# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4

## SC: System and Communications Protection

### SC-1: System And Communications Protection Policy And Procedures

The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy [Assignment: organization-defined frequency]; and 2. System and communications protection procedures [Assignment: organization-defined frequency].

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud Service Providers dated 1 May 2013.

##### CivicActions

CivicActions has developed, documented and disseminated to personnel a system and communication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the policy and associated controls. This information is maintained in the CivicActions System and Communications Protection (SC) Policy CivicActions document that can be found in the CivicActions Github repository at <https://github.com/CivicActions/compliance-docs/>.

### SC-5: Denial Of Service Protection

The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: denial of service protection.

##### Drupal

Drupal has a manual ability to block IP addresses in cases where attacks bypass cloud protection. This is managed by CivicActions Operations.

### SC-7: Boundary Protection

The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

##### Drupal

Drupal, when deployed on SELinux in full enforcing mode, minimizes the number of services and computing nodes that are exposed to the Internet. Drupal employs both the AWS platform safeguards and the Drupal Watchdog module in monitoring and recording system events. All other computing nodes used in the system are isolated within AWS.

#### a

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: boundary protection.

#### b

##### AWS

The authorization boundary is completely contained within a Virtual Private Cloud (VPC) created and managed by the AWS Infrastructure as a Service (IaaS). External connections must be explicitly configured via the AWS Security Groups (SG) mechanism. The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: boundary protection.

#### c

##### AWS

Internal organizational networks (e.g. CivicActions private networks) are physically separate from the AWS platform and are protected by managed boundary devices that include FIPS 140-2 validated encryption modules at all entry points. The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: boundary protection.

### SC-13: Cryptographic Protection

The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: cryptographic protection for data in motion (with SSH and HTTPS/SSL) and for data at rest (with Elastic Block Store (EBS) volumnes).

##### CivicActions

The information system implements: • Cryptographic modules through Secure Shell (SSH) to allow administrators to securely logon to the various system components • HTTPS/SSL (TLS) for connection to web-based services • TLS for connection to email services \* AES-256 (FIPS 140-2 validated) for data at rest (with Elastic Block Store (EBS) volumes)

### SC-20: Secure Name / Address Resolution Service (Authoritative Source)

The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

##### AWS

The system inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: secure name / address resolution service (authoritative source)

### SC-21: Secure Name / Address Resolution Service (Recursive Or Caching Resolver)

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

##### AWS

The system inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: secure name / address resolution service (recursive or caching resolver)

### SC-22: Architecture And Provisioning For Name / Address Resolution Service

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

##### AWS

The system inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: architecture and provisioning for name / address resolution service.

### SC-39: Process Isolation

The information system maintains a separate execution domain for each executing process.

##### CivicActions

Process isolation is maintained on the Linux platform. Linux is the only operating system that is part of the boundary.