# 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].

##### 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/>.

##### Project

System and communications protection policy and procedures are formally documented in the None and the Project SSP. The Department reviews and updates the policy as necessary and has been continually updated since April 2008. This is Agency common control. More data about implementation can be obtained from the Agency common control catalog.

### 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].

##### Drupal

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

##### Ilias

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

##### Project

The Project system is configured to reduce vulnerabilities in its operating system and applications to protect against Denial of Service (DoS) attacks. The Project support staff ensures the system is protected against or limits the effect of DoS attacks as specified in the None.

### 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.

##### Ilias

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

##### Project

The Project system has monitored and controlled communications at the external boundary of the information system and at key internal boundaries within the system, where appropriate. The Project allocates publicly accessible information system components (e.g., public web servers) specific IP address and port combinations. Public access into the organization’s internal networks is prevented except as appropriately mediated.

#### a

##### AWS

In this architecture, network communications to, from, and between VPCs, subnets and Amazon S3 buckets are controlled as follows: AWS Route Tables specify which subnets in each VPC are accessible through gateways and which are isolated/private. AWS Security Groups provide stateful inbound/outbound port/protocol restrictions, Amazon Simple Storage Service (Amazon S3) buckets support access control restrictions based on network source/destination.

#### b

##### AWS

In this architecture, subnetworks for publicly accessible system components are logically separated from internal private subnetworks via AWS security groups, refined routing tables, and NACLs.

#### c

##### AWS

In this architecture, connection to external networks is possible only through Internet Gateways (IGWs) or NAT gateways (in regions where supported by AWS VPC) and are restricted based on ports/protocols via AWS Security groups, and default subnet rules provided by NACLs.

### SC-12: Cryptographic Key Establishment And Management

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

##### Project

Use of cryptographic key management for the Project system is in use for at the time of implementation for authentication. CivicActions utilizes customer agency supplied PIV credentials for access to customer instances of the Project. Access enforcement and authentication requirements for Project are described in AC-2 & IA-2. AWS platform does not utilize or manage cryptographic keys within the ACE boundary.

### 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.

##### 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-15: Collaborative Computing Devices

The information system:  
 a. Prohibits remote activation of collaborative computing devices with the  
following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and  
 b. Provides an explicit indication of use to users physically present at the  
devices.

##### Project

This control is not applicable, as the Project system does employ any collaborative computing devices.

### 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.

##### CivicActions

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.

##### CivicActions

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.

##### CivicActions

### 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.