# SECURITY ASSESSMENT AND AUTHORIZATION

## CA-01 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES

Control description: <http://800-53.govready.com/control?id=CA-1>

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

The Department has published the Department of Education, Office of the Chief Information Officer, Handbook for Information Assurance Security Policy, Information Assurance Program (Handbook OCIO-01) and U. S. Department of Education Information Technology Security, Handbook for Information Technology Security, Certification and Accreditation Procedures (Handbook OCIO-05). Both of these publications are revised periodically. The LINCS System Security Policy (SSP) provides guidance on all aspects of security for the protection of LINCS information technology resources.

The Department will periodically review and update the SSP when there is a significant change to the regulatory, operational, or technical environment.

#### CivicActions Responsibility

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>.

#### Amazon Web Services (AWS) US-East/West control support

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

## CA-02 SECURITY ASSESSMENTS

Control description: <http://800-53.govready.com/control?id=CA-2>

Security control type: Hybrid

### Part a)

#### LINCS specific control or LINCS Responsibility

The LINCS Technology Project follows the U. S. Department of Education Information Technology Security, Handbook for Information Technology Security, Certification and Accreditation Procedures (Handbook OCIO-05) procedures. The LINCS Technology Project will conduct annual security assessments to comply with FISMA and NIST regulations. The Department will draw on NIST Special Publications 800-53A security controls to complete the assessment. All controls and sub-set security controls will be evaluated and a risk assessment will be conducted. The scope of the assessment includes:

1. Security controls and control enhancements under assessment
2. Assessment procedures to be used to determine security control effectiveness
3. Assessment environment, assessment team, and assessment roles and responsibilities

#### CivicActions Responsibility

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.

### Part b)

#### CivicActions Responsibility

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.

### Part c)

#### LINCS specific control or LINCS Responsibility

The LINCS Authorizing Official or Designated Representative will create a Security Assessment Report (SAR). A full assessment shall be conducted by an independent third party assessor at least every three years.

#### CivicActions Responsibility

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).

### Part d)

#### CivicActions Responsibility

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-03 SYSTEM INTERCONNECTIONS

Control description: <http://800-53.govready.com/control?id=CA-3>

Security control type: System Specific Control

#### CivicActions Responsibility

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

## CA-05 PLAN OF ACTION AND MILESTONES

Control description: <http://800-53.govready.com/control?id=CA-5>

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

The LINCS Technology Project follows the U.S. Department of Education Information Technology Security, Handbook for Information Technology Security, Certification and Accreditation Procedures (Handbook OCIO-05) procedures in managing POA&Ms.

#### CivicActions Responsibility

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-06 SECURITY AUTHORIZATION

Control description: <http://800-53.govready.com/control?id=CA-6>

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

The LINCS Technology Project follows the Department of Education, Office of the Chief Information Officer, Handbook for Information Assurance Security Policy, Information Assurance Program (Handbook OCIO-01) and U. S. Department of Education Information Technology Security, Handbook for Information Technology Security, Certification and Accreditation Procedures (Handbook OCIO-05) procedures. The LINCS Technology Project system received its first three-year security accreditation on March 3, 2009, and most recently received an ATO on February 5, 2016.

ATO re-assessment will be performed every three years or when there is a major change to the application, in which a senior organizational official will sign and approve the security accreditation.

## CA-07 CONTINUOUS MONITORING

Control description: <http://800-53.govready.com/control?id=CA-7>

Security control type: Hybrid

### Part a)

#### CivicActions Responsibility

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 specific control support

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.

### Part b)

#### CivicActions Responsibility

Configuration management and log analysis is 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.

#### Amazon Web Services (AWS) US-East/West control support

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.

### Part c)

#### Drupal specific control support

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.

### Part d)

#### CivicActions Responsibility

CivicActions conducts or oversees continuous system security monitoring.

#### Amazon Web Services (AWS) US-East/West control support

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.

### Part e)

#### CivicActions Responsibility

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.

### Part f)

#### CivicActions Responsibility

POA&M items are tracked by CivicActions Security though JIRA tickets with a security categorization assigned. 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.

### Part g)

#### CivicActions Responsibility

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

## CA-09 INTERNAL SYSTEM CONNECTIONS

Control description: <http://800-53.govready.com/control?id=CA-9>

Security control type: Inherited

#### Amazon Web Services (AWS) US-East/West control support

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