# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4

## CA: Security Assessment and Authorization

### CA-1: Security Assessment And Authorization Policy And Procedures

The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and 2. Security assessment and authorization 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 certification, accreditation, and security assessment 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 Security Assessment and Authorization Policy. This document can be found in the CivicActions Compliance Docs GitHub repository at <https://github.com/CivicActions/compliance-docs>.

### CA-2: Security Assessments

The organization: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].

#### a

##### CivicActions

CivicActions will develop a security assessment plan (SAP) that describes the security controls and control enhancements under assessment, assessment procedures used to determine effectiveness, the assessment environment, the assessment team, and the assessment roles and responsibilities.

#### b

##### CivicActions

CivicActions will assess the security controls in their system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements, All controls assigned and documented in this System Security Plan (SSP) will be tested at least annually or when there is a major change to the system.

#### c

##### CivicActions

CivicActions will produce a security assessment report that documents the results of the assessment. The Security Assessment Report must contain the results of the assessment, and may also contain recommendations and suggestions for plans of actions and milestones (POA&Ms).

#### d

##### CivicActions

CivicActions will provide the results of the security control assessment to the System Owner, Project Manager, CivicActions Security, and the Authorization Official (AO)). The security control assessment package includes the following: • Security Control Matrix • Privacy Impact Assessment • E-Authentication • Contingency Plan • Configuration Management Plan • Rules of Behavior • Incident Response Plan

### CA-3: System Interconnections

The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].

##### CivicActions

This control is not applicable. CivicActions’ systems do not have system interconnections. The only communication conducted to CivicActions’ systems is through the Internet.

### CA-5: Plan Of Action And Milestones

The organization: a. Develops a plan of action and milestones for the information system to document the organization�s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

##### CivicActions

CivicActions documents all deficiencies and vulnerabilities identified during the security certification and/or continuous monitoring phase (via security assessment, vulnerability scanning, risk assessment, etc.) within the Plan of Action and Milestones (POA&M). The POA&M document provides a platform for CivicActions to monitor and track the deficiency and its mitigation strategy. POA&M items will include: • The description of the deficiency, • Dedicated point of contact for this deficiency. • Cost of the mitigation strategy • Associated risk and NIST control • Recommended mitigation strategy POA&Ms are tracked throughout the lifecycle of the system until its mitigation. All POA&Ms are reviewed on a monthly basis by CivicActions Information System Security Officer to ensure all mitigation strategies are continuing as documented.

### CA-7: Continuous Monitoring

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

#### a

##### CivicActions

CivicActions implements a continuous monitoring strategy that incorporates configuration management, system scanning and log analysis processes: • Configuration management includes the assessment of security impact analyses of proposed and implemented changes.

• System scanning is managed by running the OpanSCAP vulnerability scanner using the DISA STIG profile.

• Log analysis is managed by feeding logs to a Graylog dashboard for analysis.

##### Drupal

CivicActions follows recommendations and best practices developed by the Drupal community for monitoring. Examples of specific logs and metrics are included in AU-2 and AU-3.

#### b

##### AWS

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

##### CivicActions

Configuration management and log analysis is carried out in real-time. OpenSCAP security scans are performed and reviewed monthly. See also: RA-5 and SI-4. Quarterly review of the control assessments supporting the monitoring is conducted by CivicActions Operations in collaboration with CivicActions’ Security Office.

#### c

##### Drupal

CivicActions works closely with the Drupal security community and reviews security announcements as part of the continuous monitoring strategy. Items found to require immediate remediation will be addressed.

#### d

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: ongoing security status monitoring.

##### CivicActions

CivicActions conducts or oversees continuous system security monitoring.

#### e

##### CivicActions

CivicActions Security reviews the results of the security scans and security assessments with associated JIRA and/or GitLab Issue tickets created to correlate and analyze security-related information generated from the monitoring tools becoming POA&M items for tracking.

#### f

##### CivicActions

POA&M items are tracked by CivicActions Security through JIRA tickets with a security categorization assigned. The information included in the POA&M item include the severity, the due date, the weakness source identifier, and the plugin ID that identified the vulnerability.

#### g

##### CivicActions

The security status of the system is reported up to the System Owner and Project Manager via CivicActions’ Security Office to be reviewed alongside other security issues relating to the system.

### CA-9: Internal System Connections

The organization: a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

##### AWS

Not applicable: There are no internal systems that connect to the FedRAMP certified AWS cloud.