Discovery LATO System Security Plan - Control Documentation

This SSP Control documentation was created using Compliance Masonry and the documentation source is stored on Discovery's Source Repository

GSA Professional Services and Human Capital Division - Discovery Application System

Standards

Components

- System and Services Acquisition Policies for Discovery
- Identification and Authentication Policies for Discovery
- Audit and Accountability Policies for Discovery
- Access Control Policies for Discovery
- Risk Assessment Policies for Discovery
- Security Planning Policies for Discovery
- System and Communications Protection Policies for Discovery
- Configuration Management Policies for Discovery
- System and Information Integrity Policies for Discovery
- Security Assessment Policies for Discovery

About the Discovery System Security Plan - Control Documentation

This Discovery System Security Plan Control documentation is a complement to the primary System Security Plan documentation and outlines narratives and compliance with required controls for a GSA Lightweight ATO process.

Who should use this document?

This document is intended to be used by GSA affiliated security professionals to review current system compliance state and plans.

Discovery Security Classification

Sensitivity Categorization of Information Types

Information Type	Confidentiality	Integrity	Availability
Administrative users	Low	Low	Low
Federal Professional Services vendors	Low	Low	Low
Vendor pools (with vendor PIIDs)	Low	Low	Low
Setaside classifications	Low	Low	Low
NAICS classifications	Low	Low	Low
Vendor contract information	Low	Low	Low
FPDS and SAM load information (timestamps)	Low	Low	Low

Security Objectives Categorization (FIPS 199)

Security Objective	Low, Moderate or High
Confidentiality	Low
Integrity	Low
Availability	Low

Information System Categorization

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

Low	Moderate	High
X		

General System Description

System Purpose and Function

The GSA Discovery application is a tool that helps contracting professionals and other interested parties conduct market research on GSA contract vehicles and their suppliers. Users can search for available vendors by contract and NAICS code. The results can be further filtered down by vendor set-aside classifications. While the current version of Discovery is somewhat limited in vendor scope and available data, this system is expected to evolve to encompass a wide range of contracting vehicles and vendor related information.

The goal of Discovery is to provide acquisition professionals the means to research various contract vehicles while research historical information and vendor availability related to their particular acquisition need in order to reduce contract duplication by encouraging the use of existing vehicles through transparency.

Discovery Data

Currently there are two primary acquisition vehicles encompassed within the Discovery ecosystem; OASIS Small Business, and OASIS Unrestricted. There are more vehicles planned in the near future which will add more vendors serving more NAICS codes. There are currently a total of six vendor pools from the two vehicles currently offered. Over time the vendor pools will grow with the addition of new vehicles.

Vendor information is loaded from a combination of information gathered from PSHC staff collected into spreadsheets and SAM registration information pulled from the SAM API. The pool information that is collected by GSA PSHC staff is loaded from source files in the code base and do not change often. The SAM is continuously checked for updated information.

Discovery collects basic information on contract awards and modifications by vendors in the aforementioned vendor pools. This information includes the NAICS classification, transaction amount, and other information such as employee count and company revenue at that point in time if available. In the future the actual data collected from contracts might change or grow. The contract information is currently pulled from the GSA FPDS API and is continuously updated to ensure that fresh contract information can be factored into market research being performed. Currently, Discovery displays 10 years worth of historical data by vendor and NAIC.

Discovery Functions

Discovery is a simple application by design. You can use the system in one of two ways; collect information from the vendor and contract focused API, or browse the website to see quick displays of information related to contracts being processed by included vendors. The frontend user centered display is generated from data pulled from the backend API.

The Discovery API is a simple data pull system that allows users to request information on vendors, contracts, and NAICS codes. In the future as more data is added the breadth and depth of these APIs will likely grow to serve the new data.

The Discovery frontend is a Javascript centric rendering and filtering interface designed to allow the user to filter down a set of vendors serving a particular NAICS code, possibly using set-aside filters. The vendor information returned includes links to a vendor page, as well as information about the contracts that the vendor has executed within the supported vehicles for that NAICS code. There are plans to re-envision the interface to provide more comprehensive and flexible displays, as well as advanced search and filtering.

To keep all of the vendor and contract data current automated scheduling of tasks is performed through background “worker” processes. The Discovery website provides a means for configuring the timing and optional parameters for these regular content updates. To update the schedule of the periodic updates from FPDS and SAM APIs administrative users need to login and will have access to a simple administrative information for creating schedules for tasks and viewing task execution results.

Discovery Links

Production Link: https://discovery.gsa.gov (https://discovery.app.cloud.gov) *Staging Link*: https://discovery-dev.app.cloud.gov *Git Repository*: https://github.com.com/PSHCDevOps/discovery

Discovery Components and Boundaries

The GSA Discovery application is a Python Django application that relies on open source technologies and ATO'd hosting technologies to provide a public repository of searchable acquisition related information.

Application components

Discovery consists of a group of interrelated Python Django applications that rely on external services for data storage, tasks queuing, session storage, and data ingestion. All of these systems with the exception of external data API sources are housed internally within the Cloud.gov environment.

The Python Django application relies upon a connection to a PostgreSQL database that contains all of the primary application related data. All data loaded from external sources gets stored and retrieved from this database. Currently we use the aws-rds Cloud.gov service to provide this database. This database contains tables pertaining to administrative users and related information, system state information, cache tables, vendor information, and contract data.

In order to continuously update the data in the Discovery system, a scheduler and workers are constantly running (in a service like Cron). This service relies upon both the PostgreSQL database used by the primary Django application, and a Redis queue for collecting background tasks for processing that are deposited in the queue by the scheduler.

To scale the Discovery application to multiple web servers with the possibility of administrative login we need to maintain our user session information in an external data store. For this, we use another Redis instance that contains all of our session data that is shared across all available web servers.

The Django Discovery application has three primary architectural components; API, frontend Javascript site, and data loaders. The data loaders are commands embedded in the application that retrieve all of the data displayed in the Discovery application. The API builds on the loaded data to provide endpoints for accessing the information. Finally the Javascript application renders acquisition related data from the API's into a user friendly format, and allows for filtered queries.

Application hosting

The networking boundaries for the Discovery system are contained fully within the ATO'd Cloud.gov architecture with the exception of external public data sources covered in the next section. The Cloud.gov architecture consists of a group of applications, services, and routes that contribute to a fully functioning system. There is no physical hardware required for the continued operations of the Discovery application.

There are two persistent spaces within the Cloud.gov Discovery organization that contain both a development staging environment and a live production environment. Each of these spaces is configured exactly the same with the exception of the number of servers of a given type currently operating, and a CDN service tied to the production Discovery domain that maps to a web application cluster. There may be other temporary application spaces created and destroyed as necessary to test various features and bug fixes in the hosting environment.

Cloud.gov services

Each Cloud.gov space contains five separate services needed to power the Discovery application. All configurations and naming conventions are the same across all spaces.

Service account *(with deployment key)* - A service that provides a temporary account, username, and password that allows our CI/CD system (CircleCI) to deploy the application to the space. By default development and production spaces have them to facilitate GitHub merge based deployments, but other temporary spaces may be configured with them as needed for testing purposes.

PostgreSQL AWS-RDS *(single database)* - The primary data store for the Discovery application. For a more detailed overview, see the Application components section above.

Redis 3.2 *(single database)* - A session store for multi web server authentication of the Django web application. For a more detailed overview, see the Application components section above.

Redis 3.2 *(single database)* - A queue for storing background tasks to be completed. For a more detailed overview, see the Application components section above.

Application configuration variables - A user provided service that stores the values of four environment variables; API_HOST, API_KEY, SAM_API_KEY, and SECRET_KEY. These environment variables are shared (or bound) to all web, scheduler, and worker servers in the space.

CDN service *(production space only)* - A custom domain, AWS Cloud Front CDN, and HTTPS certificate configuration for the production site at https://discovery.gsa.gov

Cloud.gov applications

The Discovery web application cluster are Cloud.gov servers built on the commonly used Cloud Foundry Python buildpack. All of our deployed applications use the Django web framework, so build the same dependencies from top level requirements files.

Discovery Web - The frontend Discovery website and API layer. In each of the development and production spaces we maintain a cluster of at least two application servers running behind the Cloud.gov load balancer.

Discovery Scheduler - A Django Celery Beat based scheduling service that continuously runs in the background sending background tasks for Worker servers periodically, as configured through the Django administrative interface. Only a single Scheduler server should be running in the Cloud.gov space.

Discovery Worker - A Django Celery background task processing service that continuously runs processing tasks created from the Scheduler or the application code. Currently only the Scheduler creates background tasks for Worker servers but this may change in the future. Depending on the space and volume of tasks, multiple Worker servers may be running in the Cloud.gov space.

Cloud.gov routes

Every space contains one preconfigured route from the application manifests that points to the Cloud.gov load balancer that routes traffix to the Discovery web servers. This route hostname is different on all spaces.

Data sources

Vendor pool CSVs

The Discovery application loads vendor information from various CSV files committed into the application source code. This data is updated as information changes with software releases.

SAM vendor registrations

The Discovery application reaches out and pulls publicly available vendor registration information from the SAM API. This API requires a Data.gov API KEY but otherwise has no security restrictions.

FPDS contract awards and modifications

The Discovery application reaches out and pulls publicly available vendor contract awards and modifications from the FPDS API (ATOM feed). This API does not require any type of API key and has no real security restrictions.

NIST-800-53-AC

NIST-800-53-AC-2

Account Management

Access Control Policies for Discovery

AC-2a

Control: **The organization identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, group, system, application, guest/anonymous, and temporary accounts**

The Discovery application has defined several granular roles, both at the infrasructure and application level, that allow for fine grained permissions. On the infrastructure side these include Cloud.gov organization manager, auditor, and billing manager, Cloud.gov space managers, developers, and auditors, GitHub maintainers and external contributors, and CircleCI service managers. For the application most traffic is served up to public anonymous traffic, but we do have Django site administrators capable of modifying users, content, and managing periodic tasks.

Each role is inhabited by only those people who need that ability. Role membership can often overlap due to the smaller number of internal staff and contractors working on the system at any given time.

AC-2b

Control: **The organization assigns account managers for information system accounts**

The PSHC Discovery management team assigns staff and contractors access to roles discussed in AC-2a only as needed and access is limited to the roles needed to accomplish their missions. The PSHC may delegate management of certain responsibilities to other staff members or contractors working on the platform if the system can benefit from their management. All managers are either GSA staff or current contractors.

AC-2c

Control: **The organization establishes conditions for group and role membership**

All Discovery related roles defined in AC-2a have clearly defined permissions and duties and they do not overlap. A GSA staff member or current contractor may be granted access to a role if they need the permissions or abilities to perform their management approved duties.

AC-2e

Control: **The organization requires approvals by GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO for requests to create information system accounts**

All account created for both infrastructure hosting Discovery application components and application administrative accounts are created by GSA staff that manage the Discovery system or under the request of a designated contractor. All Cloud.gov accounts are created by the Cloud.gov management team in line with their current FedRAMP'd security controls and assigned to the Discovery organizations. Discovery management then assigns the users roles needed to accomplish their objectives.

AC-2f

Control: **The organization creates, enables, modifies, disables, and removes information system accounts in accordance with GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO**

All Discovery roles, both infrastructure and application related, are designed to allow for easy onboarding and offboarding based on the underlying need of the GSA staff member of contractor. The Discovery management team approves all new users and role changes, and regular audits are performed to ensure least privilege access controls are in place.

AC-2j

Control: **The organization reviews accounts for compliance with account management requirements at leasy annually**

The Discovery management team or a delgated staff member of contractor performs regular audits of the users having access to a particular infrastructure or application role, and either corrects access permissions (if part of the Discovery management team) or makes recommendations to the Discovery Management team for further action.

It is also possible that the Cloud.gov team might revoke a user currently having access to the Discovery Cloud.gov organization and related spaces based on their defined and approved security controls.

Covered By:

- Access Control Policies for Discovery - Cloud.gov - Managing Team Members
- Access Control Policies for Discovery - GitHub - Managing Organization Teams
- Access Control Policies for Discovery - CircleCI - GitHub Integration
- Access Control Policies for Discovery - Django Documentation

NIST-800-53-AC-3

Access Enforcement

Access Control Policies for Discovery

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

All vendor and contract data within the Discovery repository is openly available to the public so no access control is required. Discovery site administrators granted according to AC-2 must authenticate through a Django authentication, authorization, and session management system.

All Cloud.gov system access is handled according to policies outlined in the AC-2 controls and Cloud.gov's implemented security controls. All access to hosting environments (production and development) are fully self contained and access must be individually granted to each environment.

All GitHub, CircleCI, and related service accounts provide accounts especially tailored to their service offerings and do not interfere with one another. As stated in AC-2, the Discovery management team may grant GSA staff and current contractors access to these services as needed.

Covered By:

- Access Control Policies for Discovery - Cloud.gov - Managing Team Members
- Access Control Policies for Discovery - GitHub - Managing Organization Teams
- Access Control Policies for Discovery - CircleCI - GitHub Integration
- Access Control Policies for Discovery - Django Documentation

NIST-800-53-AC-6

Least Privilege

Access Control Policies for Discovery

Control: **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**

The Discovery management team adheres to the principle of least privilege by assigning only the requisite role access needed to perform the functions of the GSA staff member of current contractor. Users inhabit a role only as long as they need that role to perform their functions.

Role membership is revoked either when the GSA staff member or contractor leaves the project, the Discovery management team deems it necessary, or if the role capabilities are no longer needed by the current GSA staff member or contractor. When role membership is needed again it is regranted under the direction of the Discovery management team.

NIST-800-53-AU

- AU-2: Audit Events
- AU-6: Audit Review, Analysis, and Reporting

NIST-800-53-AU-2

Audit Events

Audit and Accountability Policies for Discovery

AU-2a

Control: **The organization determines that the information system is capable of auditing the following events: 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**

The Discovery application currently logs basic events from Django, such as errors, page loads, data loading requests, scheduling updates, content changes, but does not have granular logging of authentication attempts by users. We can track authentication to the system by filtering in Logstash/Kibana on login access. In the future there will be more granular logging around authentication and account management.

All Cloud.gov and application level events (requests, failures, and warnings) are available at https://logs.fr.cloud.gov.

AU-2b

Control: **The organization 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**

The Discovery management team coordinates with relevant officials within GSA (OCIO, CISO, TTS, etc...) as needed to ensure the application is operating securely and in compliance with applicable regulations and guidelines.

AU-2c

Control: **The organization provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents**

The Discovery management team is constantly striving to improve the quality and responsiveness of the monitoring of auditable events. The organization follows the guidelines as closely as possible, is willing to make changes based on advice and a more detailed assessment from GSA security officials, and will provide a rationale for all event related audit decisions when asked.

In the future a more comprehensive audit policy will be drafted to ensure the commonly requested information is available in a handy format for security professionals and auditors.

AU-2d

Control: **The organization determines that the following events are to be audited within the information system: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. Settings to be audited continually for each identified event**

The Discovery application records requests for data, modifications, and removal. We can track authentication and other information through request submissions, and collect all Cloud.gov related information.

The administrative logging mechanism is not complete. More granular event track is still needed to encompass the guidelines outlined within this control. This logging system is in the Discovery backlog.

Covered By:

- Audit and Accountability Policies for Discovery - Cloud.gov - Log Search Interface
- Audit and Accountability Policies for Discovery - Django Documentation

NIST-800-53-AU-6

Audit Review, Analysis, and Reporting

Audit and Accountability Policies for Discovery

AU-6a

Control: **The organization reviews and analyzes information system audit records at least weekly for indications of GSA S/SO or Contractor recommendations to be approved and accepted by the GSA AO**

All application and hosting provider related log entries are stored within Logstash, available through a Kibana interface at https://logs.fr.cloud.gov. Logs are continuously checked for abnormalities, and GSA staff and current contractors working on the system can file issues on the Discovery Trello board for implementation prioritization.

In the future more granluar logging and monitoring logic and systems may be employed to ensure that errors and system issues can be caught in the most secure and timeliest fashion.

AU-6b

Control: **The organization reports findings to ISSO, ISSM, Helpdesk, and the GSA Office of the Chief Information Security Officer following the Incident Reporting Procedures in GSA IT Security Procedural Guide 01-02, Incident Response**

The Discovery management team is just relaunching the Discovery application system into production so does not have much history with the reporting needs outlined in this control. However, the Discovery management team is committed to following all established and recommended practices around reporting when the application goes live.

All members of the Discovery team are responsible for timely reporting of site issues and potential security vulnerabilities. In the future an issue reporting policy will be drafted and referenced in this documentation.

Covered By:

- Audit and Accountability Policies for Discovery - Cloud.gov - Log Search Interface
- Audit and Accountability Policies for Discovery - Discovery Trello Board

NIST-800-53-CA

- CA-8: Penetration Testing

NIST-800-53-CA-8

Penetration Testing

Security Assessment Policies for Discovery

Control: **The organization conducts penetration testing annually on internet accessible components**

The Discovery management team requests a Penetration Test to be conducted by an independent team under the management of the GSA Information Security team or via an accredited FedRAMP third-party assessment organization annually.

NIST-800-53-CM

NIST-800-53-CM-2

Baseline Configuration

Configuration Management Policies for Discovery

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

The Discovery application uses configuration management and service automation extensively to provide a fully duplicatable environment between platforms, and ensure that we are able to consistently execute operations successfully across systems, developers, and maintainers. The underlying philosophy is to create executable scripts for every operation and software setup / configuration to enhance productivity and efficient learning of the system.

The Cloud.gov hosting environment manages all configurations as a services bound to applications that expose environment variables that are generated by the system. The application infrastructure is built from a Python Cloud Foundry Buildpack, as well as Python Debian based containers. The Django application is built from requirements files in the top level directory of the source code, and the operations are all defined as executable software, mostly executed for development purposes locally on a desktop/laptop or through CircleCI to automate tasks based on source updates, such as testing, documentation generation, and application deployment.

At any given time, the application can be audited and recreated exactly as it exists at that point of time without manual administrative effort. The Discovery project seeks to minimize, as much as possible, manual human centered tasks in the development process.

Covered By:

- Configuration Management Policies for Discovery - Discovery Scripts
- Configuration Management Policies for Discovery - Cloud.gov Hosting
- Configuration Management Policies for Discovery - Django Documentation
- Configuration Management Policies for Discovery - CircleCI - Documentation

NIST-800-53-CM-3

Configuration Change Control

Configuration Management Policies for Discovery

CM-3a

Control: **The organization determines the types of changes to the information system that are configuration-controlled**

The Discovery management team and maintainers have chosen a development strategy where all code updates and configurations are versioned, tested, and deployed through automation instead of human interaction. This means all changes to the software system are configuration controlled. Our policy is that there should be nothing that is not configuration controlled.

There are certain configurations related to online services we use, such as GitHub, CircleCI, and Cloud.gov that require custom configurations, such as environment variables, that control access to other accounts and resources. These are not versioned and must be inspected within the appropriate environment. If old credentials are lost, new credentials are generated to replace them. These service "variables" are the only configurations in the system, not versioned. They are, however, auditable at any time.

CM-3b

Control: **The organization reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses**

Security is a prime consideration with the underlying hosting environment and administrative system behind the Discovery application. We only install what we need to serve the intended application purpose, and run the application in the moderately secure Cloud.gov hosting environment. The security implications of any proposed changes are researched, reviewed, and discussed with the Discovery management team and possibly the Discovery Authorizing Official or other relevant security officials.

The Discovery management team ensures that the Discovery application is compliant with all required FISMA standards and GSA security guidelines. The management team all have administrative access to all hosting and monitoring environments, and recieve notifications when new updates are pushed to the Discovery code base.

CM-3c

Control: **The organization documents configuration change decisions associated with the information system**

The Discovery management team maintains a Trello board and an application level issue queue that prioritizes all work conducted on the Discovery system. Documents may be created for certain features or fixes that outline in various levels of detail configuration changes to the system, depending upon the nature of the change. GitHub/Git maintains a log of all committers and the changes they have made so finding the source of a change is trivial.

Changes made to configurations within a service boundary, such as Cloud.gov, CircleCI, or GitHub are not versioned and there is currently no way to see consistently who changed configurations and why. However, discussions are conducted with Discovery management before any configuration change in a service environment.

CM-3d

Control: **The organization implements approved configuration-controlled changes to the information system**

Development of the Discovery application system occurs in an Agile fashion with a backlog of prioritized issues. The Discovery management team can prioritize any configuration updates as needed, or in coordination with GSA security personnel. Deployments to the online staging and production environments can happen anytime within a Sprint, allowing us to move extremely quickly to patch security vulnerabilities and other issues found during the course of normal operations of the Discovery application.

CM-3e

Control: **The organization retains records of configuration-controlled changes to the information system for a period of not less than 1 year or in accordance with record retention policies and procedures; whichever is greater**

The Discovery application system is version controlled with the Git revision control system, which carries with each project a complete history of the changes to the source code and related non secure configurations. This Git commit log is available at anytime to anyone and can highlight the source of changes to the application.

Version control is only helpful if configurations are versioned and manual entry of configurations and executed operations are avoided. To help provide an optimum environment for the near complete versioning of the Discovery application, we follow the principle of automating everything possible. Instead of documentation that tells someone how to do something with Discovery, we create scripts and other Python commands that execute sequences of known tasks with consistent naming conventions, and configuration parameters.

The only configurations and data not versioned are secure connectivity information in staging and production environments, service parameters, and data loaded from external sources, like SAM and FPDS systems. No history is stored for the changes of these variables for security reasons. If connectivity is lost or we lose credentials, they are regenerated for security purposes.

CM-3f

Control: **The organization audits and reviews activities associated with configuration-controlled changes to the information system**

The Discovery application Git history and application logs are reviewed regularly to ensure there are no changes that would adversely affect the operation or integrity of the platform. Adjustments to the configuration audit policy is reviewed and can be continuously updated and revised by the Discovery management team based on recommendations by GSA staff or current contractors working on the Discovery application.

CM-3g

Control: **The organization coordinates and provides oversight for configuration change control activities through GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO. Systems shall establish a central means (bulletin, status page, etc) of communicating major changes/development affecting services**

The Discovery application currently has no central status reporting page or bulletin for communicating major changes or outages of the Discovery application. The Discovery management team welcomes working with the GSA AO to implement a suitable interface in the future that can accellerate security related authorizations and future ATOs.

Covered By:

- Configuration Management Policies for Discovery - Cloud.gov Hosting
- Configuration Management Policies for Discovery - Django Documentation
- Configuration Management Policies for Discovery - CircleCI - Documentation
- Configuration Management Policies for Discovery - Discovery Trello Board

NIST-800-53-CM-6

Configuration Settings

Configuration Management Policies for Discovery

CM-6a

Control: **The organization establishes and documents configuration settings for information technology products employed within the information system using GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines in hardening their systems, as deemed appropriate by the GSA Authorizing Official. Implemented checklists must be integrated with Security Content Automation Protocol (SCAP) content (if available and/or to the greatest extent possible.)**

The Discovery management team, GSA staff, and current contractors working on the Discovery application system attempt to ahere to all of the guidelines outlined in this control. We are currently working on bringing our overall documentation up to speed with the guidelines and using technologies, such as Compliance Masonry (Open Control) to ensure we can leverage community efforts in this process.

We welcome all feedback from the GSA information security professionals on their desired format and informational scope for auditing security compliance within the Discovery application.

CM-6b

Control: **The organization implements the configuration settings**

As outlined in CM-3d, the Discovery team maintains as many configuration settings as possible in version control and implements new configuration updates (secure and non-secure) in accordance with an Agile development process that allows for rapid release of software updates into the staging and production environments.

CM-6c

Control: **The organization identifies, documents, and approves any deviations from established configuration settings for all information system components based on GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO**

The Discovery management team, GSA staff, and current contractors working on the Discovery application system attempt to closely adhere to all established rules and guidelines put forth by the GSA Authorizing Official, and in the instances where we can not for some reason, we clearly document and discuss the deviation with the GSA AO to get advice and approval before actually deviating from the expectations of the system.

In the event that we intend to implement a security guideline or policy, we may ask for additional time to prioritize the security recommendation with the limited development resources assigned to the project at a given time. This process is conducted in an open environment with full visibility and collaboration with the GSA security staff and Authorizing Official.

CM-6d

Control: **The organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures**

The Discovery application relies on technologies and configuration management systems used by other online properties within the GSA family of applications, particularly 18F (who originally built this application). All configuration changes to these systems are made in accordance with all applicable GSA policies and procedures.

In the event that we are not following an established organizational policy or procedure, we will make prioritized security updates to the system and underlying management processes to ensure compliance upon request.

Covered By:

- Configuration Management Policies for Discovery - USGCB Checklists
- Configuration Management Policies for Discovery - SCAP Information
- Configuration Management Policies for Discovery - Discovery Trello Board

NIST-800-53-CM-8

Information System Component Inventory

Configuration Management Policies for Discovery

CM-8a

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

With the Discovery application system everything needed to run the application is defined and included within the source code. We build standardized development machines with Vagrant, run standardized application runtime environments with Docker locally and with CircleCI, utilize community developed Python buildpacks for Cloud.gov, and define all versioned application dependencies in top level requirements files, that can be easily audited. The goal is to spin up the Discovery application cluster with a single command. This means everything needed to run Discovery is documented in executable form in the source code.

The Discovery application is layered like an onion. At the bottom we have AWS (covered in AWS FedRAMP authorization), that houses Cloud.gov (covered in FedRAMP JAB authorization), that uses standard Python environments, and service architecture. In the future we will move to using Docker images on Cloud.gov instead of buildpacks to ensure parity between local development environments, CI/CD environments, and remote hosting environments.

All versions of required software, with the exception of some development tools and Docker are pegged at a specific version that has been tested and is running in the production or staging environments. Since the Discovery application is entirely virtual, there is no hardware inventory.

CM-8b

Control: **The organization reviews and updates the information system component inventory after every change**

The Discovery application Git commit log maintains a record of every component change to the system and is reviewed before every merge into our development and production mainline branches. All application changes are deployed through CircleCI CI/CD service so all component changes must flow through the base develop and master braches before being served to the public. This history is auditable and it is easy to see who updated components, and when.

Covered By:

- Configuration Management Policies for Discovery - Cloud.gov Hosting
- Configuration Management Policies for Discovery - Django Documentation
- Configuration Management Policies for Discovery - CircleCI - Documentation
- Configuration Management Policies for Discovery - Vagrant Documentation
- Configuration Management Policies for Discovery - Docker Documentation

NIST-800-53-IA

- IA-2: Identification and Authentication (Organizational Users)
- IA-2 (1): Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts
- IA-2 (2): Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts
- IA-2 (12): Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials

NIST-800-53-IA-2

Identification and Authentication (Organizational Users)

Identification and Authentication Policies for Discovery

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

The Discovery application system uses quite a few systems to provide the capabilities to the public. Each system has different authentication mechanisms, but all are commonly used at GSA and 18F currently. These authentication systems include; GitHub, CircleCI, Cloud.gov, and native Django authentication.

All external services the Discovery application uses are approved for use at GSA and are covered by those respective authorizations. Cloud.gov is well documented for FedRAMP JAB authorization.

Currently we authenticate and manage a very small group of Django administrative users through the default Django authentication system using Redis based sessions stored across a cluster of web servers. These users have a unique username, email, and securely stored/hashed password.

Covered By:

- Identification and Authentication Policies for Discovery - Cloud.gov Hosting
- Identification and Authentication Policies for Discovery - Django Documentation
- Identification and Authentication Policies for Discovery - CircleCI - Documentation
- Identification and Authentication Policies for Discovery - GitHub Documentation

NIST-800-53-IA-2 1

Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts

Identification and Authentication Policies for Discovery

Control: **The information system implements multifactor authentication for network access to privileged accounts**

All lower level host environment access for the Discovery application system utilizes multifactor authentication for all organization managers, and space managers/developers. Services such as GitHub also provide multifactor authentication.

The application does not currently implement multifactor authentication, but in the future it is possible to use the Cloud.gov UAA authentication and access system to login to Django as an administrative user. This is currently in the Discovery backlog.

Covered By:

- Identification and Authentication Policies for Discovery - Cloud.gov Hosting
- Identification and Authentication Policies for Discovery - GitHub Documentation

NIST-800-53-IA-2 2

Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts

Identification and Authentication Policies for Discovery

Control: **The information system implements multifactor authentication for network access to non-privileged accounts**

All lower level host environment access roles (including auditors for organizations and spaces) utilize multifactor authentication. Services such as GitHub also provide multifactor authentication.

The application does not currently define non-privileged users, as all of the content hosted on the Discovery platform is freely available to the public through anonymous access.

Covered By:

- Identification and Authentication Policies for Discovery - Cloud.gov Hosting
- Identification and Authentication Policies for Discovery - GitHub Documentation

NIST-800-53-IA-2 12

Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials

Identification and Authentication Policies for Discovery

Control: **The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials**

The Discovery application system is not designed for PIV access, and most likely will not be unless prioritized by the Discovery management team with the GSA Authorizing Official and other relevant GSA security officials.

NIST-800-53-PL

- PL-8: Information Security Architecture

NIST-800-53-PL-8

Information Security Architecture

Security Planning Policies for Discovery

PL-8a

Control: **The organization 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**

The Discovery management team, GSA staff, and contractors currently working on the system take the security of the platform seriously, which is why we have automated and employed the practice of least privilege when possible in the operations of the Discovery application. The Discovery system relies upon security provided by Cloud.gov and provides a mostly anonymous browsing experience for our users that is protected from malicious injection of information or commands.

The Discovery system is just now coming back online after a lengthy period offline. The team is currently working through compliance related documentation, and have the drafing of a formal Information Security Architecture document in the project backlog. The draft of this document can be prioritized by the Discovery management team in coordination with the GSA Authorizing Official.

PL-8b

Control: **The organization reviews and updates the information security architecture at least annually to reflect updates in the enterprise architecture**

Since there is no current version of the Information Security Architecture for the Discovery application system, we still need to create the first version. The creation of an initial Information Security Architecture that is in alignment with GSA enterprise architecture is currently in the project backlog and expected to be completed within the year.

Once the first draft of the Information Security Architecture document is created, it will be continuously reviewed at least monthly for changes based on new research into security practices, discussions with GSA and other federal security professionals, and concerns and audits conducted by the Discovery team.

PL-8c

Control: **The organization ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions**

The Discovery team will maintain a security status, prioritized backlog of security issues, information security architecture, that will be integrated into a holistic security plan, which will include CONOPS documentation, and information on organizational procurements/acquisitions.

This documentation will live in the GitHub source repository and be available through a comprehensive Discovery documentation site, located at: http://pshcdevops.github.io/discovery/

Covered By:

- Security Planning Policies for Discovery - GitHub Documentation
- Security Planning Policies for Discovery - Discovery Documentation

NIST-800-53-RA

- RA-5: Vulnerability Scanning

NIST-800-53-RA-5

Vulnerability Scanning

Risk Assessment Policies for Discovery

RA-5a

Control: **The organization scans for vulnerabilities in the information system and hosted applications monthly for Operating System (OS) and web application scanning; quarterly Database scanning (as applicable); and, OS and Web application scanning with every code release, and when new vulnerabilities potentially affecting the system/applications are identified and reported**

The Discovery application is currently getting ready for relaunch in the production environment, and will be available to the public. The site has been dormant for months and scans are just starting to be conducted to detect vulnerabilities before it goes live. Once the initial penetration testing is completed, we will begin a regular routine of internal vulnerability scanning through OWASP ZAP and static code analysis, using a tool, such as Bandit (an open source static analysis tool). Any vulnerabilities or code issues found will be added to the project backlog for prioritization by the Discovery management team and the GSA Authorizing Official.

Currently before any code gets deployed through CircleCI, unit and acceptance tests for the codebase must pass, which helps us catch potential issues before they wind up on the site. In the future we will add more automated testing to this process to further reduce the potential for introduction of code vulnerabilities in a live environment.

RA-5b

Control: **The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for; 1) Enumerating platforms, software flaws, and improper configurations; 2) Formatting checklists and test procedures; and 3) Measuring vulnerability impact**

The Discovery team uses open source tools for scanning and testing that can be easily used openly and freely in other GSA projects. All tools we use are commonly used in other GSA projects, ensuring that we can evolve in a similar direction over time.

We are trying to use standards like Open Control to help eliminate redundant work and make verification of security controls and standards reporting more standardized. All issues found end up on the Discovery Trello board for prioritization by Discovery management in coordination with the GSA Authorizing Official.

The Discovery team welcomes all feedback on new processes and tools to integrate into our automated CI/CD processes in the future. All suggestions will be prioritized by the Discovery management team.

RA-5c

Control: **The organization analyzes vulnerability scan reports and results from security control assessments**

All results from vulnerability scans are researched and issues solved as quickly as possible by the Discovery team. All issues found from the vulnerability scanning results are prioritized on the project Trello board by the Discovery management team in coordination with the GSA Authorizing Official and other relevant security professionals.

The Cloud.gov hosting environment maintains it's own vulnerability scanning procedures, which should be available in the Cloud.gov SSP Control documentation.

RA-5d

Control: **The organization remediates legitimate high-risk vulnerabilities mitigated within thirty days; moderate risk vulnerabilities mitigated within ninety days in accordance with an organizational assessment of risk**

The Discovery application is built using an Agile development and maintenance philosophy giving the team immense flexibility in executing feature work to fix high risk vulnerabilities. All high risk vulnerabilities are prioritized above feature work, and can be deployed to the live staging and production environments in days or weeks. All high risk vulnerabilities are fixed and deployed to production within thirty days, and other moderate issues within sixty days of discovery.

RA-5e

Control: **The organization shares information obtained from the vulnerability scanning process and security control assessments with ISSO, ISSM, System Program Manager, and submits quarterly as part of the POA&M to the GSA OCISO (unless scanned by GSA enterprise vulnerability scanning solution) to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies)**

The relevant divisions of GSA that maintain security across the organization may have access to any and all security related documentation and security vulnerability testing results. The Discovery management team can also regularly forward security vulnerability and testing results to delegated officials within GSA when conducted if requested.

Covered By:

- Risk Assessment Policies for Discovery - CircleCI Documentation
- Risk Assessment Policies for Discovery - Discovery Trello Board

NIST-800-53-SA

- SA-11 (1): Developer Security Testing and Evaluation | Static Code Analysis
- SA-22 (1): Unsupported System Components

NIST-800-53-SA-11 1

Developer Security Testing and Evaluation | Static Code Analysis

System and Services Acquisition Policies for Discovery

Control: **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**

Currently the Discovery application maintains a process of routine unit and acceptance testing upon pushing to the official source repository or merges to the develop or master branches, but static code analysis is not yet implemented as an automatic tool that runs as part of the CircleCI CI/CD process.

There is currently a task in the Discovery project backlog to implement CI/CD based static code analysis on pushes to the official GitHub repository or merges to protected branches awaiting prioritization by the Discovery management team in coordination with the GSA Authorizing Official.

Covered By:

- System and Services Acquisition Policies for Discovery - GitHub Documentation
- System and Services Acquisition Policies for Discovery - CircleCI Documentation
- System and Services Acquisition Policies for Discovery - Discovery Trello Board

NIST-800-53-SA-22 1

Unsupported System Components

System and Services Acquisition Policies for Discovery

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

The Discovery application is built using an Agile process and components can be added and removed in a relatively short amount of time. When a component is not being used it is promptly removed from the system and the application is redeployed as soon as is feasable.

When a needed component is not actively maintained and we need fixes or features, the Discovery team has the ability to fork the project, update to our needs, and submit a pull request back to the upstream repository. We have employed this approach with two dependency libraries so far. If the changes are integrated back upstream we can eliminate our fork and start using the upstream project again to gain the community contributions that the upstream project may benefit from.

Occasionally the Discovery team under the direction of Discovery management, may replace a working and supported component due to a superior component becoming available. This may allow us to take advantage of newer features that benefit the application users in ways not originally envisioned.

Covered By:

- System and Services Acquisition Policies for Discovery - Discovery Trello Board

NIST-800-53-SC

- SC-7: Boundary Protection
- SC-12 (1): Cryptographic Key Establishment and Management | Availability
- SC-13: Cryptographic Protection
- SC-28 (1): Protection Of Information At Rest | Cryptographic Protection

NIST-800-53-SC-7

Boundary Protection

System and Communications Protection Policies for Discovery

SC-7a

Control: **The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system**

All Discovery application components are hosted within the Cloud.gov Platform as a Service boundary. All external access to the Discovery application is gated through an AWS ELB that send traffic to a router that ultimately makes requests of the application Waitress server (WSGI Python web server).

Internal to Cloud.gov, the Discovery environment is broken up into multiple, near identical, spaces (one production, one staging, and potentially other test environments). Each space has applications and services. Only the web server has an external route and is accessible through a consistent hostname. Applications talk to service instances which are protected from outside access. See Cloud.gov SSP Control documentation for more details on this system.

All incoming requests and outgoing requests are logged and tracked through a Cloud.gov Logstash / Kibana interface.

SC-7b

Control: **The information system implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks**

The Discovery application components are logically separated and only accessible in very limited circumstances. All applications are in their own space (which prevents administrative and development clashes), web accessible application instances are in another subnet than the data services they connect to. All services have internally generated connection information and credentials assigned at runtime based on system usage and internal rules. See Cloud.gov SSP Control documentation for more details.

The application itself is divided into multiple applications. Currently there are web applications, workers, and schedulers. Each interacts with each other purely through manipulation of data in the Cloud.gov service tier.

For local development and CI/CD purposes Docker and Docker Compose are used when possible to encourage a more unified system architecture starting at the underlying OS. These local clusters maintain their own Docker and virtual machine based networks and are not meant to be accessible from the outside.

SC-7c

Control: **The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture**

The Discovery application system periodically fetches all data that is available through the Discovery API and web interface. These requests pull publically available data from SAM API registrations and FPDS contract awards and modifications. All of the data is ingested through worker servers who make HTTPS requests to the underlying API endpoints. The SAM API is a RESTful interface requiring a Data.gov key, where as FPDS is loaded via ATOM FEEDS for various DUNS numbers.

All data that we request and that lives within the Discovery database is freely available through other government sources.

Covered By:

- System and Communications Protection Policies for Discovery - Cloud.gov Documentation
- System and Communications Protection Policies for Discovery - Docker Documentation
- System and Communications Protection Policies for Discovery - Django Documentation
- System and Communications Protection Policies for Discovery - SAM API

- System and Communications Protection Policies for Discovery - FPDS ATOM Feeds

NIST-800-53-SC-12 1

Cryptographic Key Establishment and Management | Availability

No information found for the combination of standard NIST-800-53 and control SC-12 (1)

NIST-800-53-SC-13

Cryptographic Protection

System and Communications Protection Policies for Discovery

Control: **The information system implements FIPS 140-2 validated encryption modules for digital media stored outside of controlled areas; e-mail; for data on portable storages devices; web sites (internal and public) with logon functions (must also implement TLS); and all sensitive information such as Personally Identifiable Information (as deemed by the data owner) transmitted outside the GSA firewall in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards**

The Discovery application system does not handle Personally Identifiable Information (PII) or send / receive emails. The Discovery data consists almost entirely of publically available government supplied information from other APIs and spreadsheets. The Django system does implement administrative users, which can maintain users, content, and scheduled tasks, but these users have no PII included in their profiles. All user Django administrative passwords are cryptographically hashed for security.

The Discovery team strives to follow all guidelines, regulations, and standards relating to encryption of sensitive data, and welcome suggestions from relevant GSA security staff on increasing our security.

Covered By:

- System and Communications Protection Policies for Discovery - Django Documentation

NIST-800-53-SC-28 1

Protection Of Information At Rest | Cryptographic Protection

System and Communications Protection Policies for Discovery

Control: **The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of Personally Identifiable Information and all sensitive information (as deemed by the data owner) on stored data (e.g., database)**

The Discovery application currently contains no PII that is not already publically available. The system has a limited number of administrative users, but these accounts have no personal information, and all passwords are hashed to prevent snooping and compromised accounts.

Covered By:

- System and Communications Protection Policies for Discovery - Django Documentation

NIST-800-53-SI

NIST-800-53-SI-2

Flaw Remediation

System and Information Integrity Policies for Discovery

SI-2a

Control: **The organization identifies, reports, and corrects information system flaws**

The Discovery management team, GSA staff, and contractors currently working on the Discovery application continuously test the system and report bugs and issues with the system. It is also possible that external contributors might file issues through the GitHub issue queue.

All information system flaws are added to the Discovery project backlog and prioritized by the Discovery management team in coordination with the Discovery team and other relevant GSA officials.

SI-2b

Control: **The organization tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation**

All software used to develop the Discovery application is installed, tested, and packaged on an included Virtual Machine image built for Vagrant. This ensures that there is a standard and isolated environment with which to conduct development of the Discovery application. On top of the Virtual machine development environment, we create Docker clusters to standardize the application runtime environment. We align the Docker build and Cloud.gov buildpack as closely as possible to ensure some level of standardization.

In the future we will replace the Python buildpack with GSA Docker repository hosted images to align all required application infrastructure and dependencies across local development, CI/CD environment, and the various hosting environments. Cloud.gov allows us to use Docker images on hosted registries instead of buildpacks, and we want to take advantage of this capability to unify and standardize.

SI-2c

Control: **The organization installs security-relevant software and firmware updates within scheduled monthly patching maintenance windows following change control processes (including testing) with the ability to push emergency patches on demand from either the direction of the CISO or the AO. In terms of vulnerability remediation, High-risk vulnerabilities shall be mitigated within thirty days; moderate risk vulnerabilities mitigated within ninety days of the release of the updates**

All Discovery application components are updated as time permits or whenever a major security vulnerability is discovered and prioritized by the Discovery management team in coordination with the CISO or Authorizing Official.

All software is immediately deployed to various host environments subject to passing of unit, acceptance, and other tests, allowing for rapid response to security vulnerabilities. Vulnerabilities can be found, fixed, and deployed in less than a week in a safe manner that does not disrupt normal operations for users of the Discovery application.

SI-2d

Control: **The organization incorporates flaw remediation into the organizational configuration management process**

All non secure Discovery application configurations are version controlled through Git, so configuration changes are pushed and merged along with the code fixes for the flaw remediation process.

All secure Discovery application configurations can be rotated as needed to maintain security.

Covered By:

- System and Information Integrity Policies for Discovery - GitHub Project Issues

- System and Information Integrity Policies for Discovery - Discovery Trello Board
- System and Information Integrity Policies for Discovery - Cloud.gov Hosting
- System and Information Integrity Policies for Discovery - CircleCI - Documentation
- System and Information Integrity Policies for Discovery - Vagrant Documentation
- System and Information Integrity Policies for Discovery - Docker Documentation

NIST-800-53-SI-4

Information System Monitoring

System and Information Integrity Policies for Discovery

SI-4a

Control: **The organization monitors the information system to detect; 1) Attacks and indicators of potential attacks in accordance with GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO; and 2) Unauthorized local, network, and remote connections**

All Discovery application requests are logged, both through Logstash/Kibana and Google Analytics. Through these two systems we can get a good picture of who is visiting the site, when, for how long, and what parts they are frequenting.

Since the Discovery application is designed to be used by anonymous people without any restrictions we do not experience unauthorized connections at the application level. See Cloud.gov SSP Control documentation for more details on the hosting provider process.

SI-4b

Control: **The organization identifies unauthorized use of the information system through GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO**

The Discovery management team authorizes maintainers and administrators when needed to act on the Discovery application system. There are various roles (such as GitHub maintainer, CircleCI manager, Cloud.gov Space developer, Django administrator) that each have their own functions, documented in the Discovery SSP. A GSA staff member or current contractor working on the Discovery system may be granted access to any roles needed to perform their GSA approved mission.

The Discovery management team in coordination with the Authorizing Official may revoke access to one or more roles as deemed necessary.

SI-4c

Control: **The organization 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**

Currently the Discovery team collects application and hosting provider based logs, and traffic information for the application frontend, but we are currently lacking application performance monitoring through a service like New Relic. There is a task in the Discovery project backlog to add New Relic monitoring to the Discovery application to more effectively track outages and performance issues.

When loading data from external sources, such as SAM and FPDS, we collect memory readings over time to track resource efficiency of the update processes.

SI-4d

Control: **The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion**

All documentation related to security monitoring is stored in GSA approved and secured storage mediums, such as Google Drive. All security related interfaces are secured with least privilege security principles.

SI-4e

Control: **The organization 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**

If the Discovery application were to experience a heightened security threat level, the Discovery team would spend more time researching the various logs and traffic patterns of the users. If there were security concerns that required constant monitoring the Discovery team would coordinate closely with other relevant security professionals and agencies.

SI-4f

Control: **The organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations**

When there is a question pertaining to required monitoring activities within the Discovery application system the Discovery team seeks advice from GSA security and legal professionals.

SI-4g

Control: **The organization provides GSA S/SO or Contractor recommendation to be approved and accepted by the GSA AO**

Any Discovery manager, GSA staff member, or current contractor working on the Discovery application system can make recommendations and add suggested tasks to the Discovery project backlog (IceBox) that can be prioritized by the Discovery management team in coordination with the GSA Authorizing Official.

Covered By:

- System and Information Integrity Policies for Discovery - Cloud.gov Hosting
- System and Information Integrity Policies for Discovery - Cloud.gov Log Search Interface
- System and Information Integrity Policies for Discovery - Google Analytics Documentation
- System and Information Integrity Policies for Discovery - Discovery Trello Board

NIST-800-53-SI-10

Information Input Validation

System and Information Integrity Policies for Discovery

Control: **The information system checks the validity of inputs. They shall be validated for correct syntax and semantics (e.g., character set, length, numerical range, and acceptable values) to ensure they match specified definitions for format and content. Input validation protections will be tested through monthly operating system and web application vulnerability scanning as defined in control RA-5**

The Discovery application is built on the Django web framework which comes with a Query system that escapes queries to prevent SQL injection attacks from user requests or data. This combined with the current limited number of forms on the fontend display gives us a very small likelihood of attack.

All known application vulnerabilities are fixed when found, or the Django version is updated with security fixes.

Covered By:

- System and Information Integrity Policies for Discovery - Django Documentation

System and Services Acquisition Policies for Discovery

References

- Discovery Circle CI
- Discovery Documentation Site
- Discovery Github Repository

Verifications

- CircleCI Documentation
- Discovery Trello Board
- GitHub Documentation

Identification and Authentication Policies for Discovery

References

- Discovery Circle CI
- Discovery Documentation Site
- Discovery Github Repository

Verifications

- CircleCI - Documentation
- Cloud.gov Hosting
- Django Documentation
- GitHub Documentation

Audit and Accountability Policies for Discovery

References

- Discovery Circle CI
- Discovery Documentation Site
- Discovery Github Repository

Verifications

- Cloud.gov - Log Search Interface
- Discovery Trello Board
- Django Documentation

Access Control Policies for Discovery

References

- Discovery Circle CI
- Discovery Documentation Site
- Discovery Github Repository

Verifications

- CircleCI - GitHub Integration
- Cloud.gov - Managing Team Members
- Django Documentation
- GitHub - Managing Organization Teams

Risk Assessment Policies for Discovery

References

- Discovery Circle CI
- Discovery Documentation Site
- Discovery Github Repository

Verifications

- CircleCI Documentation
- Discovery Trello Board

Security Planning Policies for Discovery

References

- Discovery Circle CI
- Discovery Documentation Site
- Discovery Github Repository

Verifications

- Discovery Documentation
- GitHub Documentation

System and Communications Protection Policies for Discovery

References

- Discovery Circle CI
- Discovery Documentation Site
- Discovery Github Repository

Verifications

- Cloud.gov Documentation
- Django Documentation
- Docker Documentation
- FPDS ATOM Feeds
- SAM API

Configuration Management Policies for Discovery

References

- Discovery Circle CI
- Discovery Documentation Site
- Discovery Github Repository

Verifications

- CircleCI - Documentation
- Cloud.gov Hosting
- Discovery Scripts
- Discovery Trello Board
- Django Documentation
- Docker Documentation
- SCAP Information
- USGCB Checklists
- Vagrant Documentation

System and Information Integrity Policies for Discovery

References

- Discovery Circle CI
- Discovery Documentation Site
- Discovery Github Repository

Verifications

- CircleCI - Documentation
- Cloud.gov Hosting
- Cloud.gov Log Search Interface
- Discovery Trello Board
- Django Documentation
- Docker Documentation
- GitHub Project Issues
- Google Analytics Documentation
- Vagrant Documentation

Security Assessment Policies for Discovery

References

- Discovery Circle CI
- Discovery Documentation Site
- Discovery Github Repository