AUDIT AND ACCOUNTABILITY (AU)

AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES (AU-1)

The organization:

(a) 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

(b) Reviews and updates the current:

(1) Audit and accountability policy [*FedRAMP Assignment: at least every three years*]; and

(2) Audit and accountability procedures [*FedRAMP Assignment: at least annually*].

AU-1	Control Summary Information
Responsible Role: Information Systems Security Manager, Information Systems Security Officer, System Owner	
Parameter AU-1(a): Information Systems Security Manager, Information Systems Security Officer, System Owner	
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	**Agency Auditing and Accountability Policy and Procedures** Audit and Accountability Policy is included in *CIO P 2100.1 - GSA IT Security Policy, Chapter 5. Policy on Technical Controls*. It states, "Security-activity auditing capabilities must be employed on all GSA information systems."

AU-1 What is the solution and how is it implemented?	
	GSA OCISO ISP also defined agency-wide audit and accountability procedures in *IT Security Procedural Guide: Audit and Accountability (CIO-IT Security-01-08).* GSA policies are available on GSA InSite to GSA staff and also available upon request to other agencies and auditors. **18F Program Auditing and Accountability Policy** The 18F Program Office develops, documents, and disseminates to all 18F staff the 18F Audit and Accountability Policy, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and procedures to facilitate the implementation of the audit and accountability policy and associated audit controls. The 18F Audit and Accountability policy is listed within 18F's public GitHub repository: https://github.com/18F/compliance-docs/blob/master/AU-Policy.md (which is accessible to all 18F staff).
Part b	**Agency AU Policy** The GSA Office of the CISO is responsible for reviewing and updating the above documents annually, and notifying System Program Managers and Information Systems Security Officers and Managers (ISSO/Ms). **18F Program Policy** The 18F Program Office will review and update the current 18F Audit and Accountability Policy at least every 3 years and any documented audit procedures at least annually.

AUDIT EVENTS (AU-2)

The organization:

(a) 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*];

(b) 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;

(c) Provides a rationale for why the auditable events are deemed to be adequate to

support after-the-fact investigations of security incidents; and

(d) 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	Control Summary Information
Responsible Role: Program Manager, System Owner, Cloud Operations, Information Systems Security Officer	
Parameter AU-2(a): audited continually for each identified event	
Parameter AU-2(d): Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☒ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☒ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)	

AU-2 What is the solution and how is it implemented?	
Part a	AWS Auditable Events: 18F has implemented CloudTrail and CloudWatch 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. CloudTrail captures and records important information about each API call for the list of auditable events: - User – the IAM user name of the person who was interacting with the AWS account. - IP Address – the IP Address where the interactions originated from. - Event Name – the type of interaction that occurred. - Service – the AWS Service that was interacted with. - Time – the date and time that the event occurred. - Region – the AWS Region(s) where the interactions occurred. - Resource ID – the resource ID from the event.

AU-2 What is the solution and how is it implemented?	

	cloud.gov Auditable Events
	- cloud.gov provides an audit trail through the BOSH tasks command. This command shows all actions that an operator has taken with the platform. Additionally, operators can redirect 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.
	- 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:
	  o Tail their application logs.
	  o Dump a recent set of application logs (where recent is a configurable number of log packets).
	  o 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.
	
	Customer Responsibility:
	All applications will partially inherit some of the ELK stack auditing functions and capabilities that reside on the cloud.gov PaaS. Application System Owners must ensure their application's activities are monitored and captured within audit logs.

Part b	Audit logs will be made available to client organizations and for mutual support in response to security breaches, system and user access, incident reporting and continuous monitoring. 18F will generate and distribute audit reports, provide dashboard access for audited events, and send audit log data to SIEM and log analysis systems as needed.
Part c	18F Audit Retention The 18F PMO has established processes for regularly reviewing audit log information, and reporting security issues if discovered. Reviews will occur at a minimum of weekly and are integrated with processes for incident response, in order to ensure standardization and cross-functional collaboration. cloud.gov PaaS uses the following automated mechanisms CloudTrail, CloudWatch, and ELK Stack to integrate audit monitoring, analysis and reporting into an overall

AU-2 What is the solution and how is it implemented?	
	process for investigation and response to suspicious activities. In addition, the 18F PMO employs automated mechanisms such as PagerDuty, StatusPage.io and Slack to immediately alert security personnel of inappropriate or unusual activities that have security implications.
Part d	AWS Auditable Events: - When 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: - User – the IAM user name of the person who was interacting with the AWS account. - IP Address – the IP Address where the interactions originated from. - Event Name – the type of interaction that occurred. - Service – the AWS Service that was interacted with. - Time – the date and time that the event occurred. - Region – the AWS Region(s) where the interactions occurred. - Resource ID – the resource ID from the event. cloud.gov Auditable Events: - 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 18F applications and system components that interact with a hosted app during updates and execution. - The BOSH CLI which is used to capture audit events from several log types within the cloud.gov platform itself. These logs consist of VM logs (Job logs, Errand logs, Monit logs, Agent logs, Log rotation and Syslog configuration) and Director task logs. **Customer Responsibility:** Application System owners are responsible for making sure audit events are captured based on AU-2d parameter requirements for their web applications.

CONTROL ENHANCEMENT AU-2 (3)

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.

AU-2 (3)	Control Enhancement Summary Information
Responsible Role: Cloud Operations, Information Systems Security Officer	
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 Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)	

AU-2 (3) What is the solution and how is it implemented?
The Information Systems Security Officer, supported by Cloud Operations, will review all auditable events on a near real-time basis using its event and monitoring solution, which includes CloudTrail, CloudWatch, BOSH and the ELK stack for cloud.gov and through captured user and event API calls within its AWS virtual infrastructure. Cloud Operations will update the defined auditable events at least annually or when changes in the threat environment occur or are identified by risk assessment. All updates and changes in the threat environment will be included in updates provided to the JAB.

CONTENT OF AUDIT RECORDS (AU-3)

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, Information Systems Security Manager	
Implementation Status (check all that apply): ☒ Implemented	

AU-3	Control Summary Information

☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☐ Service Provider System Specific
☒ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☐ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)

AU-3 What is the solution and how is it implemented?

18F collects, monitors, and maintains audit logs through the use of CloudTrail, CloudWatch, ELK Stack and BOSH. CloudTrail and CloudWatch

The events monitored include but are not limited to successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events for the virtual private network and the cloud.gov Platform as a Service. These events are tracked for all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.
The following platform specific monitoring includes:

Audit contents from AWS Cloud Trail

CloudTrail Log File Name Format CloudTrail uses the following
file name format for the log file objects it uploads to your S3 bucket:
AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.FileNameFormat YYYY, MM, DD, HH, and mm are the digits of the year, month, day, hour, and minute (respectively) when the log file was delivered. Hours are in 24-hour format. The Z indicates that the time is in UTC.

Audit contents from cloud.gov from the BOSH CLI:

State, Timestamp, User, Deployment , Description, Result

CONTROL ENHANCEMENT AU-3 (1)

The information system generates audit records containing the following additional information: [*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*]].

AU-3 (1) Additional FedRAMP Requirements and Guidance: Requirement: The service provider defines audit record types. 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 Enhancement Summary Information
Responsible Role: Cloud Operations, System Owner, Information Systems Security Officer	
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 Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)	

AU-3 (1) What is the solution and how is it implemented?
The cloud.gov information system generates audit records containing the following additional information: 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. CloudTrail can generate a subset of audit records containing additional information within the Virtual infrastructure. EC2:

AU-3 (1) What is the solution and how is it implemented?
• Security Groups • Security Group Rules • Key Pairs • AMIs • Spot Instances • Reserved Instance • Instances • Volumes • Snapshots • Placement Groups • Elastic Load Balancers (including attaching or detaching instances to them) • Network Interfaces • Elastic IPs IAM: • Account Aliases • Account Summaries • Access Keys • MFA Devices • Policies • Password Policies • Groups • Users S3: • Bucket Logging • Logging Target Bucket • Bucket Logging Prefix • Bucket Website Enabled • Bucket Website Index Document • Bucket Website Error Document • Bucket Notifications Enabled • Public Buckets • Bucket Notifications • Bucket Lifecycle Rules • Bucket Permissions cloud.gov can generate additional audit information such as $remote_addr - $remote_user [$time_local] ' '"$request" $status $bytes_sent ' '"$http_referer" "$http_user_agent" "$gzip_ratio"';

AUDIT STORAGE CAPACITY (AU-4)

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 Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)	

AU-4 What is the solution and how is it implemented?
For the cloud infrastructure and cloud.gov platform, 18F define the amount of storage dedicated to audit logs records on their EC2 instances and S3 buckets. cloud.gov uses elastic file storage 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. Cloud System Administrators are responsible for maintaining the configuration that enforces the audit settings. The log management framework will provide the capability to retain logs for 180 days online and one-year offline, with sufficient capacity as to mitigate the risk of exceeding storage space. In the event the threshold is acceded, administrators can add additional storage capacity without impacting the system.

RESPONSE TO AUDIT PROCESSING FAILURES (AU-5)

The information system:

(a) Alerts [*Assignment: organization-defined personnel or roles*] in the event of an audit processing failure; and

(b) Takes the following additional actions: [*FedRAMP Assignment: low-impact: overwrite oldest audit records; moderate-impact: shut down*].

AU-5	Control Summary Information
Responsible Role: Cloud Operations	
Parameter AU-5(a): Alerts Cloud Operations, Information Systems Security Officer, Program Manager	
Parameter AU-5(b) Alert will 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 Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)	

AU-5 What is the solution and how is it implemented?	
Part a	Planned control. 18F has the ability to elastically grow the audit storage capacity, which reduces the likelihood of such capacity being exceeded within the information system; however 18F will ensure to implement an alert system using AWS CloudTrail and ELK stack to alert cloud operators to any processing failures related to audit storage capacity.
Part b	Planned control. In the unlikelihood the audit storage capacity has been reached, 18F will stop the cloud.gov loggreator from streaming logs to any third party SIEM tools and send out an alert though automated mechanisms such as PagerDuty, StatusPage.io and Slack to immediately alert processing failures.

AUDIT REVIEW, ANALYSIS, AND REPORTING (AU-6)

The organization:

(a) Reviews and analyzes information system audit records [*FedRAMP Assignment: at least weekly*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*]; and

(b) Reports findings to [*Assignment: organization-defined personnel or roles*].

AU-6	Control Summary Information
Responsible Role: Cloud Operations, Information Systems Security Officer	
Parameter AU-6(a)-1: At least weekly	
Parameter AU-6(a)-2: inappropriate or unusual activity	
Parameter AU-6(b): Reports findings to System owner, Information systems security 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)	

AU-6	Control Summary Information
☐ Inherited from pre-existing Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)	

AU-6 What is the solution and how is it implemented?	
Part a	Planned Control: Through the use of CloudTrail, BOSH and the ELK logging system, the 18F security team monitors and reviews audit logs for unapproved and unusual activities on a continual basis. Reporting rules have been developed to look for, identify, and report potentially inappropriate or unusual activity to be reviewed regularly within the audit tools dashboard as well as regular reports that are automatically generated on a weekly basis and sent to the 18F PMO, GSA's Security team and other partner agencies as required.
Part b	When a credible source to the GSA Agency provides information that causes reason to enhance audit activities, 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*. The GSA Agency may also, through analysis pertaining to the GSA Agency environment provides additional audit measures that will require an increase in review, analysis, and reporting for a necessary. 18F 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 18F, the review of audit logs shall be increased and any appropriate changes to audit content collection shall be implemented.

CONTROL ENHANCEMENT AU-6 (1)

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 Enhancement Summary Information
Responsible Role: Cloud Operations	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned	

AU-6 (1)	Control Enhancement Summary Information

☐ Alternative implementation
☐ Configured by customer
☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☐ Service Provider System Specific
☒ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☐ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)

AU-6 (1) What is the solution and how is it implemented?
Planned Control: cloud.gov PaaS uses the following automated mechanisms CloudTrail, CloudWatch, and ELK Stack to integrate audit monitoring, analysis and reporting into an overall process for investigation and response to suspicious activities. In addition, the 18F PMO will employ automated mechanisms such as CloudWatch logs that collect and tracks 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 18F AWS account to a CloudWatch Logs log group. CloudTrail events that are sent to CloudWatch Logs will trigger alarms according to the metric filters defined. 18F will configure CloudWatch alarms to send notifications to PagerDuty, StatusPage.IO and Slack or make changes to the resources that are monitored based on log stream events that the metric filters extract.

CONTROL ENHANCEMENT AU-6 (3)

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

AU-6 (3)	Control Enhancement Summary Information

Responsible Role: Cloud Operations, Information Systems Security Officer

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate

AU-6 (3)	Control Enhancement Summary Information

☐ Service Provider System Specific
☒ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)

AU-6 (3) What is the solution and how is it implemented?
Planned control. 18F analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. This information helps System Owners, Security Operations and Cloud Operations track changes made to its cloud infrastructure and cloud.gov platform resources and to troubleshoot operational issues. All ELK Stack logging and monitoring data from the cloud.gov platform will be sent to CloudWatch and CloudTrail for additional correlation and analysis.

AUDIT REDUCTION AND REPORT GENERATION (AU-7)

The information system provides an audit reduction and report generation capability that:

(a) Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
(b) 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)
☐ Corporate (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)

AU-7 What is the solution and how is it implemented?	
Part a	CloudTrail produces data that can be used to detect abnormal behavior, retrieve event activities associated with specific objects, or provide a simple audit trail for the cloud infrastructure. 18F can evolve current logging analytics by using the 25+ different fields in the event data that AWS CloudTrail provides to build queries and create customized reports focused on internal investigations, external compliance, etc. CloudTrail enables 18F to monitor API calls for specific known undesired behavior(s) and raise alarms using log management or security incident and event management (SIEM) tools. The BOSH CLI which is used to capture audit events from several log types within the cloud.gov platform itself. These logs consist of VM logs (Job logs, Errand logs, Monit logs, Agent logs, Log rotation and Syslog configuration) and Director task logs. Through the BOSH CLI, custom filtering using command line arguments and option flags support audit reduction and generation functions. The ELK Stack which captures logs related to application hosted on top of the cloud.gov platform has the capability to provide audit reduction and report generation capability through the Kibana Dashboard. Kibana has the capacity to build search queries on numerous criteria regarding application logs.
Part b	All Audit reports generated by CloudTrail, BOSH and the ELK Stack does not alter the original content or time ordering of audit records. All Audit files can be viewed in their raw and JSON standard formats. AWS CloudTrail produces log data from a single internal system clock by generating event time stamps in Coordinated Universal Time (UTC), consistent with the ISO 8601 Basic Time and date format standard.

CONTROL ENHANCEMENT AU-7 (1)

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 Enhancement Summary Information
Responsible Role: Cloud Operations	
Parameter AU-7(1):	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

AU-7 (1)	Control Enhancement Summary Information

☐ Not applicable

Control Origination (check all that apply):
☐ Service Provider Corporate
☐ Service Provider System Specific
☒ Service Provider Hybrid (Corporate and System Specific)
☐ Configured by Customer (Customer System Specific)
☐ Provided by Customer (Customer System Specific)
☒ Shared (Service Provider and Customer Responsibility)
☐ Inherited from pre-existing Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)

AU-7 (1) What is the solution and how is it implemented?

18F uses CloudTrail to monitor AWS deployments in the cloud by getting a history of AWS API calls of the 18F account, including API calls made via the AWS Management Console, the command line tools, and higher-level AWS services. 18F 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.

cloud.gov BOSH audit logs which compose of VM Logs and Director logs show the following audit fields which displays 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 following event details captured include: cloud config update, runtime config update, deployment create/update/delete, VM create/delete, disk create/delete and BOSH SSH events.

TIME STAMPS (AU-8)

The information system:

(a) Uses internal system clocks to generate time stamps for audit records; and
(b) Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [*Assignment: organization-defined granularity of time measurement*].

AU-8	Control Summary Information

Responsible Role: Cloud Operations

Parameter AU-8(b): Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time

Implementation Status (check all that apply):
☒ Implemented
☐ Partially implemented

AU-8	Control Summary Information
☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☒ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)	

AU-8 What is the solution and how is it implemented?	
Part a	The cloud.gov information system pulls from multiple NTP sources including http://tf.nist.gov/tf-cgi/servers.cgi for all the cloud.gov servers to generate time stamps for audit records. All the cloud.gov NTP servers are synchronized with Amazon's NTP canonical server. Systems poll the NTP servers at least hourly to synchronize.
Part b	The cloud.gov information records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

CONTROL ENHANCEMENT AU-8 (1)

The information system:

(a) Compares the internal information system clocks [*FedRAMP Assignment: at least hourly*] with [*FedRAMP Assignment: authoritative time source: http://tf.nist.gov/tf-cgi/servers.cgi*]; and

(b) 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)	Control Enhancement Summary Information
Responsible Role: Cloud Operations	
Parameter AU-8(1)(a)-1: At least hourly	
Parameter AU-8(1) (a)-2: authoritative time source with Amazon's NTP canonical server.	

AU-8 (1)	Control Enhancement Summary Information
Parameter AU-8(1) (b): Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than 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 Provisional Authorization (PA) for AWS GovCloud (June 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 Amazon's NTP canonical server.
Part b	All the cloud.gov NTP servers are synchronized with Amazon's NTP canonical server.

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)	Additional Control Enhancement 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 Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)	

AU-8 (1) What is the solution and how is it implemented?	
Req. 1	The cloud.gov information system pulls from multiple NTP sources including http://tf.nist.gov/tf-cgi/servers.cgi for all the cloud.gov servers to generate time stamps for audit records.
Req. 2	The cloud.gov NTP servers are synchronized with Amazon's NTP canonical server. Systems poll the NTP servers at least hourly to synchronize.

PROTECTION OF AUDIT INFORMATION (AU-9)

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	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	

AU-9	Control Summary Information
Responsible Role: Cloud Operations, Information Systems Security Officer	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☒ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)	

AU-9 What is the solution and how is it implemented?
Planned Control: To maintain the integrity of log data, 18F carefully manages access around the generation and storage of audit log files. The ability to view or modify log data is restricted to 18F security and Cloud Operations authorized users. Audit logs from CloudTrail are stored and protected in specified S3 buckets for cloud.gov which is limited to read only access and multifactor authentication by security staff. This ensures the logs cannot be modified without proper authorization. Audit logs from the cloud.gov Platform are only accessible to the 18F Cloud Operations personnel and can only be viewed by using the BOSH CLI. ELK Stack logs and monitoring data from the applications stored on top of cloud.gov are stored and protected in the Logstash database within the cloud.gov EC2 instances.

CONTROL ENHANCEMENT AU-9 (2)

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 Enhancement 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	

AU-9 (2)	Control Enhancement Summary Information
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☒ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)	

AU-9 (2) What is the solution and how is it implemented?
Planned Control: 18F plans to implement a backup strategy to send all cloud.gov audit logs to encrypted S3 buckets where data is redundantly stored across multiple facilities and multiple devices in each facility. All S3 buckets will only be accessible to authorized 18F staff using role-based-access-controls (RBAC) and CloudTrail auditing implemented for logging and monitoring purposes. 18F will set up weekly backups of all cloud.gov audit logs to the S3 buckets being audited.

CONTROL ENHANCEMENT AU-9 (4)

The organization authorizes access to management of audit functionality to only [*Assignment: organization-defined subset of privileged users*].

AU-9 (4)	Control Enhancement Summary Information
Responsible Role: Cloud Operations, Information Systems Security Officer	
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)	

AU-9 (4)	Control Enhancement Summary Information
☐ Inherited from pre-existing Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)	

AU-9 (4) What is the solution and how is it implemented?
The 18F organization authorizes access to management of audit functionality to only designated 18F cloud operators. 18F will use IAM polices to restrict access to EC2 instance 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 auditing and monitoring tools use RBAC functionality to ensure management of auditing tools is secured.

AUDIT RECORD RETENTION (AU-11)

The organization retains audit records for [*FedRAMP Assignment: at least ninety 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	
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 Provisional Authorization (PA) for AWS GovCloud (June 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. The log management framework will provide the capability to retain logs for 180 days online and one-year offline, with sufficient capacity as to mitigate the risk of exceeding storage space. This information helps System Owners, Security Operations and Cloud Operations track changes made to its resources and to troubleshoot operational issues.

AUDIT GENERATION (AU-12)

The information system:

(a) 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*];

(b) Allows [*Assignment: organization-defined personnel or roles*] to select which auditable events are to be audited by specific components of the information system; and

(c) 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	
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 Provisional Authorization (PA) for AWS GovCloud (June 21, 2016)	

AU-12 What is the solution and how is it implemented?	
Part a	The cloud.gov information system provides the audit record generation capability for the auditable events defined in AU-2 a. All application logs generated using the cloud.gov platform can be accessed from the logs.cloud.gov component. The list of auditable events defined in AU-2 are: 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. Cloud Operations are responsible for maintaining the configuration that enforces the audit settings.
Part b	cloud.gov Operators select which auditable events are to be audited by specific components of the cloud.gov information system where audit capability is deployed.
Part c	The 18F 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 AWD virtual infrastructure operating systems where audit capability is deployed. The content as defined in AU-3 is sufficient information to, at a minimum, establish: - what type of event occurred, - when (date and time) the event occurred, - where the event occurred, - the source of the event, - the outcome (success or failure) of the event, and - The identity of any user/subject associated with the event. Cloud operators are responsible for maintaining the configuration that enforces the audit settings.