# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4

## SA: System and Services Acquisition

### SA-1: System And Services Acquisition Policy And Procedures

The organization:  
 a. Develops, documents, and disseminates to [Assignment: organization-defined  
personnel or roles]:  
 1. A system and services acquisition 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 services  
acquisition policy and associated system and services acquisition controls; and  
 b. Reviews and updates the current:  
 1. System and services acquisition policy [Assignment: organization-defined  
frequency]; and  
 2. System and services acquisition procedures [Assignment: organization-defined  
frequency].

##### CivicActions

CivicActions has developed, documented and disseminated to personnel a system and services acquisition 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 by the CivicActions System and Services Acquisition (SA) Policy document that can be found in the CivicActions GitHub repository at <https://github.com/CivicActions/compliance-docs/>.

##### Project

The Project complies with the None. The Project will identify new threats/vulnerabilities and technologies that may require updating of solicitation documents.

This is Agency common control. More data about implementation can be obtained from the Agency common control catalog.

### SA-2: Allocation Of Resources

The organization:  
 a. Determines information security requirements for the information system  
or information system service in mission/business process planning;  
 b. Determines, documents, and allocates the resources required to protect the  
information system or information system service as part of its capital planning and investment control process; and  
 c. Establishes a discrete line item for information security in organizational  
programming and budgeting documentation.

##### Project

The Project System Owner is responsible for leading the annual budgeting process and for tracking organizational spending. The System Owner coordinates with the CivicActions Project Manager and CivicActions Security on at least monthly basis to track security priorities and spending patterns and determine financial requirements. The System Owner also coordinates the approval process for interim increases to the security budget, if required. This data is used to support the development of the annual budget.

Security costs are included in Exhibit 53 in the Department’s on-line electronic Capital Planning and Investment Control system (eCPIC) in order to provide adequate business case information for budget purposes. Security costs are represented across the life cycle in the business case (Exhibit 300) for major investments and (Exhibit 53) for non-major projects - Project is a non-major project. Security costs are summarized and listed as a line item on the Exhibit 53 in the budget submitted to Treasury.

Costs for providing security at the infrastructure level are contained in the business cases for infrastructure supporting computing platforms, desktop processing, the network environment, and web capability. Since the Exhibit 53 includes projections for multiple fiscal years, its intention is to identify and anticipate security resources required.

#### a

##### CivicActions

CivicActions’ Security Office, in collaboration with the System Owner, act and/or meet on a pre-determined basis to determine information system security requirements and to develop implementation budgets and plans.

#### b

##### CivicActions

The CivicActions Security Office, in collaboration with the System Owner, determines, designates, documents, and allocates the resources required to protect the system as part of its capital planning and investment control processes.

#### c

##### CivicActions

The annual budget developed by the System Owner includes explicit budgetary line items for FISMA security requirements. Additional security-related expenditures that fall outside of explicit compliance requirements are addressed in sub-lines under the CivicActions Information Technology budget.

### SA-3: System Development Life Cycle

The organization:  
 a. Manages the information system using [Assignment: organization-defined system  
development life cycle] that incorporates information security considerations;  
 b. Defines and documents information security roles and responsibilities throughout  
the system development life cycle;  
 c. Identifies individuals having information security roles and responsibilities;  
and  
 d. Integrates the organizational information security risk management process  
into system development life cycle activities.

##### Project

The Project draws from the None, NIST SP 800-64, and Agile software development methodology to ensure security requirements are incorporated during each phase of the life cycle. This helps to ensure the development of secure systems and effective risk management.

#### a

##### CivicActions

The system and application(s) are managed by CivicActions using the Agile software development methodology, which provides a continuous System Development Life Cycle (SDLC) methodology. CivicActions Agile management continues to improve the software through ongoing planned code releases. The process is overseen by the Change Control Board (CCB) as described in CM-1. Each point release introduces code and configuration changes to the website through the following SDLC methodology:

* Code release planning: A code release ticket is created in the Change Request project of the CivicActions ticketing system which describes the overall goals of the code release. The code release ticket is linked to other tickets in the ticketing system which describe issues to be addressed by the planned code release. Those issues may include bug fixes and feature enhancements as well as upgrades to newer versions of the software packages that have been used to build the website.
* Sprints: The tickets covered by the planned code release are then implemented through a series of planned sprints, each of which typically lasts two weeks. Each sprint begins with a sprint planning session at which the CCB selects a list of tickets to be implemented. CivicActions Development holds daily coordination meetings throughout the sprint to share information and resolve any problems that may be blocking progress toward completion. At the end of the sprint, a retrospective is performed in which progress is reviewed to determine which issues have been resolved and which need further work.
* Development/unit testing: Work on each ticket is performed within a separate code branch within the CivicActions Git repository, and tested using the GitLab Runner continuous integration platform. Developers also write unit tests to prove their code behaves as expected and address security considerations such as information leakage, bounds checking, and input validation. Once work on a ticket is completed, the developer creates a merge request, and the changes are submitted to at least one other developer for review to ensure they meet functional requirements and address security considerations before the pull request is merged into the Git repository’s development branch for the planned code release.
* Integration testing: Once all work tickets have been completed, the code and configuration necessary to implement the changes are merged into the website’s staging server, where it undergoes additional testing to ensure there are no conflicts between the work that has been done on individual tickets.
* User acceptance testing (UAT): The code release undergoes manual testing against a checklist of expected site behaviors and options each of the website’s defined user roles to further verify that the functional changes work as expected and to identify any changes in user experience that need to be documented in release notes to be shared with the customer.
* Approval for deployment: After all the planned code release has passed all of the above tests, the code release is scheduled for deployment to production and presented to CivicActions’ Change Control Board (CCB) for review and approval.
* Deployment to production: A full backup of the website is performed immediately prior to the deployment.
* Security scan: After the deployment to production, the website undergoes a security scan using a web vulnerability scanner.
* Security issues to be addressed in the planned code release may come from a variety of sources:
* Customer support requests received by the CivicActions Help Desk
* Security concerns, incidents, and site performance issues reported by users
* Security incident reports, including server log analysis and root cause analysis of those incidents performed by the CivicActions Security Office and Operations staff
* Security notifications received by the CivicActions Security Office from external security teams and other software vendors
* Vulnerabilities detected during security scans of the website performed by the CivicActions Security Office
* Issues reported by the CivicActions Security Office, Operations staff and Development
* Security issues reported through continuous monitoring

#### b

##### CivicActions

The CivicActions organization defines and documents information security roles and responsibilities throughout the SDLC. The following teams participate in this process:

* Customer Support: Files tickets when incidents are reported and shares incident reports with customers
* The CivicActions Security Office: Receives security notifications from the Drupal security team and other software vendors; performs security scans; uses CivicActions JIRA ticketing system to request mitigation of all reported vulnerabilities
* CivicActions Development: Performs server log analysis when security incidents are reported; assists in root cause analysis
* Change Control Board: Meets weekly to review and approve upcoming planned code changes to the website, include security-related code releases.
* AWS Cloud: Monitors server and application events; proactively respond to security incidents, and reports incidents to CivicActions
* Users: Communicates customer security requirements and expectations, and alerts the CivicActions customer support team whenever it detects a security or site performance issue

Security responsibilities performed by these teams include the following:

* Perform configuration management during information system design, development, implementation, and operation;
* Implement only organization-approved changes;
* Document approved changes;
* Manage and control changes to the system;
* Fully test all changes, taking into account security considerations as well as other functional requirements;
* Track security flaws and flaw resolution; and
* Employ code analysis tools to examine software for common flaws and document the results of the analysis.

#### c

##### CivicActions

Each of the CivicActions teams described in SA-3(b) has a team leader who is responsible for defining the roles and responsibilities of individual personnel members within that team. CivicActions uses role-based management for access and authentication implementation and enforcement.

#### d

##### CivicActions

The CivicActions organization integrates the organizational information security risk management process into system development life cycle activities by requiring that the processes defined in SA-3(a) and (b) above are adhered to by all information system developers and associated security personnel.

### SA-4: Acquisition Process

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:  
 a. Security functional requirements;  
 b. Security strength requirements;  
 c. Security assurance requirements;  
 d. Security-related documentation requirements;  
 e. Requirements for protecting security-related documentation;  
 f. Description of the information system development environment and environment  
in which the system is intended to operate; and  
 g. Acceptance criteria.

##### CivicActions

The CivicActions System and Services Acquisition Policy affects all personnel with purchasing authorization and applies to all purchases or deployments including infrastructure, software or hardware. The CivicActions System and Services Acquisition Policy contains the process for determining acceptance criteria for all system software and application services.

The Acquisition Security Policy includes an assessment that evaluates the product based on the vendor’s security practices, policies, and past performance. It also details the potential maintenance and end-of-life ramifications with regards to security.

The CivicActions Security Office is responsible for determining the security documentation that must be included in the information system or services acquisition contracts.

Configuration and design of the development and production environments are hosted in the CivicActions Git repository. All documentation is strictly controlled regarding transportation and storage in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

##### Project

The Project follows the guidelines and procedures within the overarching None. The requirements in the information system acquisition contract permit updating security controls as new threat/vulnerabilities are identified and new technologies are implemented.

The Project System and Services Acquisition Policy contains the process for determining acceptance criteria for all Project system software and services.

The Project organization reviews and approves all acquisition contracts in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

### SA-4 (10): Use Of Approved Piv Products

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

##### Project

CivicActions/Project and AWS describes this control as “not applicable”, as PIV credentials are not applicable to the Project system. Access and Authentication requirements for the Project system for internal CivicActions and customer are implemented under access management and enforcement (AC-2 and AC-3) and identification and authentication for all users (IA-2 and IA-8).

It is the responsibility of CivicActions for implementation of PIV capability for authentication as required.

### SA-5: Information System Documentation

The organization:  
 a. Obtains administrator documentation for the information system, system component,  
or information system service that describes:  
 1. Secure configuration, installation, and operation of the system, component,  
or service;  
 2. Effective use and maintenance of security functions/mechanisms; and  
 3. Known vulnerabilities regarding configuration and use of administrative  
(i.e., privileged) functions;  
 b. Obtains user documentation for the information system, system component,  
or information system service that describes:  
 1. User-accessible security functions/mechanisms and how to effectively use  
those security functions/mechanisms;  
 2. Methods for user interaction, which enables individuals to use the system,  
component, or service in a more secure manner; and  
 3. User responsibilities in maintaining the security of the system, component,  
or service;  
 c. Documents attempts to obtain information system, system component, or information  
system service documentation when such documentation is either unavailable or nonexistent and takes [Assignment: organization-defined actions] in response;  
 d. Protects documentation as required, in accordance with the risk management  
strategy; and  
 e. Distributes documentation to [Assignment: organization-defined personnel  
or roles].

##### Project

Client maintains adequate documentation for the Project system. The Project system documentation is protected as required and made available to authorized personnel. Procedures for protecting system documentation include management in the private CivicActions Git repository and the publicly available documentation trees for Free and Open Source Software (FOSS). The documentation maintained for the Project system includes:

* System Security Plan (SSP) – this document
* Configuration documentation
* Incident Response and Contingency Plans
* Rules of Behavior (Acceptable Use Policy)
* FOSS Reference Manuals (Drupal, GNU/Linux, Apache, MySQL, PHP, Postfix, etc.)

#### a

##### AWS

In this architecture, documentation of the infrastructure configuration in the form of AWS CloudFormation templates in JSON or YAML format, architecture diagrams, deployment user guide and security controls implementation details is included.

AWS built-in features include online documentation for management of the infrastructure at http://aws.amazon.com/documentation/

##### CivicActions

Some application features are built on a custom basis and are not part of standard FOSS packages. Administrator documentation for those custom features is maintained in the CivicActions Git repository documentation system.

##### Ilias

Public documentation related to Ilias is maintained by the Ilias Association and is located at <https://Ilias.de/documentation>. This documentation contains administrator documentation for the information system that describes: - secure configuration, installation, and operation of the system, component, or service; - effective use and maintenance of security functions/mechanisms; and - known vulnerabilities regarding configuration and use of administrative functions;

#### b

##### AWS

AWS built-in features include online documentation of AWS services at http://aws.amazon.com/documentation/

1. AWS built-in features include online documentation for AWS account users at http://aws.amazon.com/documentation/ such as user Guides, API reference guides, CLI reference guides and developer reference guides to provide information on how to effectively use security functions.
2. AWS built-in features include online documentation for AWS account users within the infrastructure at http://aws.amazon.com/documentation/ such as user Guides, API reference guides, CLI reference guides and developer reference guides to provide information on how to access AWS services and components in a more secure manner.
3. AWS built-in features include online documentation for AWS account users at https://aws.amazon.com/security/security-resources/ that provides information related to security responsibilities of customers using AWS services.

##### CivicActions

The publicly-available FOSS package documentation described in control SA-5(a) also includes user documentation for non-administrators as described in control AC-3. This includes documentation on how to create and manage user accounts as well as how to create, update and delete content.

CivicActions follows the user documentation standard practice to provide context-sensitive help as well as access to a Help Desk in publicly facing applications.

The CivicActions Customer Support team, described in control SA-3(b), handles questions about how to use the system. Questions are submitted by sending an email to support@civicactions.com, which triggers the creation of a ticket in the CivicActions customer support ticketing system.

##### Ilias

The public documentation at Ilias.de contains user documentation for the information system that describes: - user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; - methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and - user responsibilities in maintaining the security of the system, component, or service;

#### c

##### CivicActions

If the information needed to answer a question is not already included in the website’s public-facing documentation, a ticket is created to determine whether the question is sufficiently general in nature to warrant adding the answer to the website’s documentation.

##### Ilias

As a popular and well-used and maintained free and open source (FOSS) project, in the event that sought after documentation is not available on Ilias.de, it can usually be found in one of the many forums, mailing lists or Stack Exchange sites covering Ilias and its many contributed modules.

#### d

##### AWS

AWS built-in features include online documentation that is protected by AWS from unauthorized modification or deletion within AWS system.

##### CivicActions

All administrator documentation is housed in a protected Git repository. User documentation is publicly available.

##### Ilias

The Ilias.de documentation is multi-sourced on GitHub and private repositories.

#### e

##### AWS

AWS built-in features include online documentation located at http://aws.amazon.com/documentation/ that is publicly available.

##### CivicActions

As needed and approved by the CivicActions Security Office, documentation is available to appropriate personnel by granting access to the private Git repository.

##### Ilias

As the Ilias.de documentation is publicly available, there is no need to provide distribution mechanisms.

### SA-9: External Information System Services

The organization:  
 a. Requires that providers of external information system services comply with  
organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;  
 b. Defines and documents government oversight and user roles and responsibilities  
with regard to external information system services; and  
 c. Employs [Assignment: organization-defined processes, methods, and techniques]  
to monitor security control compliance by external service providers on an ongoing basis.

##### CivicActions

CivicActions does not have any dedicated interconnections between information system components within the authorization boundary and external third-party vendor information systems for the purposes of storing, processing or transmitting federal agency data.

##### Project

Project does not have any dedicated interconnections between information system components within the authorization boundary and external third-party vendor information systems for the purposes of storing, processing, or transmitting federal agency data.

Project is hosted on the AWS Cloud platform, which was approved under the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013.

### SA-12: Supply Chain Protection

The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.

##### AWS

In this architecture, initial private/public SSH keys stored in Identity and Access Management (IAM) are supplied to Amazon EC2 instances upon launch, and the public key portion is managed within the AWS Amazon EC2 service. In addition, server-side encryption is used for Amazon S3 storage and Amazon RDS databases, using key management provided by AWS for the storage buckets and Amazon RDS databases.

### SA-13: Trustworthiness

The organization:  
 a. Describes the trustworthiness required in the [Assignment: organization-defined  
information system, information system component, or information system service] supporting its critical missions/business functions; and  
 b. Implements [Assignment: organization-defined assurance overlay] to achieve  
such trustworthiness.

##### AWS

In this architecture, encryption mechanisms are employed for data at rest and in transit. For data at rest, AES-256 Server Side encryption is employed for data stored in Amazon S3, and Amazon RDS databases. For data in transit, to protect against exposure of any cleartext data transmitted deliberately (upload/download) or incidentally during interactive systems management operations, Amazon S3 object access can only be conducted over encrypted sessions via TLS; the bastion host, Amazon EC2 instances and associated security groups are configured for encrypted SSH sessions only. For web user access, the Elastic Load Balancing (ELB) employs a TLS endpoint.

AWS built-in features employ TLS for AWS Management Console sessions, AWS API calls, and AWS Command Line Interface connections.

## SA: SA

### SA-39:

##### AWS

In this architecture, the AMIs that make up the operating systems deployed on Amazon EC2 instances maintain separate execution domains/address spaces for executing processes within the customer operating environment.

AWS built-in features of the hypervisors that support the infrastructure maintain separate execution domains/address spaces for executing processes.