloud to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS), which allows cloud.gov to establish a secure communication session with its storage or compute instances within AWS.   + There are several external entry points to the System Boundary which are represented within *Figure 9‑1 Network Diagram*. Access to the System through each of these boundary points is controlled through the utilization of identity domains and access control domains which have been implemented in such a way as to ensure a valid user only has access to what is necessary for them to perform within their regular roles and responsibilities. * Transmission Protection   + cloud.gov connects to an AWS access point via HTTPS using Transport Layer Security (TLS), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery.   + cloud.gov utilizes the AWS Virtual Private Cloud (VPC), which provides a private subnet within the AWS cloud. Each VPC is configured to utilize Routing Rules, Subnet Rules, and Security Group Rules. Each of these controls must have appropriate rules and routes in-place before any external service is able to reach a host within AWS.   + The cloud.gov VPCs are segmented into subnets as follows: production, staging, tooling, and development.   The AWS network provides significant protection against traditional network security issues, and cloud.gov implements further protection. The following are a few examples:   * Distributed Denial of Service (DDoS) Attacks. AWS API endpoints are hosted on large, Internet-scale infrastructure. Proprietary DDoS mitigation techniques are used. Additionally, AWS’s networks are multi-homed across a number of providers to achieve Internet access diversity. * Man in the Middle (MITM) Attacks. All of the AWS APIs are available via TLS-protected endpoints which provide server authentication. Amazon EC2 AMIs automatically generates new SSH host certificates on first boot and logs them to the instance’s console. BOSH, the configuration management tool used by cloud.gov Cloud Operations, can then use the secure APIs to call the console and access the host certificates before logging into the instance for the first time. cloud.gov uses TLS for all interactions with AWS. * IP Spoofing. Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own. * 18F utilizes the ELK Stack, CloudTrail, and Prometheus to monitor and alert on any suspicious activities and connections to its virtual infrastructure. * Each Amazon VPC is a distinct, isolated network within the cloud; network traffic within each Amazon VPC is isolated from all other Amazon VPCs. Each VPC is configured to utilize Routing Rules and VPC Peering, Subnet Rules, and Security Group Rules. Each of these controls must have appropriate rules and routes in-place before any external service is able to reach a host within cloud.gov. * Amazon EC2 provides a complete firewall solution (using AWS Security Groups). Cloud Operations manages AWS Security Group configuration according to our overall configuration management policy. This mandatory inbound firewall is configured in a default deny-all mode. The Cloud Operations team explicitly opens the ports needed to allow inbound traffic. The traffic is restricted by protocol, by service port, or source IP address (individual IP or Classless Inter-Domain Routing (CIDR) block). The firewall is configured in groups permitting different classes of instances to have different rules.   **cloud.gov Application Boundary Protection**   * cloud.gov implements network traffic rules using Linux iptables on the component VMs. Operators can configure rules to prevent system access from external networks and between internal components, and to restrict applications from establishing connections over the network interface. * Cloud Operations use Cloud Foundry application security groups (ASGs) (<https://docs.cloudfoundry.org/adminguide/app-sec-groups.html>) to specify egress access rules for its applications hosted on the platform. Cloud Operations uses this functionality to securely restrict application outbound traffic to predefined routes.   **Spoofing**  If an IP, MAC, or ARP spoofing attack bypasses the physical firewall for the deployment, the cloud.gov network traffic rules help prevent the attack from accessing application containers. The cloud.gov platform uses application isolation, operating system restrictions, and encrypted connections to further mitigate risk. When deploying a hosted application container, the platform restricts allowed traffic to only expected ports by configuring the container’s network interface. |
| Part b | The cloud.gov platform implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks. The subnets and their segregation points are identified within *Figure 9‑1 Network Diagram*.  **AWS Boundary Protection**  Each VPC is configured to utilize Routing Tables, and Security Groups. Each of these controls must have appropriate rules and routes in-place before any external service is able to reach a host within cloud.gov.  **Operating System (EC2) Boundary Protection**  Snort is deployed and configured on all instances. Through the use of custom alerting rules within the log management solution the audit logs of both external facing instances as well as internal instances are monitored for indications of a potential attack. The system security team is continually working to develop and implement new use-cases that advance the capability to detect an attacker both externally and internally. |
| Part c | The cloud.gov PaaS is internal to the cloud.gov Virtual Private Cloud (VPC) and does not connect to external networks or information systems outside the cloud.gov Virtual Private Cloud (VPC), except as noted in the ***Services Table*** referenced in AC-20. |

#### SC-7 (3) Control Enhancement (M) (H)

The organization limits the number external network connections to the information system.

| SC-7 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-7 (3) What is the solution and how is it implemented? |
| --- |
| cloud.gov limits the number of external network connections to the information system through the use of AWS network security groups, which restrict the number of network connections. Specifically, Cloud Operations configures the network security groups to allow a specific limited number of Elastic Load Balancers, and this sets an upper bound on network connections.  cloud.gov Cloud Foundry components run on AWS instances (VMs) within AWS VPCs. In this configuration, the only access points visible on a public network are AWS load balancers that map to one or more Cloud Foundry routers inside cloud.gov. |

#### SC-7 (4) Control Enhancement (M)

The organization:

1. Implements a managed interface for each external telecommunication service;
2. Establishes a traffic flow policy for each managed interface;
3. Protects the confidentiality and integrity of the information being transmitted across each interface;
4. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
5. Reviews exceptions to the traffic flow policy [FedRAMP Assignment: at least at least annually] and removes exceptions that are no longer supported by an explicit mission/business need.

| SC-7 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-7(4)(e): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-7 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | This is an inherited control: AWS GovCloud implements a managed interface for each external telecommunication service. |
| Part b | The Cloud Operations team establishes a traffic flow policy for each managed interface as AWS VPC security groups. |
| Part c | The Cloud Operations team protects the confidentiality and integrity of the information being transmitted across each interface by using TLS for HTTP based connection and SSH system access. |
| Part d | cloud.gov does not allow exceptions to the baseline traffic flow policy. If Cloud Operations needs to update the traffic flow policy for an AWS VPC security group, Cloud Operations follows the standard cloud.gov Configuration Management Plan ( <https://cloud.gov/docs/ops/configuration-management/> ) to propose and review that change. |
| Part e | cloud.gov does not allow exceptions to the baseline traffic flow policy. See part d. |

#### SC-7 (5) Control Enhancement (M) (H)

The information system at managed interfaces denies network traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

| SC-7 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-7 (5) What is the solution and how is it implemented? |
| --- |
| cloud.gov's managed interfaces deny network traffic to VPCs by default and allow network communications traffic by exception through the application of AWS security control group definitions that are default-deny. Cloud Operations configures these AWS security group definitions using configuration files managed according to the cloud.gov Configuration Management Plan ( <https://cloud.gov/docs/ops/configuration-management/> ). |

#### SC-7 (7) Control Enhancement (M) (H)

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

| SC-7 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-7 (7) What is the solution and how is it implemented? |
| --- |
| The GSA VPN implements this control by disallowing split tunneling. |

#### SC-7 (8) Control Enhancement (M) (H)

The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.

| SC-7 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-7(8)(1): Tooling VPC | |
| Parameter SC-7(8)(2): GSA network | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-7 (8) What is the solution and how is it implemented? |
| --- |
| Access to administrative tools in the Tooling VPC (such as Nessus and Concourse) is restricted to the GSA network. Remote users must connect to the GSA VPN.  **AWS**  cloud.gov does not require authenticated proxy servers for AWS access. Cloud Operations team members gain access to this system through the AWS IAM multi-factor authentication process to perform administrative functions and duties at the IaaS layer, in order to administer any managed interfaces. |

#### SC-7 (12) Control Enhancement (M)

The organization implements [*Assignment: organization-defined host-based boundary protection mechanisms*] at [Assignment: organization-defined information system components].

| SC-7 (12) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-7(12)-1: host-based boundary protection using security groups | |
| Parameter SC-7(12)-2: AWS and cloud.gov system components | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-7 (12) What is the solution and how is it implemented? |
| --- |
| **AWS**  Cloud Operations configurescloud.gov AWS boundary protections, including:   * Each Amazon VPC is a distinct, isolated network within the cloud; network traffic within each Amazon VPC is isolated from all other Amazon VPCs. Each VPC is configured to utilize Routing Rules and VPC Peering, Subnet Rules, and Security Group Rules. Each of these controls must have appropriate rules and routes in-place before any external service is able to reach a host within cloud.gov. * Amazon EC2 provides a complete firewall solution (using AWS Security Groups). Cloud Operations manages AWS Security Group configuration according to our overall configuration management policy. This mandatory inbound firewall is configured in a default deny-all mode. The Cloud Operations team explicitly opens the ports needed to allow inbound traffic. The traffic is restricted by protocol, by service port, or source IP address (individual IP or Classless Inter-Domain Routing (CIDR) block). The firewall is configured in groups permitting different classes of instances to have different rules.   See SC-7 (a) for additional details about AWS boundary protections.  **cloud.gov**   * Cloud Operations implements host-based boundary protection by hardening virtual machines using guidelines from the Ubuntu CIS benchmark where applicable to our environment. * Host-based boundary protection for application services hosted on cloud.gov is provided by Cloud Foundry (CF) components. CF Application Security Groups (ASGs) control the traffic flowing out of applications. Each CF application uses a dedicated Linux container, and each container includes a dedicated virtual network interface. Application security groups are a collection of ‘allow’ rules that can be made with global or application specific assignments enabling access to be set on individual application requirements. These requirements are added through whitelisting and whitelisting is layered on top of a series of container-centric lock-downs, allowing limited access to other applications and services.   See SC-7 (a) for additional details about cloud.gov boundary protections. |

#### SC-7 (13) Control Enhancement (M)

The organization isolates [FedRAMP Assignment: See SC-7 (13) additional FedRAMP Requirements and Guidance] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

SC-7 (13) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

| SC-7 (13) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-7(13): key information security tools, mechanisms, and support components associated with system and security administration | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-7 (13) What is the solution and how is it implemented? |
| --- |
| Essential management facilities for operations, monitoring, deploying changes, alerting, and other administrative needs are isolated from customer-facing components via use of a separate Tooling VPC in AWS and a security group policy which prevents traversal from the production VPC to the Tooling VPC. |

#### SC-7 (18) Control Enhancement (M) (H)

The information system fails securely in the event of an operational failure of a boundary protection device.

| SC-7 (18) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-7 (18) What is the solution and how is it implemented? |
| --- |
| Boundary protection devices provided by AWS are the sole source of traffic into the VPC where our components reside, and are deployed redundantly. If they were to fail all at once, no traffic would be transmitted into the VPC where cloud.gov components reside. |

### SC-8 Transmission confidentiality and Integrity (M) (H)

The information system protects the [FedRAMP Assignment: confidentiality AND integrity] of transmitted information.

| SC-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-8: confidentiality and integrity of transmitted information | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-8 What is the solution and how is it implemented? |
| --- |
| cloud.gov provides integrity and confidentiality protection over data in transit by applying HTTPS to all public interfaces connecting to the service. See HTTPS (TLS) <https://tools.ietf.org/html/rfc5246> for details.  **cloud.gov**  HTTPS is forced for all connectivity to the system, HSTS (HTTP Strict Transport Security) is enabled, and the domain “cloud.gov” is preloaded in all major browsers to ensure that all connections are encrypted and are verified using a valid TLS certificate.  **Customer Responsibility**  HTTPS is also forced for customer applications, and HSTS is enabled by default. Customers are responsible for enabling stricter HSTS settings and asking browsers to preload their domains if that is required.  Obtaining the certificates for custom domains is a customer responsibility. cloud.gov ensures that the certificates are installed in a dedicated AWS Elastic Load Balancer. |

#### SC-8 (1) Control Enhancement (M) (H)

The information system implements cryptographic mechanisms to [FedRAMP Assignment: prevent unauthorized disclosure of information AND detect changes to information] during transmission unless otherwise protected by [FedRAMP Assignment: a hardened or alarmed carrier Protective Distribution System (PDS)].

| SC-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-8(1)-1: prevent unauthorized disclosure of information AND detect changes to information | |
| Parameter SC-8(1)-2: a hardened or alarmed carrier Protective Distribution System (PDS) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-8 (1) What is the solution and how is it implemented? |
| --- |
| cloud.gov requires use of HTTPS (TLS) for all public interfaces connecting to the service. HTTPS (TLS) uses cryptographic mechanisms to prevent unauthorized disclosure of information and prevent changes to information during transmission.  A hardened or alarmed carrier Protective Distribution System (PDS) is provided at the AWS CSP layer. See FedRAMP AWS CSP SSP for further details. |

### SC-10 Network Disconnect (M)

The information system terminates the network connection associated with a communications session at the end of the session or after [FedRAMP Assignment: no longer than thirty (30) minutes for RAS-based sessions and no longer than sixty (60) minutes for non-interactive user sessions] of inactivity.

| SC-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-10: no longer than 30 minutes for RAS-based sessions or no longer than 60 minutes for non-interactive user sessions | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-10 What is the solution and how is it implemented? |
| --- |
| cloud.gov terminates all network connections when sessions end. AWS ELBs are configured to terminate idle connections after 60 seconds of inactivity.  **Operator Access**  Connections to ephemeral jumpboxes used by Cloud Ops terminate after 10 minutes of inactivity. Cloud Ops configures this setting by configuring the `intercept\_idle\_timeout` parameter for Concourse at <https://github.com/18F/cg-deploy-concourse/blob/master/concourse.yml>  Connections from ephemeral jumpboxes used by Cloud Ops to virtual machines managed by BOSH terminate after 10 minutes of inactivity. Cloud Ops configures this setting using the `ClientAliveInterval` and `ClientAliveCountMax` parameters for SSH config at <https://github.com/18F/cg-harden-boshrelease/blob/master/src/harden/files/etc/ssh/sshd_config>  **Customer SSH Access**  cloud.gov offers customers SSH access to containers using an authenticated proxy.  Customer SSH connections to application instances terminate after 5 minutes of inactivity. This is the default configuration value of the IdleConnectionTimeout parameter at <https://github.com/cloudfoundry/diego-ssh/blob/master/cmd/ssh-proxy/config/config.go>  Users can disable SSH access on an individual space or app basis. |

### SC-12 Cryptographic Key Establishment & Management (L) (M) (H)

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

SC-12 Additional FedRAMP Requirements and Guidance:

Guidance: Federally approved and validated cryptography.

| SC-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-12: NIST requirements for key generation, distribution, storage, access, and destruction | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-12 What is the solution and how is it implemented? |
| --- |
| **cloud.gov External Connectivity**  Cloud Operations obtains certificates from two approved providers, COMODO (through SSLmate) and Let's Encrypt, to encrypt and verify public connections. The certificates are only stored in the AWS Identity and Access Management server certificate store to be used on Elastic Load Balancers. Cloud Operations doesn’t store public certificates or keys anywhere else and if necessary obtains new certificates using the same providers.  cloud.gov includes a service broker (<https://docs.cloudfoundry.org/services/api.html>) to automate the provisioning of TLS certificates for customer applications. The broker automatically stores the certificates and their private keys in AWS IAM (<http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_server-certs.html>). The broker associates the certificate with an Amazon CloudFront distribution (<https://aws.amazon.com/cloudfront/>) which handles the TLS termination for the custom domain and forwards traffic to an in-boundary ELB over a TLS v1.2 connection. This service relies on Let’s Encrypt (<https://letsencrypt.org/>) for automated TLS certificate issuance.  **cloud.gov Internal Connectivity**  Cloud Operations generates internal encryption keys and cryptographic certificates using the latest generally available version of OpenSSL. Cloud Operations encrypts and uploads server certificates and keys as secrets to AWS S3. Cloud Operations permanently destroys all local copies of these certificates. Concourse loads all secrets from S3, decrypts them, and uploads them to BOSH over an encrypted internal connection. BOSH in turn installs the certificates and keys into the hosts based on each service’s needs.  Cryptographic keys and certificates are rotated at least yearly. Once a new key/certificate pair is generated, the previous one is removed from S3 by overwriting the encrypted file. |

#### SC-12 (2) Control Enhancement (M) (H)

The organization produces, controls, and distributes symmetric cryptographic keys using [FedRAMP Selection: NIST FIPS-compliant] key management technology and processes.

| SC-12 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-12(2): NIST FIPS compliant key management | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-12 (2) What is the solution and how is it implemented? |
| --- |
| **cloud.gov external connectivity**  Public connections to cloud.gov terminate their TLS connections using AWS ELBs. AWS ELB uses FIPS 140-2 validated cryptographic modules. For more information about ELB TLS please refer to the GovCloud package  **cloud.gov internal connectivity**  Internal connections use the latest unmodified OpenSSL package to ensure that all the latest security vulnerabilities are patched. cloud.gov uses FIPS-compliant ciphers for the OpenSSL settings.  To fully comply with the notification requirement prescribed in 15 CFR 740.13, 18F notified the National Security Agency (NSA) and Commerce’s Bureau of Industry and Security (BIS) on April 28th, 2016 of this change, since the cloud.gov software is available and can be distributed globally. (Specifically, the 18F Director of Infrastructure sent email with details to crypt@bis.doc.gov and enc@nsa.gov, as directed by the regulation.)  None of the keys and certificates generated by Cloud Operations are distributed to other team members. Only automated systems have access to any cryptographic material. |

#### SC-12 (3) Control Enhancement (M) (H)

The organization produces, controls, and distributes asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user’s private key].

| SC-12 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-12(3): (not applicable) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-12 (3) What is the solution and how is it implemented? |
| --- |
| cloud.gov does not produce, control or distribute asymmetric cryptographic material. |

### SC-13 Use of Cryptography (L) (M) (H)

The information system implements [FedRAMP Assignment: FIPS-validated or NSA-approved cryptography] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

| SC-13 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-13: FIPS-validated cryptography | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-13 What is the solution and how is it implemented? |
| --- |
| **cloud.gov Application Cryptographic Protection**  cloud.gov forces all application to use HTTPS. Application, API and all traffic handled by cloud.gov is routed through an AWS ELB where the HTTPS connection is terminated.  For more information about ELB TLS please refer to the GovCloud package. Also, See <https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf> for further details.  **cloud.gov Internal Cryptographic Protection**  cloud.gov does not use OpenSSL FIPS Object Module because the latest, patched version of OpenSSL does not include the OpenSSL FIPS Object Module. However, cloud.gov uses FIPS-compliant ciphers for the OpenSSL settings.  cloud.gov uses the latest available OpenSSL version and updates it to new versions of OpenSSL as they get released, so that cloud.gov has the fullest possible set of security patches. Due to the frequency of vulnerabilities being discovered in OpenSSL, cloud.gov reduces overall security risk by using the latest versions instead of staying on older (validated) versions. |

### SC-15 Collaborative Computing Devices (M) (H)

The information system:

1. Prohibits remote activation of collaborative computing devices with the following exceptions:[FedRAMP Assignment: no exceptions] and
2. Provides an explicit indication of use to users physically present at the devices.

SC-15 Additional FedRAMP Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

| SC-15 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-15(a): Not applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov has no collaborative computing devices. |
| Part b | Not applicable. See above. |

SC-15 Additional FedRAMP Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

| SC-15 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | Not applicable. See above. |

### SC-17 Public Key Infrastructure Certificates (M) (H)

The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.

| SC-17 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-17: None | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-17 What is the solution and how is it implemented? |
| --- |
| Cloud Operations issues no public key certificates. Instead, Cloud Operations obtains certificates from two providers approved by 18F Infrastructure: COMODO (through SSLmate) and Let's Encrypt. |

### SC-18 Mobile Code (M) (H)

The organization:

1. Defines acceptable and unacceptable mobile code and mobile code technologies;
2. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
3. Authorizes, monitors, and controls the use of mobile code within the information system.

| SC-18 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The cloud.gov team uses JavaScript as part of user-facing web applications, including the main cloud.gov website and its web user interface (dashboard).  As part of the cloud.gov Delivery Process (<https://github.com/18F/cg-product/blob/master/DeliveryProcess.md> ) and Configuration Management Plan ( <https://cloud.gov/docs/ops/configuration-management/> ), the cloud.gov team evaluates all proposed new code for security impact, which includes evaluating the programming languages / technologies used in that code. For details about these processes, see CM-3 and CM-4. |
| Part b | cloud.gov evaluates all code and technologies before integrating them with the cloud.gov system, including mobile code and mobile code technologies. For details about these processes, see CM-3 and CM-4. |
| Part c | cloud.gov uses its Delivery Process and Configuration Management Plan to authorize, monitor, and control the use of all code in the cloud.gov system. For details about these processes, see CM-3 and CM-4. |

### SC-19 Voice Over Internet Protocol (M) (H)

The organization:

1. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
2. Authorizes, monitors, and controls the use of VoIP within the information system.

| SC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Not applicable. VoIP is not used in or for cloud.gov. |
| Part b | Not applicable. See above. |

### SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H)

The information system:

1. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
2. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

| SC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, Application System Owner | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **cloud.gov**  By using and configuring AWS Route 53, cloud.gov combines DNS management with our HTTP Strict Transport Security (HSTS) endpoints to achieve data origin authentication and integrity verification along with the authoritative name resolution data the system returns in response to external name/address resolution queries.  18F does not implement DNSSEC. HTTPS serves as an alternative and compensating control, providing all of the same security assertions, and more. By implementing HTTPS in this fashion, any successful DNS poisoning would cause the system to fail into a "closed state" and throw an error in the browser, such that our systems could not be impersonated.  **Customer Responsibility**  For customer applications, customers are responsible for selecting a name resolution service that fulfills this requirement and any requirements of their respective agency. cloud.gov requires HTTPS for all applications regardless of the name resolution service provided. See <https://cloud.gov/docs/apps/custom-domains/> . |
| Part b | **cloud.gov**  cloud.gov implements HSTS with “includeSubDomains” option to ensure that child zones are also protected by HSTS protection. Moreover, the domain name “cloud.gov” has been pre-loaded in modern browsers to require HTTPS.  **Customer Responsibility**  For customer applications, customers are responsible for selecting a name resolution service that fulfills this requirement and any requirements of their respective agency. cloud.gov requires HTTPS for all applications regardless of the name resolution service provided. See <https://cloud.gov/docs/apps/custom-domains/> . (Same as SC-20, part a.) |

### SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H)

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

| SC-21 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-21 What is the solution and how is it implemented? |
| --- |
| For application name resolution (finding names outside of the cloud.gov environment), cloud.gov uses AWS EC2 name servers. cloud.gov relies on EC2 name servers to perform data origin authentication and data integrity verification for name/address resolution responses. |

### SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H)

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

| SC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-22 What is the solution and how is it implemented? |
| --- |
| **cloud.gov External DNS**  cloud.gov implements Route 53 exclusively for external DNS services. Route 53 DNS utilizes multiple servers using weighted round-robin DNS. See <https://aws.amazon.com/route53/> for further details.  **cloud.gov Internal DNS**  Internally cloud.gov implements PowerDNS and Consul to resolve the names of internal cloud foundry components. These internal systems are not accessible from the internet and are managed using our configuration management policy (  <https://cloud.gov/docs/ops/configuration-management/> ).  **Customer Responsibility**  Customers are responsible for managing their own DNS services. Public name resolution is not a service provided by cloud.gov. |

### SC-23 Session Authenticity (M) (H)

The information system protects the authenticity of communications sessions.

| SC-23 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-23 What is the solution and how is it implemented? |
| --- |
| cloud.gov protects the authenticity of sessions by exclusively using HTTPS. All traffic is communicated via HTTPS utilizing cryptographic algorithms in TLS. In addition, the cloud.gov domain is configured to utilize HTTP Strict Transport Security (HSTS), which declares that web browser should only interact with cloud.gov using secure HTTPS connections. |

### SC-28 Protection of Information at Rest (M) (H)

The information system protects the [FedRAMP Selection: confidentiality AND integrity]] of [Assignment: organization-defined information at rest].

SC-28 Additional FedRAMP Requirements and Guidance:

Guidance: The organization supports the capability to use cryptographic mechanisms to protect information at rest.

| SC-28 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-28-1: confidentiality AND integrity | |
| Parameter SC-28-2: system and customer data at rest | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-28 What is the solution and how is it implemented? |
| --- |
| **System Configuration Information and Other Sensitive Data**  EBS volumes, RDS, and S3 buckets are encrypted at rest. This uses built-in AWS features, documented by AWS:   * **EBS:** “Your data and associated keys are encrypted using the industry-standard AES-256 algorithm.” - <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html> * **S3:** AES-256 - <http://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html> * **RDS:** AES-256 - <http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>   All system information is in these components.  **Customer Application Databases**  EBS volumes, RDS, and S3 buckets are encrypted at rest, with the same AWS technology as system information.  **Customer Responsibility**  If desirable, customers are responsible for further encrypting any sensitive information in their customer applications before it is written to storage components or databases. |

#### SC-28 (1) Control Enhancement (M)

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) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SC-28(1)-1: internet traffic, system data, customer data | |
| Parameter SC-28(1)-2: ELBs, EBS volumes, RDS, S3 buckets | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-28 (1) What is the solution and how is it implemented? |
| --- |
| The following cryptographic mechanisms are used to prevent unauthorized disclosure and modification of data during transmission and in storage.  **Internet Traffic**  Applications running on Cloud Foundry receive requests through the URLs configured for the application. HTTP requests arrive on ports 80 and 443. Additionally, Cloud Foundry requires a channel for TCP/WebSocket traffic. The default cf-release manifest assigns port: 4443 for TCP/WebSocket communications.  All traffic from the public internet to the Cloud Controller and UAA happens over HTTPS. Inside the boundary of the system, components communicate over a publish-subscribe (pub-sub) port: 4222 message bus, NATs.  **System Configuration Information and Other Sensitive Data**  EBS volumes, RDS, and S3 buckets are encrypted at rest. All system information is in these components, including configuration information.  **Authentication Information**  For people: cloud.gov accounts are delegated to agency single-sign-on accounts.  For machine users: Machine user account information (service accounts, such as deployer accounts) is stored in the UAA database. Operators configure encryption of the identity store in the UAA. When users register an account with the Cloud Foundry platform, the UAA acts as the user store and stores user passwords in the UAA database using bcrypt. Bcrypt is a blowfish encryption algorithm, which enables Cloud Foundry to store a secure hash of users' passwords.  cloud.gov does not create, store or process any personally identifiable information (PII).  **Customer Application Configuration Information**  The Cloud Controller stores the configuration for an application in an encrypted database table. This configuration data includes user-specified environment variables and service credentials for any services bound to the app. Application developers push their code using the cloud.gov API. Cloud Foundry secures each call to the CF API using the UAA and TLS.  **Customer Application Databases**  EBS volumes, RDS, and S3 buckets are encrypted at rest.  **Customer Responsibility**  Customers are responsible for further securing/encrypting any sensitive information in their customer applications, and for auditing the permissions their users have for managing their applications. |

### SC-39 Process Isolation (L) (M) (H)

The information system maintains a separate execution domain for each executing process.

| SC-39 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SC-39 What is the solution and how is it implemented? |
| --- |
| cloud.gov maintains a separate execution domain for each executing process by running within its own self-contained environment, a Garden container that isolates processes, memory, network, and the file system. Network traffic for each container flows through a dedicated interface to which container-specific ingress and egress rules can be applied.  In addition, the Garden containers provide each process with its own private, virtual address space. These virtual address spaces are completely separate from one another, so a process running one application cannot affect another.  Processes in Garden containers are restricted from writing to system-related device nodes, and they are unable to use a host of Linux kernel ABI facilities, limiting the surface area available in attempts to escape the container. Further details on hardening precautions are available in the Cloud Foundry documentation: <https://docs.cloudfoundry.org/concepts/container-security.html#hardening> |

## System and Information Integrity (SI)

### SI-1 System and Information Integrity Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
2. Reviews and updates the current:
   1. System and information integrity policy [FedRAMP Assignment: at least every three (3) years]; and
   2. System and information integrity procedures [FedRAMP Assignment: at least at least annually].

| SI-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), System Owner | |
| Parameter SI-1(a): cloud.gov development and design team | |
| Parameter SI-1(b)(1): At least every three years | |
| Parameter SI-1(b)(2): At least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SI-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The General Services Administration (GSA) distributes corporate policies and procedures. GSA has a corporate IT Security Policy for this control across the entire agency: <https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf>  18F maintains policies (which are cross-references to the GSA IT Security Policy) and system-specific procedures in an official repository on GitHub, which are distributed to all cloud.gov development and design team members as part of team onboarding. See <https://github.com/18F/compliance-docs/blob/master/SI-Policy.md> for the System and Information Integrity procedures. 18F lists any system-specific procedures at the bottom of each policy document in the GitHub repository. |
| Part b | GSA reviews and updates the corporate IT Security Policy at least every 3 years, as described in the policy itself: “The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it.”  The cloud.gov team reviews and updates the system-specific procedures at least annually, as part of the FedRAMP annual authorization process. |

### SI-2 Flaw Remediation (L) (M) (H)

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 [FedRAMP Assignment: thirty 30 days of release of updates] of the release of the updates; and
4. Incorporates flaw remediation into the organizational configuration management process.

| SI-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-2(c) within 30 days of release of updates | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The cloud.gov team identifies all system flaws related to cloud.gov, reports system flaws to Information System Owners, Authorizing Officials, Cloud Operations, and GSA Information Security, and corrects system flaws.  cloud.gov uses two main automated methods to identify, report, and correct flaws:  **1) Keeping core software updated:**  cloud.gov continuously updates Cloud Foundry releases and BOSH stemcells to keep cloud.gov core software up to date with upstream security patches. The Cloud Foundry open source project creates Cloud Foundry releases with updates to address code issues, and it creates new stemcells with patches for the latest security fixes to address any underlying operating system issues. New Cloud Foundry releases are located at <https://github.com/cloudfoundry/cf-release>. (The Cloud Operations team can also generate local versions of these assets to provide flaw mitigation when an upstream fix is not yet available.)  Concourse automatically detects, tests, and deploys Cloud Foundry updates and stemcell (operating system) updates. Cloud Operations configures and monitors Concourse to ensure proper operation of this automatic system.  **2) Scanning software:**  cloud.gov implements a comprehensive range of automated scanning tools to identify potential system flaws, including Code Climate, OWASP ZAP, Nessus, and ClamAV. These scanning tools report findings to Cloud Operations via automated methods including PagerDuty and email, and Cloud Operations corrects any identified flaws.  For details about Nessus and OWASP ZAP, see section 10.3 (*Vulnerability scanning and penetration testing*) and RA-5. For details about ClamAV and Code Climate, see SI-3 and related controls such as SI-3 (1) and SI-3 (2). |
| Part b | Prior to operating system and software patch deployment in our production environment: all patches (including flaw remediation patches) are installed and tested in our staging environments for assessment to determine if patch deployment causes issues or anomalies. BOSH automatically validates configurations, and Concourse automatically runs unit tests and acceptance tests. |
| Part c | cloud.gov installs security-relevant software and firmware updates within 30 days of release of updates. This is primarily managed by the automatic Concourse updates of Cloud Foundry, as described in part a, and further ensured by the automated Nessus and OWASP ZAP scans that detect potential vulnerabilities.  And as stated in RA-5, high-risk vulnerabilities must be mitigated within 30 days; moderate-risk vulnerabilities mitigated within 90 days; low-risk vulnerabilities mitigated within 180 days; and all findings that are not remediated immediately are tracked in the cloud.gov Plan of Action and Milestones (POAM). |
| Part d | All changes to cloud.gov-developed code are managed through the Configuration Management Plan ( <https://cloud.gov/docs/ops/configuration-management/> ), as described in CM-9. This includes changes for flaw remediation. |

#### SI-2 (2) Control Enhancement (M) (H)

The organization employs automated mechanisms [FedRAMP Assignment: at least monthly] to determine the state of information system components with regard to flaw remediation.

| SI-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-2(2): At least monthly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-2 (2) What is the solution and how is it implemented? |
| --- |
| The Cloud Operations team employs the following automated mechanisms to determine the state of information system components with regard to flaw remediation:  **cloud.gov Custom Code**  Code Climate scans all proposed 18F or GSA originated code (in the form of scanning the code in each GitHub pull request) before integration into the cloud.gov system, so that cloud.gov team members must remediate identified flaws before integrating the code. See RA-5 for detail.  **cloud.gov Web Application Components**  For components of the cloud.gov system that are run as web applications on the platform by the cloud.gov team (for example login.fr.cloud.gov, dashboard.fr.cloud.gov, etc.): The Cloud Operations team runs manual monthly internal web scans using the OWASP ZAP web vulnerability scanner. (See RA-5 for detail.) Any flaws identified with these scans are tracked in the Plan of Action and Milestones (POAM).  **cloud.gov Platform**  GSA Information Security maintains a centralized Nessus Manager / Tenable Security Center for the agency, to assist them in determining the state of systems across the agency.  The Cloud Operations team runs monthly internal vulnerability assessments on operating systems and databases using Nessus.  Any flaws identified with these scans are tracked in the Plan of Action and Milestones (POAM). See RA-5 for detail. |

#### SI-2 (3) Control Enhancement (M) (H)

The organization:

1. Measures the time between flaw identification and flaw remediation; and
2. Establishes [Assignment: organization-defined benchmarks] for taking corrective actions.

| SI-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-2(3)(b): time benchmarks based on the GSA IT Security Policy | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-2 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov tracks the time between flaw identification and remediation in its Plan of Actions and Milestones (POAM), updated at least monthly as part of FedRAMP Continuous Monitoring. A cloud.gov team member manually updates the POAM with information from both automated scans and any manually-identified flaws. |
| Part b | Benchmarks for flaw remediation are described in RA-5 part d: The *GSA IT Security Policy* mandates that Critical and High risk findings be addressed within 30 days. Moderate risk findings are mandated to be addressed within 90 days. As required by FedRAMP, Low risk findings are addressed within 180 days. |

### SI-3 Malicious Code Protection (L) (M)

The organization:

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:
   1. Perform periodic scans of the information system [FedRAMP Assignment: at least weekly] and real-time scans of files from external sources at [FedRAMP Assignment: to include endpoints] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
   2. [FedRAMP Assignment: to include alerting administrator or defined security personnel] in response to malicious code detection; and
4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

| SI-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-3(c)(1)-1: at least weekly | |
| Parameter SI-3(c)(1)-2: at information system entry and exit points | |
| Parameter SI-3(c)(2): to include alerting administrator or defined security personnel | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov employs ClamAV to detect and quarantine malicious code within the cloud.gov system in the cloud.gov authorization boundary. ClamAV runs at the host level (on each virtual machine), where it scans all file content as soon as the file is modified.  All 18F-developed open source code that is used in the cloud.gov system is scanned using static analysis tools from Code Climate. Cloud Operations configures the Code Climate static analysis service to run on all 18F GitHub repositories that hold 18F-developed cloud.gov source code. When anyone proposes a change (in the form of a GitHub pull request) to an 18F-developed component that cloud.gov depends on, the Code Climate service automatically runs its static analysis tool on the change. |
| Part b | All virtual machines running ClamAV use its built-in FreshClam daemon to fetch updated virus definitions hourly.  Code Climate is a Software as a Service that is continuously updated. |
| Part c | Cloud Operations configures ClamAV in cloud.gov to provide real-time scans of cloud.gov, which are done continuously. If ClamAV detects malicious code, ClamAV identifies the virus in the file and quarantines it. Then ClamAV sends a notification to Cloud Operations through Prometheus (which sends alerts via PagerDuty).  Code Climate provides scanning of proposed custom code for the cloud.gov platform before the code is integrated into the system, as described in part a. Code Climate displays scan result information in two ways:   1. On the GitHub pull request page (since it integrates with the GitHub service). These results are reviewed by a cloud.gov team member before they decide whether to approve “merge” (integrate) the pull request; for repositories configured to only allow Cloud Operations team members to approve and merge pull requests (such as core platform configuration repositories), a Cloud Operations team member must review the results as part of reviewing the pull request. 2. Static analysis scan results are stored in the Code Climate tool, so that the Cloud Operations team can see static analysis results for all changes introduced to the system by 18F-developed components. |
| Part d | When PagerDuty notifies Cloud Operations of a potential incident (such as one identified by ClamAV), a Cloud Operations team member investigates the report as described in the Incident Response guide ( <https://cloud.gov/docs/ops/security-ir/> ). If the Cloud Operations team member determines that the report is a false positive, they manually resolve the alert in the PagerDuty console. Cloud Operations verifies that a potential incident is genuine before taking systems offline, so that false positives do not affect the availability of cloud.gov.  When Cloud Operations identifies a false positive in Code Climate scan results, they use the workflow tools provided by the Code Climate scanning software to flag the erroneous result, which prevents it from appearing in future scans. |

#### SI-3 (1) Control Enhancement (M) (H)

The organization centrally manages malicious code protection mechanisms.

| SI-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-3 (1) What is the solution and how is it implemented? |
| --- |
| ClamAV is installed on all virtual machines using BOSH, as configured by the Cloud Operations team. Once ClamAV is installed, it uses its built-in FreshClam daemon to automatically fetch updated virus definitions hourly.  Cloud Operations configures ClamAV to send alerts using Prometheus and PagerDuty, which is our centralized alerting system. ClamAV sends alerts for detected potential malicious activity, as well as sending alerts if the scan did not successfully run.  Each alert in PagerDuty remains unresolved until Cloud Operations takes action to mark it resolved. The PagerDuty console provides an overview (dashboard) of unresolved alerts from ClamAV and other scans. |

#### SI-3 (2) Control Enhancement (M) (H)

The information system automatically updates malicious code protection mechanisms.

| SI-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-3 (2) What is the solution and how is it implemented? |
| --- |
| All virtual machines running ClamAV use its built-in FreshClam daemon to fetch updated definitions hourly. |

#### SI-3 (7) Control Enhancement (M) (H)

The information system implements nonsignature-based malicious code detection mechanisms.

| SI-3 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-3 (7) What is the solution and how is it implemented? |
| --- |
| ClamAV uses multiple host-based inspection engines, including bytecode detection and logic conditionals. As the cloud.gov system continues to operate and scale, additional tools that use heuristics methods are deployed in order to detect deviance from acceptable baseline behavior. |

### SI-4 Information System Monitoring (L) (M) (H)

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
   2. Unauthorized local, network, and remote connections;
2. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
3. 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;
4. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
5. 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;
6. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
7. 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-4 Additional FedRAMP Requirements and Guidance:

Guidance: See US-CERT Incident Response Reporting Guidelines.

| SI-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-4(a)(1): the GSA IT Security Policy | |
| Parameter SI-4(b): network and host-based monitoring | |
| Parameter SI-4(g)-1: cloud.gov system metrics | |
| Parameter SI-4(g)-2: Cloud Operations, ISSO, ISSM, System Owner | |
| Parameter SI-4(g)-3: On an as-needed basis | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The Cloud Operations team monitors the cloud.gov system (within the cloud.gov authorization boundary) to detect potential attacks and intrusions in accordance with *GSA IT Security Policy* Chapter 4, *Policy on Operational Controls* (linked from <https://github.com/18F/compliance-docs/blob/master/SI-Policy.md> ) and the FedRAMP Incident Communication procedures (linked from <https://www.fedramp.gov/documents/> ). |
| Part b | Cloud Operations identifies un-authorized access to the cloud.gov system using automated monitoring tools within its Virtual Private Cloud for monitoring, log management and event analysis. Cloud Operations monitors for attacks and indicators of potential attacks, unauthorized local, network, and remote connections.  cloud.gov utilizes CloudTrail, CloudWatch, CloudWatch Logs, and Prometheus to identify unauthorized use of the information system. Prometheus detects any unauthorized instances, applications, or access within cloud.gov’s AWS environment. Prometheus aggregates various audit logs and alerts based on abnormal activity or attacks within the cloud.gov platform as a service. The CloudTrail service logs all unauthorized access or connections to EC2 instances from within the AWS virtual private network. |
| Part c | The infrastructure that hosts cloud.gov provides monitoring and intrusion detection of unusual activity at the physical and network layers. Cloud Operations is responsible for monitoring everything related to the cloud.gov virtual infrastructure and has deployed ClamAV, Snort, and Tripwire within its Virtual Private Cloud to log and detect malicious activities. |
| Part d | The cloud.gov Program Manager and System Owner ensure intrusion and monitoring tools are protected from unauthorized access by only granting access to certain members from the Cloud Operations team. All monitoring and intrusion information data is protected by limiting accounts to authorized privileged users only and is maintained in secured repositories for review by those members. |
| Part e | The cloud.gov team uses additional sources such as Pivotal, US-CERT Advisories, OMB Mandates, commercial and open source security communities, and other sources to provide indication of increased risk to organizational operations and assets, individuals, other organizations. The level of monitoring activity and manual inspection performed is adjusted commensurate with the alerts received. |
| Part f | Information system monitoring is conducted in accordance and compliance with 18F security policies and all applicable laws, Executive Orders, directives, and regulations. |
| Part g | The cloud.gov system and team monitor all information system components. In the event of an event or incident, information will be provided as it is available. Scheduled reports will be provided for events such as after-hours administrative logins, users being added to privileged groups, persistent malware detections, etc., to designated members of the Cloud Operations team as needed. |

#### SI-4 (1) Control Enhancement (M) (H)

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

| SI-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-4 (1) What is the solution and how is it implemented? |
| --- |
| cloud.gov uses three principal security tools to facilitate constant monitoring and intrusion detection of the system. Tripwire looks for system-provisioned files that have been modified. Snort looks for suspicious patterns of traffic on the host network interface. ClamAV looks for attack signatures in all files (even those related to customer code). Tripwire, Snort, and ClamAV work in concert to provide monitoring and alerting of system anomalies that may indicate an intrusion. Cloud Operations uses BOSH to configure and deploy the three security tools to all EC2 instances (all cloud.gov virtual machines).  All potential incidents identified by these tools are shipped to a centralized system, Prometheus. Prometheus is an event stream processor that uses heuristics for deciding when events warrant sending alerts. Since our logs and events are funneled through it, Prometheus acts as a log correlation tool via real-time analysis rather than post-incident correlation. Prometheus sends alert information to a database and a centralized notification system (PagerDuty).  See SI-6 for more detail about these individual tools. |

#### SI-4 (2) Control Enhancement (M) (H)

The organization employs automated tools to support near real-time analysis of events.

| SI-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-4 (2) What is the solution and how is it implemented? |
| --- |
| Cloud Operations uses BOSH to configure and deploy Prometheus to support near real-time analysis of events. Prometheus continuously analyzes metrics and logs from various cloud.gov components and alerts Cloud Operations via PagerDuty when an anomaly is detected.  Prometheus makes use of system performance metrics (gathered via collectd), Cloud Foundry metrics, BOSH health monitor state changes, Snort alerts, Tripwire alerts, ClamAV alerts, and AWS metrics and system lists. Cloud Operations configures Prometheus with a list of rules that process the inputs. See AC-2 (12) for additional detail on anomaly detection. See also diagram 10-4.3 (Monitoring and Alerting Data Flow). |

#### SI-4 (4) Control Enhancement (M) (H)

The information system monitors inbound and outbound communications traffic [FedRAMP Assignment: continuously] for unusual or unauthorized activities or conditions.

| SI-4 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-4(4): continually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-4 (4) What is the solution and how is it implemented? |
| --- |
| The Cloud Operations team uses Snort to monitor inbound and outbound communications traffic continually for unusual or unauthorized activities or conditions within the cloud.gov information system. Cloud Operations uses a set of Snort rules (maintained by the Snort community) that are continuously updated (every hour) using Concourse. |

#### SI-4 (5) Control Enhancement (M) (H)

The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].

SI-4(5) Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with the incident response plan.

| SI-4 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-4(5)-1: Cloud Operations and Information Systems Security Officer (ISSO)s | |
| Parameter SI-4(5)-2: Snort or ClamAV alerts; or a system metric exceeds a defined threshold | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-4 (5) What is the solution and how is it implemented? |
| --- |
| The cloud.gov system uses Prometheus for host-based monitoring and alerting. Prometheus sends an alert via PagerDuty to Cloud Operations when the following events happen:   * Each time Snort, Tripwire, or ClamAV identify a potential incident. * Each time CPU, memory, disk usage, or swap usage exceed defined thresholds (Cloud Operations configures these thresholds to reflect ordinary usage).   If Cloud Operations identifies an alert as indicating compromise or potential compromise (such as security breach, insider threat, phishing, data leakage, or denial of service), they will follow the cloud.gov Security Incident Response Guide ( <https://cloud.gov/docs/ops/security-ir/> ). This guide includes reporting the potential incident to appropriate authorities at 18F and GSA, who will further escalate the potential report if appropriate. |

#### SI-4 (14) Control Enhancement (M) (H)

The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

| SI-4 (14) | Control Summary Information |
| --- | --- |
| Responsible Role: AWS GovCloud | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-4 (14) What is the solution and how is it implemented? |
| --- |
| cloud.gov is completely virtualized via AWS GovCloud. There are no direct network paths between GSA wireless access points and cloud.gov. Therefore, cloud.gov completely leverages the Provisional Authorization for AWS GovCloud for this control. |

#### SI-4 (16) Control Enhancement (M) (H)

The organization correlates information from monitoring tools employed throughout the information system.

| SI-4 (16) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-4 (16) What is the solution and how is it implemented? |
| --- |
| The cloud.gov team correlates security information from monitoring tools with Prometheus, PagerDuty, and Grafana.  All cloud.gov monitoring and alerting tools send information through Prometheus, which sends alerts to both Cloud Operations team members (via PagerDuty) and also stores the information in a database for display by Grafana.  Grafana is a visualization tool that displays metrics data about many aspects of cloud.gov, including Cloud Foundry components (including errors and overall application information, such as number of running applications) and CPU/memory/disk usage across virtual machines. |

#### SI-4 (23) Control Enhancement (M) (H)

The organization implements [Assignment: organization-defined host-based monitoring mechanisms] at [Assignment: organization-defined information system components].

| SI-4 (23) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-4(23)-1: host-based monitoring systems | |
| Parameter SI-4(23)-2: at the cloud.gov container and application level | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-4 (23) What is the solution and how is it implemented? |
| --- |
| The Cloud Operations team has implemented host-based monitoring and alerting, using the following tools to collect events from all the servers and applications:   * AWS CloudWatch: performance metrics * ClamAV: malicious code detection * Snort: network intrusion detection system (IDS) * Tripwire: intruder detection / file integrity * Nessus: patch / vulnerability scanning   Prometheus receives metrics. If a system metric exceeds a defined threshold, Prometheus raises the alert to the team via PagerDuty so that the team can take action. There is a Prometheus client on each system to extend these alerts as needed. |

### SI-5 Security Alerts & Advisories (L) (M) (H)

The organization:

1. Receives information system security alerts, advisories, and directives from [FedRAMP Assignment: to include US-CERT] on an ongoing basis;
2. Generates internal security alerts, advisories, and directives as deemed necessary;
3. Disseminates security alerts, advisories, and directives to [FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities]; and
4. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

| SI-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations, GSA Information Security | |
| Parameter SI-5(a): US-CERT | |
| Parameter SI-5(c) System Owner, ISSM, ISSO, Cloud Operations, Authorizing Official | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | GSA Information Security and cloud.gov’s ISSM, ISSO, and Authorizing Official receive alerts, advisories, and directives from US-CERT. |
| Part b | GSA Information Security generates internal security alerts, advisories, and directives as deemed necessary for any system that GSA is aware of, not limited to cloud.gov components. |
| Part c | GSA Information Security sends alerts and directives to all relevant staff, including Cloud Operations, via email. Depending on the nature of the alert or advisory, GSA Information Security may send an alert email to additional management and staff. |
| Part d | Cloud Operations implements security directives in accordance with the requested time frames, or notifies the issuing organization of the degree of noncompliance. Normal processes for backlog management incorporate urgency and risk when determining prioritization of security implementation and remediation activity. |

### SI-6 Security Functionality Verification (M) (H)

The information system:

1. Verifies the correct operation of [Assignment: organization-defined security functions];
2. Performs this verification [FedRAMP Assignment: to include upon system startup and/or restart at least monthly];
3. Notifies [FedRAMP Assignment: to include system administrators and security personnel] of failed security verification tests; and
4. [Selection (one or more): shuts the information system down; restarts the information system; [FedRAMP Assignment: to include notification of system administrators and security personnel] when anomalies are discovered.

| SI-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-6(a): services that detect malicious code, viruses, file integrity, network traffic, and security compliance of the OS | |
| Parameter SI-6(b): upon system startup and/or restart at least monthly | |
| Parameter SI-6(c): system administrators and security personnel (specifically Cloud Operations, System Owner, and GSA IT) | |
| Parameter SI-6(d)-1: isolates affected components | |
| Parameter SI-6(d)-2: system administrators and security personnel (specifically members of the Cloud Operations team, who notify other relevant staff) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov verifies the correct operation of services that detect malicious code, viruses, file integrity, network traffic, and security compliance of the OS using a continuous integration tool called Concourse.  Cloud Operations configures Concourse acceptance tests (also called “smoke tests” and “integration tests”) to test for expected operation of a comprehensive range of cloud.gov functionality, including security functions related to: authentication and authorization, roles and permissions, creating and deleting spaces, pushing and deleting applications, and regressions. |
| Part b | cloud.gov performs verification of correct operation continuously (daily or more often) using:   * BOSH - When BOSH deploys software to a virtual machine, it verifies deployments using checksums to ensure correctness. (This is the health monitor check.) * Tripwire - Performs file alteration checks on all cloud.gov virtual machines on initial deploy and a daily basis thereafter, and records all data to CloudWatch Logs. * Nessus - Performs host audit against malicious code and known vulnerabilities (daily). * Snort - Performs network audit against malicious traffic. (This inspects network activity on a continuous basis.) * ClamAV - Performs host audit against malicious code. (This runs continuously; files are scanned when they are written/accessed.) |
| Part c | The Cloud Operations team is notified of a failure in security verification via PagerDuty (SMS/phone and email pages), which contain specific detail regarding the job name, host name and a description of where the failure occurred.  The cloud.gov team notifies the cloud.gov System Owner and GSA IT via email and the Incident Response Process in the event that potential incidents are detected. |
| Part d | When anomalies are discovered, Cloud Operations is paged via PagerDuty. As described in the Security Incident Response Guide ( <https://cloud.gov/docs/ops/security-ir/> ). Cloud Operations isolates affected components from the rest of system using AWS security groups. Once Incident Response is complete, Cloud Operations terminates the host and removes it from the environment. |

### SI-7 Software & Information Integrity (M) (H)

The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].

| SI-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-7: all hosts | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-7 What is the solution and how is it implemented? |
| --- |
| cloud.gov employs Tripwire to detect unauthorized changes to cloud.gov hosts (virtual machines) within the cloud.gov authorization boundary. Tripwire performs file integrity checks on the host OS and all deployed software on all cloud.gov EC2 instances upon initial deploy and a daily basis thereafter, and records all data to CloudWatch Logs. |

#### SI-7 (1) Control Enhancement (M) (H)

The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [FedRAMP Selection (one or more): at startup; at [FedRAMP Assignment: to include security-relevant events]; [FedRAMP Assignment: at least monthly]].

| SI-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-7(1)-1: cloud.gov software and information | |
| Parameter SI-7(1)-2: to include security-relevant events | |
| Parameter SI-7(1)-3: at least monthly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-7 (1) What is the solution and how is it implemented? |
| --- |
| cloud.gov performs the following checks to deter and detect unauthorized changes to software and information within the cloud.gov authorization boundary:   * **Software changes:** Tripwire runs at startup and each day, reviewing files and logging changes which are sent to central logging for indefinite retention. Specifically, Tripwire contains a whitelist of system files (static operating system components and files intentionally deployed during system provisioning) to monitor and alert on changes; it ignores log file updates and database data. * **Firmware changes:** Amazon periodically upgrades host firmware and retires (reboots) a physical host running our VM instances. When the host is retired, cloud.gov automatically replaces the VM instances by deploying new instances onto another host. Any change to firmware requiring a reboot will result in the same behavior. * **Operating system changes:** Operating system image updates are delivered as part of a hardened, minimal stemcell image from the upstream Cloud Foundry project. A new stemcell release causes a redeployment by Concourse. Each stemcell deployment results in BOSH terminating existing instances and creating new, previously unused instances in their place.   Any changes to deployed instances are monitored by Tripwire, ClamAV, Nessus, Snort, and BOSH. See SI-4 (1) for additional details. |

#### SI-7 (7) Control Enhancement (M) (H)

The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.

| SI-7 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-7(7): file alterations (including configuration changes), network access | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-7 (7) What is the solution and how is it implemented? |
| --- |
| **AWS Responsibility**  AWS is responsible for controlling the firmware installed in physical hardware underlying the system.  **cloud.gov Responsibility**  Tripwire, Snort, and ClamAV run automatically at intervals on all hosts. See SI-4 (23) for additional detail on the kinds of changes that these tools will identify as potential incidents. When they identify potential incidents these tools log alerts to the local syslog agent. The syslog agent sends logs through a centralized system (Prometheus) that sends the information about alerts to a database and a centralized notification system (PagerDuty), as well as CloudWatch Logs. When Cloud Operations is notified of a potential incident via PagerDuty, an engineer investigates the report as described in the Incident Response guide ( <https://cloud.gov/docs/ops/security-ir/> ). |

### SI-8 Spam Protection (M) (H)

The organization:

1. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
2. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policies and procedures.

| SI-8 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | This control is not applicable since cloud.gov does not accept or process any messages for other information systems or external sources. Therefore, spam protection is not necessary.  **Customer Responsibility**  If a customer application accepts or processes messages, the Application System Owner is responsible for fulfilling this requirement. |
| Part b | This control is not applicable since cloud.gov does not accept or process any messages for other information systems or external sources. Therefore, spam protection is not necessary.  **Customer Responsibility**  If a customer application accepts or processes messages, the Application System Owner is responsible for fulfilling this requirement. |

#### SI-8 (1) Control Enhancement (M) (H)

The organization centrally manages spam protection mechanisms.

| SI-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-8 (1) What is the solution and how is it implemented? |
| --- |
| This control is not applicable since cloud.gov does not accept or process any messages for other information systems or external sources. Therefore, spam protection is not necessary.  **Customer Responsibility**  If a customer application accepts or processes messages, the Application System Owner is responsible for fulfilling this requirement. |

#### SI-8 (2) Control Enhancement (M) (H)

The organization automatically updates spam protection mechanisms.

| SI-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-8 (2) What is the solution and how is it implemented? |
| --- |
| This control is not applicable since cloud.gov does not accept or process email for other information systems or external sources.  **Customer Responsibility**  If a customer application accepts or processes email, the Application System Owner is responsible for fulfilling this requirement. |

### SI-10 Information Input Validation (M) (H)

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

| SI-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-10: customer input | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-10 What is the solution and how is it implemented? |
| --- |
| **cloud.gov Web User Interface (Dashboard)**  The cloud.gov web user interface (dashboard) is the only 18F-developed custom code where users and administrators can provide input.  Customers use the dashboard to manage their applications. All user input submitted via web forms is sanitized to prevent it being interpreted as a system command. The dashboard functions via cloud.gov’s API, which has internal checks to prevent input outside the expected syntax and parameters.  **cloud.gov CLI (Command Line Interface)**  Users and administrations also use the Cloud Foundry CLI (maintained by the Cloud Foundry open source project) to access cloud.gov; cloud.gov recommends it to users in the cloud.gov documentation.  The Cloud Foundry CLI requires specific syntax and parameters, or the command will fail to run. It checks to verify that inputs match specified definitions for format and content. All inputs passed to interpreters are pre-screened to prevent the content from being unintentionally interpreted as commands.  **cloud.gov Login**  cloud.gov fallback identity provider: all user input submitted via web forms is sanitized to prevent it being interpreted as a system command. The IDP has internal checks to prevent input outside the expected syntax and parameters.  For customers who do not use the cloud.gov fallback identity provider, cloud.gov’s login is delegated to customer enterprise identity systems, which are responsible for checking the validity of their input.  **Customer Responsibility**  Customers are responsible for checking the validity of inputs in customer applications. |

### SI-11 Error Handling (M) (H)

The information system:

1. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
2. Reveals error messages only to [Assignment: organization-defined personnel or roles].

| SI-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-11(b): Org Manager, Org Auditor, Space Manager, Space Developer, Space Auditor | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | cloud.gov’s user-facing interfaces are the cloud.gov external website, the web UI (dashboard), and the Cloud Foundry CLI.  The external website is a static website that only provides brief non-informative error messages (such as error codes 404 and 500).  The web UI (dashboard) and Cloud Foundry CLI are both powered by the Cloud Foundry API within cloud.gov. The Cloud Foundry API is designed to not reveal error message information to users beyond appropriate user-accessible information. |
| Part b | The Cloud Foundry API shows only appropriate error messages, and it shows them only to logged-in users with assigned roles for that org or space (such as Org Manager, Org Auditor, Space Manager, Space Developer, and Space Auditor). |

### SI-12 Information Output Handling and Retention (L) (M) (H)

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

| SI-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-12 What is the solution and how is it implemented? |
| --- |
| All 18F and GSA staff must comply with the *GSA IT Security Policy*. This policy is the primary document that ensures staff compliance with all applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. Multiple staff from the GSA Office of General Counsel and the GSA Office of the Chief Information Security Officer continuously ensure this policy is up to date.  In regards to information storage, GSA maintains its own records program and has issued a management directive ( <https://www.gsa.gov/portal/mediaId/119434/fileName/OAS_P_18201_Records_Management_Directive_(Signed_3-7-2014)_(Rev_11-19-2015).action> ) to ensure full compliance.  cloud.gov stores all logs that pertain to 18F's AWS actions in CloudTrail, which is also accessible by the GSA Information Security team, who coordinate if necessary with any other GSA stakeholders who help manage information handling and retention compliance: the FOIA team, Records, General Counsel, etc.  cloud.gov does currently create any permanent records. All internal records are classified as temporary. Records are kept in the components listed in this document, or in the appropriate internal GSA systems, or both.  There are no physical input or output devices from cloud.gov's AWS environment, besides the physical layer managed by AWS itself.  **Customer Responsibility**  If applications on cloud.gov have additional information handling and storage requirements, is the customer's responsibility to ensure their application’s data is accessible and exportable to necessary stakeholders. |

### SI-16 Memory Protection (M) (H)

The information system implements [Assignment: organization-defined fail-safe procedures] to protect its memory from unauthorized code execution.

| SI-16 | Control Summary Information |
| --- | --- |
| Responsible Role: Cloud Operations | |
| Parameter SI-16-1: Cloud Foundry components and AWS GovCloud controls | |
| Parameter SI-16-2: n/a | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for AWS GovCloud , 6/21/2016 | |

| SI-16 What is the solution and how is it implemented? |
| --- |
| **cloud.gov**  The stemcell VM image includes a Linux kernel compiled with the NX (no-execute) bit enabled. The kernel leverages the hardware features provided by Intel, exposed through AWS’ EC2 Ring 0 Hypervisor, to enable memory protection for each virtual machine instance. The Linux kernel uses the NX functionality to configure running programs to have memory areas which are physically not executable by the kernel. This prevents attackers from being able to use many classes of unauthorized code execution exploits. For example, an attacker-supplied JMP instruction in that space cannot result in the kernel executing a function in that space, rendering most classes of attack useless.  cloud.gov further separates customer resources using Cloud Foundry’s built-in container security. For details about how cloud.gov isolates container memory using Garden containers, see SC-39 (including the reference to <https://docs.cloudfoundry.org/concepts/container-security.html> ).  **AWS**  cloud.gov is completely virtualized via AWS GovCloud. cloud.gov leverages the Provisional Authorization for AWS GovCloud for this control at the AWS level. |

# Acronyms

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website [Documents](https://www.fedramp.gov/resources/documents-2016/) page under Program Overview Documents.

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.

SYSTEMS SECURITY PLAN ATTACHMENTS

# Attachments

Table ‑. Attachment File Naming Convention

|  |  |  |
| --- | --- | --- |
| Attachment | File Name | File Extension |
| Information Security Policies and Procedures | cloud.gov A1 ISPP v1.3 | .docx |
| Information Security Policies and Procedures - Corporate Policies and Procedures | cloud.gov A1 ISSP Corporate v1.0 | .pdf |
| User Guide | cloud.gov A2 UG v1.1 | .docx |
| E-Authentication Worksheet | Included in Section 15 | n/a |
| PTA | Included in Section 15 | n/a |
| PIA If needed) | None | n/a |
| Rules of Behavior | cloud.gov A5 ROB v1.2 | .docx |
| Information System Contingency Plan | cloud.gov A6 ISCP v1.3 | .docx |
| Configuration Management Plan | cloud.gov A7 CMP v1.1 | .docx |
| Incident Response Plan | cloud.gov A8 IRP v1.2 | .docx |
| CIS Summary Report | cloud.gov A9 CIS Report v1.2 | .docx |
| CIS Worksheet | cloud.gov A9 CIS WS - SSP v1.37 | .xlsx |
| FIPS 199 | Included in Section 15 | n/a |
| Services Table | cloud.gov A11 Services Table - SSP v1.37 | .docx |
| FedRAMP Laws and Regulations | cloud.gov A12 FedRAMP Laws and Regulations | .xlsx |
| Inventory | cloud.gov A13 INV - 3-23-18 | .xlsx |
| Diagram - Customer Data Flow | Diagram - Customer Data Flow - SSP v1.37 | .pdf |
| Diagram - Jumpbox | Diagram - Jumpbox - SSP v1.37 | .pdf |
| Diagram - Network | Diagram - Network - SSP v1.37 | .pdf |
| Diagram - Monitoring | Diagram - Monitoring - SSP v1.37 | .pdf |
| Diagram - Software Deployment | Diagram - Software Deployment - SSP v1.37 | .pdf |

ATTACHMENT 1 - Information Security Policies and Procedures

All Authorization Packages must include an Information Security Policies and Procedures attachment, which will be reviewed for quality.

ATTACHMENT 2 - User Guide

All Authorization Packages must include a User Guide attachment, which will be reviewed for quality.

ATTACHMENT 3 – e-Authentication Worksheet

The E-Authentication section explains the objective for selecting the appropriate e-Authentication level for the candidate system. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63, Revision 1, Electronic Authentication Guideline.

### Introduction and Purpose

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

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

### Information System Name/Title

This E-Authentication Plan provides an overview of the security requirements for the cloud.gov (cloud.gov) in accordance with OMB Memo M-04-04.

Table 15‑2 Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| F1607067912 | cloud.gov | cloud.gov |

### E-Authentication Level Definitions

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

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

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

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

### Review Maximum Potential Impact Levels

18F / GSA has assessed the potential risk from E-Authentication errors, or E-Authentication misuse, related to a user’s asserted identity. 18F / GSA has taken into consideration the potential for harm (impact) and the likelihood of the occurrence of the harm and has identified an impact profile as found in Table 15‑3 Potential Impacts for Assurance Levels.

Assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Table 15‑3 Potential Impacts for Assurance Levels

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

### E-Authentication Level Selection

18F / GSA has identified that they support the E-Authentication Level that has been selected for the cloud.gov as noted in Table 15‑4 E-Authentication Level. The selected E-Authentication Level indicated is supported for federal agency consumers of the cloud service offering. Implementation details of the E-Authentication mechanisms are provided in the System Security Plan under control IA-2

Table 15‑4 E-Authentication Level

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

ATTACHMENT 4 – PTA / PIA

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in ATTACHMENT 12 – FedRAMP Laws and Regulations.

### Privacy Overview and Point of Contact (POC)

The Table 15‑5 - cloud.gov Privacy POC individual is identified as the cloud.gov Privacy Officer and POC for privacy at 18F / GSA.

Table ‑ - cloud.gov Privacy POC

| Name | Britta Gustafson |
| --- | --- |
| Title | Deputy Director of cloud.gov |
| CSP / Organization | 18F / GSA |
| Address | 1800 F Street NW, Washington, DC, 20405 |
| Phone Number | 415-920-3653 |
| Email Address | britta.gustafson@gsa.gov |

#### Applicable Laws and Regulations

The FedRAMP Laws and Regulations may be found on: [www.fedramp.gov](http://www.fedramp.gov) Templates. A summary of FedRAMP Laws and Regulations is included in the System Security Plan (SSP) ATTACHMENT 12 – FedRAMP Laws and Regulations.

Table 12‑1 cloud.gov Laws and Regulations include additional laws and regulations that are specific to cloud.gov. These will include laws and regulations from the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law (PL), United States Code (USC), and Homeland Security Presidential Directives (HSPD).

Table ‑ cloud.gov Laws and Regulations

| Identification Number | Title | Date | Link |
| --- | --- | --- | --- |
| n/a | n/a | n/a | n/a |
| n/a | n/a | n/a | n/a |

#### Applicable Standards and Guidance

The FedRAMP Standards and Guidance may be found on: [www.fedramp.gov](http://www.fedramp.gov) Templates. The FedRAMP Standards and Guidance is included in the System Security Plan (SSP) ATTACHMENT 12 – FedRAMP Laws and Regulations. For more information, see the Program Documents Overview section of the FedRAMP website.

Table 12‑2 cloud.gov Standards and Guidance includes any additional standards and guidance that are specific to cloud.gov. These will include standards and guidance from Federal Information Processing Standard (FIPS) and National Institute of Standards and Technology (NIST) Special Publications (SP).

Table ‑ cloud.gov Standards and Guidance

| Identification Number | Title | Date | Link |
| --- | --- | --- | --- |
| n/a | n/a | n/a | n/a |
| n/a | n/a | n/a | n/a |

#### Personally Identifiable Information (PII)

Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

* Social Security numbers
* Passport numbers
* Driver’s license numbers
* Biometric information
* DNA information
* Bank account numbers

PII does not refer to business information or government information that cannot be traced back to an individual person.

### Privacy Threshold Analysis

18F / GSA performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the cloud.gov (cloud.gov) components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by 18F / GSA can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

#### Qualifying Questions

|  |  |
| --- | --- |
| No | 1. Does the ISA collect, maintain, or share PII in any identifiable form? |
| No | 1. Does the ISA collect, maintain, or share PII information from or about the public? |
| No | 1. Has a Privacy Impact Assessment ever been performed for the ISA? |
| No | 1. Is there a Privacy Act System of Records Notice (SORN) for this ISA system?  If yes; the SORN identifier and name is: Enter SORN ID/Name. |

If answers to Questions 1-4 are all “No” then a Privacy Impact Assessment may be omitted. If any of the answers to Question 1-4 are “Yes” then complete a Privacy Impact Assessment.

#### Designation

Check one.

|  |  |
| --- | --- |
|  | A Privacy Sensitive System |
|  | Not a Privacy Sensitive System (in its current version) |

The Privacy Impact Assessment Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

ATTACHMENT 5 - Rules of Behavior

All Authorization Packages must include a Rules of Behavior (RoB) attachment, which will be reviewed for quality.

The RoB describes controls associated with user responsibilities and certain expectations of behavior for following security policies, standards and procedures. Security control PL-4 requires a CSP to implement rules of behavior.

The Rules of Behavior Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

The Template provides two example sets of rules of behavior: one for Internal Users and one for External Users. The CSP should modify each of these two sets to define the rules of behavior necessary to secure their system.

ATTACHMENT 6 – Information System Contingency Plan

All Authorization Packages must include an Information System Contingency Plan attachment, which will be reviewed for quality.

The Information System Contingency Plan Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

The Information System Contingency Plan Template is provided for CSPs, 3PAOs, government contractors working on FedRAMP projects, government employees working on FedRAMP projects and any outside organizations that want to make use of the FedRAMP Contingency Planning process.

ATTACHMENT 7 - Configuration Management Plan

All Authorization Packages must include a Configuration Management Plan attachment, which will be reviewed for quality.

ATTACHMENT 8 - Incident Response Plan

All Authorization Packages must include an Incident Response Plan attachment, which will be reviewed for quality.

ATTACHMENT 9 - CIS Report and Worksheet

All Authorization Packages must include Control Implementation Summary (CIS) Report and Worksheet attachments, which will be reviewed for quality.

Templates for both can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

The Report Template has a sample format. The CSP may modify the format as necessary to comply with its internal policies and FedRAMP requirements.

ATTACHMENT 10 - FIPS 199

All Authorization Packages must include a Federal Information Processing Standard (FIPS) 199 Section, which will be reviewed for quality.

The FIPS-199 Categorization report includes the determination of the security impact level for the cloud environment that may host any or all of the service models: IaaS, PaaS and SaaS. The ultimate goal of the security categorization is for the CSP to be able to select and implement the FedRAMP security controls applicable to its environment.

### Introduction and Purpose

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

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

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

### Scope

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

### System Description

The cloud.gov system has been determined to have a security categorization of Moderate (M). See *Section 9 General System Description*.

### Methodology

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

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

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

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

| Information Type | NIST SP 800-60 V2 R1  Recommended Confidentiality Impact Level | NIST SP 800-60 V2 R1  Recommended Integrity Impact Level | NIST SP 800-60 V2 R1  Recommended Availability Impact Level | CSP Selected Confidentiality Impact Level | CSP Selected Integrity Impact Level | CSP Selected Availability Impact Level | Statement  for Impact Adjustment Justification |
| --- | --- | --- | --- | --- | --- | --- | --- |
| (C.3.5.1) | Low | Moderate | Low | Moderate | Moderate | Moderate | cloud.gov may host customer systems with Low or Moderate impact levels for data types. |
| (C.3.5.2) | Low | Moderate | Low | Moderate | Moderate | Moderate | cloud.gov may host customer systems with Low or Moderate impact levels for data types. |
| (C.3.5.3) | Low | Moderate | Low | Moderate | Moderate | Moderate | cloud.gov may host customer systems with Low or Moderate impact levels for data types. |
| (C.3.5.4.) | Low | Low | Low | Moderate | Moderate | Moderate | cloud.gov may host customer systems with Low or Moderate impact levels for data types. |

ATTACHMENT 11 – Services Table

See the attached table for a list of internal and external services used in this system.

ATTACHMENT 12 – FedRAMP Laws and Regulations

The Table 15‑8 FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance lists all of the FedRAMP templates in which FedRAMP laws, regulations, standards and guidance are referenced.

Table ‑ FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance

| Phase | | Document Title | |
| --- | --- | --- | --- |
| Document Phase | | SSP | System Security Plan |
|  | SSP Attachment 4 | PTA/PIA | Privacy Threshold Analysis and Privacy Impact Assessment |
|  | SSP Attachment 6 | ISCP | Information System Contingency Plan |
|  | SSP Attachment 10 | FIPS 199 | FIPS 199 Categorization |
| Assess Phase | | SAP | Security Assessment Plan |
| Authorize Phase | | SAR | Security Assessment Report |

The FedRAMP Laws and Regulations can be submitted as an appendix or an attachment. The attachment can be found on this page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

Note: All NIST Computer Security Publications can be found at the following  
URL: <http://csrc.nist.gov/publications/PubsSPs.html>

ATTACHMENT 13 – FedRAMP Inventory Workbook

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan

- Security Assessment Plan

- Security Assessment Report

- Information System Contingency Plan

- Initial POAM

- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

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