
# Screendoor Federal Security Documentation

This repository is a collection of security documentation that is intended to support the signing of an Authority to Operate (ATO). This documentation is for the cloud-hosted version of Screendoor, although much of it will be pertinent to an on-premises installation as well.

Screendoor has not gone through the full FedRAMP authorization process. Obtaining a full FedRAMP authorization is currently an 18-24 month process, and comes at a cost that is fully prohibitive to an organization of our size. However, we are hosted on Amazon Web Services (AWS), a FedRAMP Compliant CSP, and we have gathered the necessary documentation in support of a "Lightweight ATO" as defined by GSA.

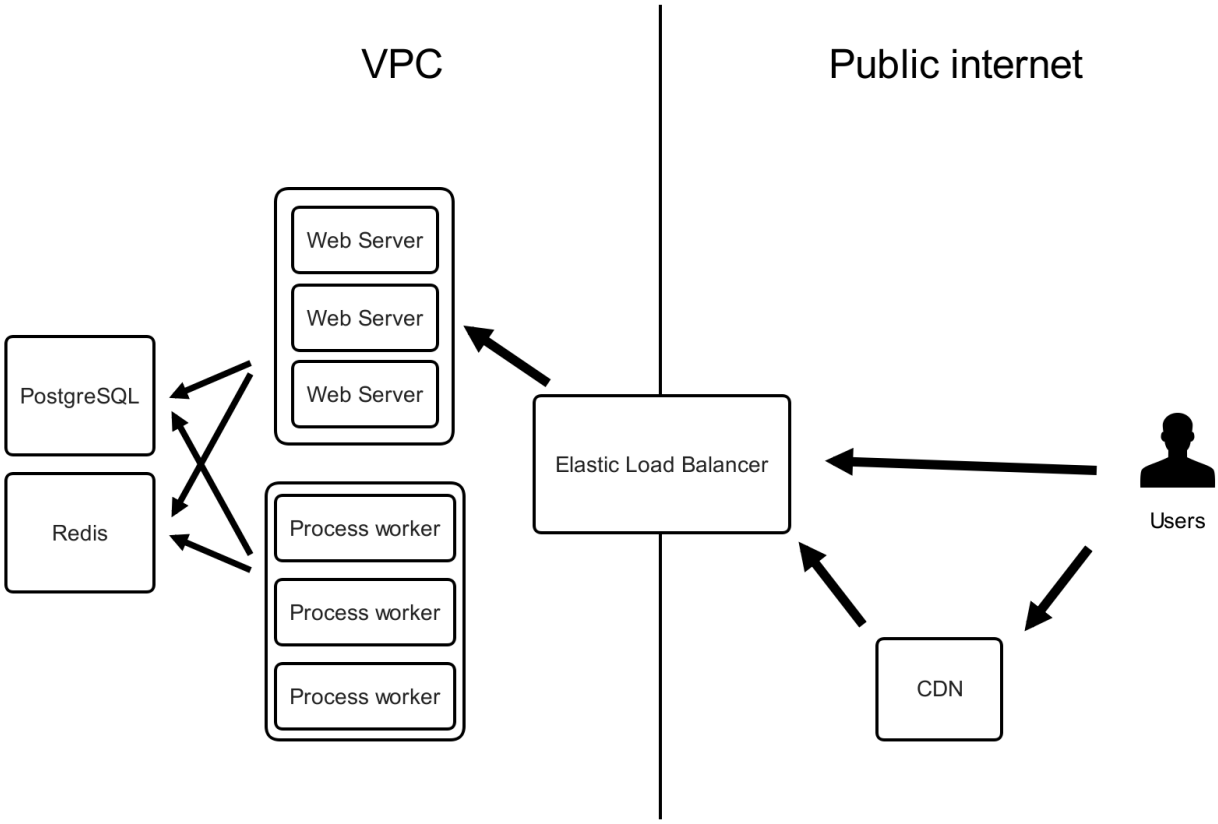
# What is Screendoor?

Screendoor is a cloud-based application that allows government users to build forms, collect responses from the public, and define workflows to manage those incoming responses. It supports a variety of use cases, such as RFP submission and scoring, innovation challenges, fellowship applications, and more. Screendoor is built by the Department of Better Technology (DOBT), a startup founded by former Presidential Innovation Fellows.

# How is Screendoor built, and how does it store information?

Screendoor is a Ruby on Rails application that is hosted in the AWS US-Oregon region.

Internally, all network traffic occurs within Amazon's Virtual Private Cloud. All traffic to the public internet occurs over encrypted protocols such as `https` and `wss`.




# FISMA Categorization

The majority of Screendoor's federal customers are categorized as FISMA Low, since they do not collect PII as per GSA's definition.

# Static scans

Screendoor is continuously scanned with Brakeman, a static code analysis tool for Ruby on Rails. Scans are run continuously on DOBT's continuous integration (CI) system.

See `files/brakeman.txt` for the report.

# Dynamic scans

Screendoor's most recently dynamic scan was performed with HP Fortify On Demand. The results were:

- 4 issues classified as "Low"
- 1 issue classified as "Medium"
  - This issue is a false positive. The scan reports a non-SSL cookie being used, but upon further investigation, it was identifying a Google Analytics cookie. All cookies that Screendoor uses are set as "SSL only".
- 1 *false positive* classified as "High"
  - This issue has been resolved. The scan reported Screendoor as supporting TLS 1.0, but Screendoor's SSL configuration has been updated and it now receives an "A+" from SSL Labs. (See `files/ssl-labs.png` .)

View the report at `files/hp dynamic scan.pdf` .

# System security plan

We have documented our compliance with the 24 NIST controls that are part of a "Lightweight ATO process", as described by GSA CISO Kurt Gabars.

## Account Management

### NIST Controls: AC-2

All requests to Screendoor are authorized at the application level, and will return a 401 status code if the user does not have permission to access the requested resource. Screendoor's user permissions are assigned by role (e.g. "Read only", "Reviewer", "Manager", "Administrator",) and only administrators have the ability to modify these permissions. New accounts must be created by an existing administrator, and administrators also have the ability to remove user accounts. Screendoor does not utilize group credentials.

## Access Control

### NIST Controls: AC-3, AC-6

Screendoor enforces access control policies at the system as well as the application level. Processes run on the principle of "least privilege", and root or admin accounts are not used for application purposes. In addition, DOBT restricts privileged account usage to designated members of the DOBT Ops team. Within the virtual infrastructure the admin account is not used for privileged access; it is used for billing and metrics only.

# Auditing and Accountability

## NIST Controls: AU-2, AU-6

The DOBT Ops team reviews all events that can be audited on a realtime basis using its event and monitoring solutions, and there are systems in place for capturing and storing these events for future review.

DOBT establishes processes for regularly reviewing these audit logs, and reporting security issues if discovered. Reviews will occur on at least a weekly basis.

DOBT employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and responses to suspicious activities.

DOBT employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities that have security implications.

# Security Assessment and Authoriation

## NIST Controls: CA-8

For compliance with NIST Publication 800-53 CA-8, Parameter 1 Penetration Testing of all DOBT Infrastructure and Application Components will occur annually. Parameter 2 Penetration Testing of Publicly Accessible Infrastructure will be performed on the direction of the DOBT Ops team.

# Configuration Management

## NIST Controls: CM-2, CM-3, CM-6, CM-8

DOBT uses Amazon's Ubuntu 12.04.4 LTS image as a baseline configuration. All

additional configuration (for example, nginx.conf) is stored in version control, and any changes to the configuration are tested in a pre-production environment before being deploying to production.

The AWS management console is used to inventory and monitor all resources within the DOBT virtual private cloud. AWS Trusted Advisor is used to find unused or under-utilized resources. The data contained within both the management console and trusted advisor is updated in real-time.

# Identification and Authentication

## NIST Controls: IA-2

All users in Screendoor are uniquely identified with an email address and password combination. In addition, Multifactor authentication is available to all users of the system, both for privileged as well as non-privileged accounts.

Any administrative actions taken on Screendoor by DOBT employees requires authentication via encrypted SSH keys that are only available to specific members of the DOBT Ops team.

# Planning

## NIST Controls: PL-8

DOBT has developed an information security architecture for the Screendoor 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.

DOBT reviews and updates the information security architecture at least quarterly, and ensures that planned information security architecture changes are reflected in the

security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

# Risk Assessment

## NIST Controls: RA-5

DOBT conducts monthly operating system (OS) and web application scanning; quarterly database scanning; and OS and web application scanning with every code release.

DOBT employs vulnerability scanning tools that promote interoperability such as Common Vulnerability Scoring System v2 (CVSS2), Common Platform Enumeration (CPE), and Common Vulnerability Enumeration (CVE), as well as OWASP TOP 10 vulnerabilities.

High-risk vulnerabilities are mitigated within thirty days (30), and moderate risk vulnerabilities are mitigated within ninety days (90).

DOBT shares information obtained from the vulnerability scanning process with the DOBT Ops team in order to help eliminate similar vulnerabilities in other information systems.

# System and Services Acquisition

## NIST Controls: SA-11, SA-22

DOBT utilizes static code analysis tools such as Brakeman and Codeclimate in order to continuously monitor developers' code for security flaws. If a flaw is detected, the developer is alerted immediately, and the code is unable to be deployed until the flaw is remediated. The results of these scans are logged to DOBT's continuous integration (CI) system, where they are available for historical access.

DOBT does not use software where support is no longer available from the developer, vendor, or manufacturer. DOBT implements automated processes that run at least weekly in order to ensure that all software is kept up-to-date, and that the DOBT Ops team is notified of any out-of-date-software.

If it is deemed necessary to use unsupported software, DOBT will provide written justification for its continued use.

# System and Communications Protection

## NIST Controls: SC-7

DOBT implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks. For internal networks, DOBT utilizes the Amazon Virtual Private Cloud, which leverages multiple layers of security, including security groups and network access control lists, to help control access to server instances in each subnet.

All public access to DOBT systems is performed over encrypted protocols such as `https` and `wss`. All requests to DOBT's systems over insecure protocols such as `http` and `ws` are automatically redirected to their secure counterparts.

# System and Information Integrity

## NIST Controls: SI-2, SI-4, SI-10

DOBT identifies all system flaws related to Screendoor, reports flaws to information system owners, authorizing officials, and the DOBT Ops team. DOBT proactively installs software updates (such as patches, service packs, hot-fixes, and anti-virus signatures) to its infrastructure on a monthly basis. Software updates are tested for side-effects in a pre-production environment before being deployed to production. DOBT incorporates flaw remediation into its configuration management process.

The DOBT Ops team monitors Screendoor's infrastructure to detect potential attacks and intrusions from internal and external sources.

DOBT detects unauthorized access to Screendoor using automated monitoring tools, log management, and event analysis. DOBT monitors for attacks and indicators of potential attacks, such as unauthorized local, network, and remote connections.

The infrastructure that hosts Screendoor provides monitoring and intrusion detection at the physical and network layers. DOBT is responsible for monitoring everything related to

its virtual infrastructure, and has deployed monitoring and detection tools within its virtual private cloud to log and detect malicious activities to its information systems including Screendoor.

DOBT ensures that intrusion and monitoring tools are protected from unauthorized access by only granting access to certain members of its Ops team. All monitoring and intrusion information data is protected by limiting accounts to authorized users only, and is maintained in secure repositories for review by those members.

Information system monitoring will be heightened based US-CERT Advisories, advisories from commercial security communities, and other sources.

Screendoor checks the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) and verifies that inputs match specified definitions for format and content. The Ruby on Rails framework ensures that user inputs are always sanitized before being used in database queries.

To mitigate attack vectors such as cross-site scripting and other injection attacks, Screendoor sanitizes user-inputs before rendering them to other users of the system.

There is no manual override for any of Screendoor's input validation.

## References and attachments

- AWS FedRAMP Compliance
- USAID Privacy Threshold Analysis `files/USAID_PTA.pdf`