

---

# Table of Contents

|                            |     |
|----------------------------|-----|
| Introduction               | 1.1 |
| About the SSP              | 1.2 |
| System Classification      | 1.3 |
| General System Description | 1.4 |

## Standards

|  |       |
|--|-------|
| AU   | 2.1   |
| AU-1: Audit and Accountability Policy and Procedures             | 2.1.1 |
| AU-2: Audit Events   | 2.1.2 |
| PE   | 2.2   |
| PE-2: Physical Access Authorizations                             | 2.2.1 |
| SC   | 2.3   |
| SC-1: System and Communications Protection Policy and Procedures | 2.3.1 |
| SC-7: Boundary Protection  | 2.3.2 |

## Components

|              |     |
|--------------|-----|
| Audit Policy | 3.1 |
| Audit Policy | 3.2 |

# Freedonia website SSP introduction

These documents constitute the System Security Plan for the Freedonia "Hello World" application. The contents of this file, (from `markdowns/README.md` ) are rendered to appear as the introduction of the SSP by Masonry and GitBook.

## Version and update information

We have yet to implement a strategy to version this document with a creation date and relevants tags.

The source documents are under source-code control with Git and GitHub at the following URL: <https://github.com/pburkholder/freedonia-compliance>

If there are errors or corrections, please submit them to <https://github.com/pburkholder/ato1day-compliance/issues>.

## Standards

- AU
  - AU-1: Audit and Accountability Policy and Procedures
  - AU-2: Audit Events
- PE
  - PE-2: Physical Access Authorizations
- SC
  - SC-1: System and Communications Protection Policy and Procedures
  - SC-7: Boundary Protection

## Components

- Audit Policy
- Audit Policy



## About the System Security Plan

This document is released in template format. Once populated with content, this document will include detailed information about service provider information security controls.

The System Security Plan is the main document in which the CSP describes all the security controls in use on the information system and their implementation.

## Who should use this document?

This document is intended to be used by service providers who are applying for a Provisional Authorization through the Freedonia Federal government FredRAMP program. FredRAMP Federal agencies may want to use it to document information systems security plans that are not part of the FredRAMP program.

Other uses of this template include using it to document organizational information security controls for the purpose of creating a plan to manage a large information security infrastructure. Complex and sophisticated systems are difficult to manage without a documented understanding of how the infrastructure is architected.

## Caveat Emptor!

Much of the narrative is largely baloney as we try to figure out how to represent these interacting consumable layers.

# Freedonia compliance

This System Security Plan provides an overview of the security requirements for the Freedonia Compliance (freedonia-compliance) and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the

Freedonia Compliance information system.

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

| Unique Identifier    | Information System Name | Information System Abbreviation |
|----------------------|-------------------------|---------------------------------|
| freedonia-compliance | Freedonia Compliance    | fd-comp                         |

## 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   |          |      |

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

## Information Types

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

TKTK: The following table needs updating for Freedonia Compliance, currently showing Cloud.gov specs:

| Information Type                     | Confidentiality | Integrity | Availability |
|--------------------------------------|-----------------|-----------|--------------|
| C.3.5.1 System Development           | Low             | Moderate  | Low          |
| C.3.5.2 life-cycle/Change Management | Low             | Moderate  | Low          |
| C.3.5.3 System Maintenance           | Low             | Moderate  | Low          |
| C.3.5.4 Infrastructure Maintenance   | Low             | Low       | Low          |

## E-Authentication Determination

### E-Authentication Question

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

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

TKTK: The above table is inherited from Cloud.gov

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

## E-Authentication Determination

| System Name                     | System Owner | Assurance Level | Date Approved |
|---------------------------------|--------------|-----------------|---------------|
| Cloud.Gov Platform as a Service | 18F/GSA      | Level 2         | Feb 18, 2016  |

TKTK: The above table is inherited from Cloud.gov

## Information System Owner

| Name             | Title                        | Organization | Address | Phone Number | Email Address                          |
|------------------|------------------------------|--------------|---------|--------------|--|
| Peter Burkholder | Freedonia President-for-Life | GovReady     | Address | 202-555-1212 | 1800 J Street NW<br>Washington, DC 200 |

## Authorizing Official

| Name       | Title                | Organization | Address                                  | Phone Number | Email Address     |
|------------|----------------------|--------------|--|--------------|-------------------|
| Aaron Snow | Authorizing Official | 18F/GSA      | 1800 F Street, NW<br>Washington DC 20405 |              | aaron.sn[at]gsa.g |

## Other Designated Contacts

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

## Assignment of Security Responsibility

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

## Information System Operational Status

The system is currently in the life-cycle phase noted in the table that follows. (**Only operational systems can be granted an ATO**).

TKTK: Is a live system that is in alpha considered Operational or UnderDevelopment?

## System Status

| Operational | Under Development | Major Modification | Other |
|-------------|-------------------|--------------------|-------|
|             | X                 |                    |       |

## Information System Type

(this space currently blank)



## Leveraged Authorizations

The Cloud.Gov information system plans to leverage a pre-existing Provisional Authorization. Provisional Authorizations leveraged by this IAWS FedRAMP ATO (issued by the HHS are noted in the table that follows.

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

TKTK Clarify how the above applies to a generic implementation on a public cloud.

# General System Description

## System Function or Purpose

Freedonia Compliance is an online catalog of the current compliance state of Freedonia Compliance, operated by GovReady.

## Information System Components and Boundaries

GovReady runs two VPCs (development and production) for Freedonia Compliance. In each is a single node running Nginx, Node.js and Gitbook with content built from Git repositories hosted by GitHub.

The Freedonia Compliance Information System is hosted within the AWS East Public Cloud in the Northern Virginia Region. AWS services utilized include EC2, EBS, VPC, S3, MFA, Route 53, ELB and IAM. These are listed as leveraged hardware, network and server components.

Physical aspects of the Freedonia Compliance information system are outside of the authorization boundary due to all hardware being physically managed by AWS. While other services are reviewed and approved for use by the GSA OCISO, they were deemed to be ancillary support services that do not directly process/store data but rather provide general support services. These services include Cloudwatch, Cloudtrail, CloudFormation, AWS Config and Trusted Advisor.

TKTK: Update the ff paragraph: The authorization boundary diagram represented within Figure 9-1 depicts the core components which make up the System in its entirety. The diagram specifically depicts, outlined in red, those components that are within the authorization boundary and those that are outside of the boundary. AWS components outside the boundary belong to an authorized System thus allowing for inheritance of the component. Other support services outside the Cloud.Gov information system authorization boundary include, Pager Duty, New Relic, Slack, Trello, GitHub, Code Climate and Cloudability. Pagerduty, Slack and Trello are communication tools used by 18F developers and support staff while New Relic, GitHub and Code climate are developer based tools in support of the Cloud.Gov system. .

## **Network Architecture**

The following architectural diagram(s) provides a visual depiction of the system network components that constitute Cloud.Gov.

TKTK

## **Freedonia/GovReady Security Domain Stack**

### **Identification and Authentication Control**

TKTK: How to write this so that:

- We consume AWS/IAM setting by consuming freedonia-aws-compliance
  - And leverage CloudFormation or IAM+SDK or Terraform to build to spec
- We consume generic tooling for, say, GitHub and SSH by consuming freedonia-tooling-compliance
- The actual I&A for fd-comp is minimal

### **ACLs, Software defined Firewalls and Security Groups**

### **Audit Logging, Monitoring and intrusion detection**

### **Vulnerability Scanning, Penetration testing**

- InSpec?
- OpenVAS?

### **Cloud Inventory and Asset Management**

- TKTK

### **Static and Dynamic Code Analysis**

- TKTK

### **Incident Response Resolution and Communication**

- TKTK

## **Configuration Management and Version Control**

- TKTK

# **System Environment**

## **Cloud.Gov Virtual Private Cloud (VPC) environment**

### **Public Subnet**

### **Private Subnet - Core Tier**

### **Private Subnet - Metrics**

## **User Accounts**

TODO: Update for Freedonia Compliance

All users have their employee status categorized with a sensitivity level in accordance with PS-2. Employees (or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in the table that follows. At this time all users who have access to the 18F AWS VPC and the underlying Cloud.Gov PaaS are internal users. There is no external access granted to users outside of the 18F/USDS programs and GSA.

A user account represents an individual person within the context of a Cloud Foundry installation. A user can have different roles in different spaces within an org, governing what level and type of access they have within that space. The combination of these roles defines the user's overall permissions in the org and within specific spaces in that org. A list of standard cloud foundry user account types can be found in the table below.

## **Types of Users**

TODO: Update for Freedonia Compliance

| <b>Role</b>     | <b>Internal or External</b> | <b>Sensitivity Level</b> | <b>Authorized Privileges and Functions Performed</b>  |
|-----------------|-----------------------------|--------------------------|---|
| Org Manager     | Internal                    | High                     | Add and manage users, View users and edit org roles, View the org quota, Create, view, edit, and delete spaces, Invite and manage users in spaces, View the status, number of instances, service bindings, and resource use of each application in every space in the org, Add domains  |
| Org Auditor     | Internal                    | Low                      | View users and org roles, View the org quota  |
| Space Manager   | Internal                    | High                     | Add and manage users in the space, View the status, number of instances, service bindings, and resource use of each application in the space  |
| Space Developer | Internal                    | Moderate                 | Deploy an application, Start or stop an application, Rename an application, Delete an application, Create, view, edit, and delete services in a space, Bind or unbind a service to an application, Rename a space, View the status, number of instances, service bindings, and resource use of each application in the space, Change the number of instances, memory allocation, and disk limit of each application in the space, Associate an internal or external URL with an application |
| Space Auditor   | Internal                    | Low                      | View the status, number of instances, service bindings, and resource use of each application in the space   |

## Hardware Inventory

|   |
|---|
| <b>None - Leveraged from AWS Infrastructure</b> |
|   |

## Software Inventory

TODO: How do we make this executable?

| Hostname      | Function  | Version          | Patch Level | Virtual (Yes / No) |
|---------------|---|------------------|-------------|--------------------|
| Code Climate  | CloudFoundry Static code analysis tool for the source code    | Latest Version   | NA          | Yes                |
| GitHub        | CloudFondry and Cloud.Gov code repository and version control | Latest Version   | NA          | Yes                |
| Freedonia AMI | operating system used in deployed EC2 instances for Cloud.Gov | Ubuntu 12.04 LTS | 12          | Yes                |

The following table lists all other applications and components used in relation to the Cloud.Gov PaaS information system.

| Component Name | Function   | Version        | Patch Level | Virtual |
|----------------|--|----------------|-------------|---------|
| Nessus         | Vulnerability scanner for the Cloud.Gov platform                           | Latest Version | NA          | Yes     |
| New Relic      | Application and performance metrics for Cloud.Gov                          | Latest Version | NA          | Yes     |
| Cloudability   | Monitor, optimize and govern Cloud Costs related to the AWS Infrastructure | Latest Version | NA          | Yes     |
| Slack          | Message, alert and communications app                                      | Latest Version | NA          | Yes     |

Trello| Used for agile, scrum and story boarding| Latest Version | NA | Yes| |VisualOps| Visual DevOps tool for AWS| Latest Version| NA | Yes| |Pager Duty| Incident communication platform used by DevOps| Latest Version|

## Network Inventory

|   |
|---|
| <b>None - Leveraged from AWS Infrastructure</b> |
|   |

## Ports, Protocols and Services

| Ports<br>(T or U) | Protocols | Services                    | Purpose  | Used By                                |
|-------------------|-----------|-----------------------------|--|--|
| 80<br>(T)         | HTTP      | HTTP                        | CF ec2 web service                                     | AWS, Cloud Foundry                     |
| 22<br>(T)         | SSH       | Secure Shell (SSH)          | Secure command line interface                          | AWS, Cloud Foundry Jumpbox             |
| 53<br>(U)         | DNS       | DNS Service                 | Inbound DNS requests                                   | AWS, Cloud Foundry                     |
| 123<br>(T)        | NTP       | Network Time Protocol (NTP) | Sync time within the network                           | Cloud Foundry, AWS CloudTrail, Syslogs |
| 1                 | ICMP      | Internet Control Message    | Information and diagnostics for network devices (Ping) | AWS, Cloud Foundry                     |

## System Interconnections

|                              |
|------------------------------|
| <b>None - Not Applicable</b> |
|                              |

## **FRIST-800-53-AU**

- [AU-1: Audit and Accountability Policy and Procedures](#)
- [AU-2: Audit Events](#)



# FRIST-800-53-AU-1

## Audit and Accountability Policy and Procedures

### Audit Policy

This text describes how our organization is meeting the requirements for the Audit policy, and also references a more complete description at [./AU\\_policy/README.md](#)

Since the AU-1 `control` is document and disseminate a policy on Audit and Accountability, then this narrative suffices to provide that control. A verification step could be something that checks that the referenced policy is no more than 365 days old.

# **FRIST-800-53-AU-2**

## **Audit Events**

No information found for the combination of standard FRIST-800-53 and control AU-2

## **FRIST-800-53-PE**

- [PE-2: Physical Access Authorizations](#)

## **FRIST-800-53-PE-2**

### **Physical Access Authorizations**

No information found for the combination of standard FRIST-800-53 and control PE-2

## **FRIST-800-53-SC**

- [SC-1: System and Communications Protection Policy and Procedures](#)
- [SC-7: Boundary Protection](#)

## **FRIST-800-53-SC-1**

### **System and Communications Protection Policy and Procedures**

No information found for the combination of standard FRIST-800-53 and control SC-1

# **FRIST-800-53-SC-7**

## **Boundary Protection**

No information found for the combination of standard FRIST-800-53 and control SC-7

# Audit Policy

## References

- [AU Policy](#)



# Audit Policy

## References

- [AU Policy](#)