# LINCS System Security Plan

# NIST SP 800-53 Revision 4

## SI: System and Information Integrity

### SI-1: System And Information Integrity Policy And Procedures

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

##### AWS

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

##### CivicActions

CivicActions has developed, documented and disseminated to personnel a system and information integrity 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 Information Integrity (SI) Policy document that can be found in the CivicActions Github repository at <https://github.com/CivicActions/compliance-docs/>.

##### LINCS

System and information integrity policy and procedures for the LINCS Technology Project system are formally documented in the LINCS SSP, which provides the roles and responsibilities as it pertains to physical and environmental protection systems. The LINCS Technology Project system support staff monitors the network on a daily basis and employs up-to-date patches to protect the integrity of the system. Additional information is contained within the Department of Education, Handbook for Information Assurance Security Policy (Handbook OCIO-01. This is Agency common control. More data about implementation can be obtained from the Agency common control catalog.

### SI-2: Flaw Remediation

The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process.

##### AWS

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

##### Drupal

Drupal contains built-in security status monitoring of the core application and contributed modules.

#### a

##### CivicActions

Identification of information system security flaws are detected as early as possible by the following methods: • Vulnerability scans, as described in RA-5. • Log analysis from monitoring described in SI-4. • Service flaw notifications (CVEs, etc.) are received by CivicActions Security and passed on to CicvicActions Operations when relevant. Any security issues found are ticketed through JIRA and/or the Git issue queue. CivicActions Operations prioritizes the high findings. Changes made to correct the information system as a result of the system flaws are scheduled and coordinated through the CCB Change Request Process and appropriate approvals required from the CCB as implemented in CM-3.

#### b

##### CivicActions

CivicActions testing of the system as a result of security flaw remediation are done through a development environment though use of internal software and automated testing that ensures the system is working as intended. When a change is made by a developer, testing though a peer review is conducted as part of the Change Request process to ensure the correct analysis is completed. Then changed code is tested in an automatic test environment as described in Configuration Management Plan (CMP). Tracking of the testing is documented in JIRA and/or the Git issue queue.

#### c

##### CivicActions

CivicActions security-software updates are tested prior to place to production. The CivicActions Security framework for installation requires updates to be made within 30 days for high vulnerabilities, 90 days for moderate vulnerabilities, and 240 for low vulnerabilities. An issue ticket is created to track the any updates made to the system.

#### d

##### CivicActions

Flaw remediation is part of the CivicActions configuration management process. Any security issues found are ticketed through JIRA or the Git issue queue. CivicActions Security prioritizes the high findings within the application. Changes made to correct the system as a result of the system flaws are scheduled and coordinated through the CCB Change Request Process and appropriate approvals required from the CCB Chair as implemented in CM-3.

### SI-2(2): SI-2(2)

The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process.

##### AWS

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

##### CivicActions

The OpenSCAP and OWASP ZAP security scanners are used to perform monthly vulnerability scans of all system components and assess web application interfaces to identify any performance or security issues/flaws. Vulnerabilities and findings identified are handled and remediated in accordance with the implementation of RA-5. Reports are generated to CivicActions Security and Operations for review, analysis, and remediation.

### SI-3: Malicious Code Protection

The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

#### a

##### CivicActions

Virus scans are performed by ClamAV, a server-hosted tool protecting the application from Trojans, Viruses and other malicious cyber-threats. Real-time scans are conducted whenever files are uploaded from any external source and malicious code is blocked or quarantined when detected. All file-based traffic traversing the server is sanitized before being delivered. All input form text is validated and sanitized.

#### b

##### CivicActions

Anti-virus definitions and malicious code protection mechanisms are configured and updated automatically on a nightly basis.

#### c

##### CivicActions

CivicActions Operations receives information system security alerts, advisories and notifications in response to malicious code detection. These messages are sent to group email distribution lists to ensure all members of the team receive the proper information in a timely manner.

#### d

##### CivicActions

False positives during malicious code detection and eradication are dealt with on a case by case basis. Potential impacts on the availability of the information system are detailed in a false positive report depending on if the report is for the OS, database or web application.

### SI-4: Information System Monitoring

The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c. Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

##### AWS

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

#### a

##### CivicActions

CivicActions systems use a collection of monitoring systems, including: • ClamAV - provides signature based malware detection/quarantine • OSSEC host-based intrusion detection system (HIDS) • AIDE Advanced Intrusion Detection Environment (IDS)) • fail2ban, an intrusion prevention system (IPS) framework • SELinux - a Mandatory Access Control (MAC) IPS • auditd - a secure system audit daemon • CloudWatch - AWS monitoring and measurement system • StatusCake - website monitoring tool • OpsGenie - a slack/email/text/phone incident escalation tool

#### b

##### CivicActions

Logs from the systems described in SI-4(a) are sent to the CivicActions SIEM tool for analysis. These logs can identify unauthorized use of the information system.

#### c

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: information system monitoring. CivicActions leverages the AWS platform and a host-based intrusion detection system (HIDS) for monitoring strategically within the information system to collect organization-determined essential information and at ad hoc locations within the system; see inheritance below.

##### CivicActions

Monitoring and log collection occurs throughout the system.

#### d

##### AWS

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

##### CivicActions

The Configuration Management process, remote log gathering and SELinux MAC protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

#### e

##### AWS

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

##### CivicActions

In the event of a performance score lower than CivicActions standards, a notification is sent to CivicActions Security. CivicActions subscribes to security mailing lists in the event the monitoring activity is required based on law enforcement information, intelligence information, or other credible sources of information.

#### f

##### AWS

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

##### CivicActions

Internal legal counsel is utilized as required when system notifications indicate such action based on user and/or malicious activity. Legal counsel is engaged for any actions that may necessitate increased user monitoring, or evidence/forensic actions.

#### g

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: information system monitoring. AWS’s monitoring mechanisms provide notification including audit records, input from malicious code protection mechanisms, data from intrusion detection and prevention mechanisms, and boundary protection devices to the AWS Security Team on a daily basis.

##### CivicActions

System alerts generated by CivicActions internal monitors (StatusCake, OSSEC, ClamAV, others) are sent to the Incident Response team via OpsGenie.

### SI-5: Security Alerts, Advisories, And Directives

The organization: a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

##### Drupal

CivicActions Security and Operations receive Drupal Security Advisories on a regular basis.

##### LINCS

LINCS Technology Project representatives and system administrators receive alerts from US-CERT on a regular basis. Support personnel take appropriate action in response to relevant areas of concern.

#### 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: AWS security alerts, advisories, and directives. The AWS Insight control panel provides direct access to the monitored systems.

##### CivicActions

CivicActions Security and Operations receive the following security alerts, advisories and directives on an ongoing basis: • Mailing lists relevant to web application security • US-CERT • Technical Cyber Security Alerts • Drupal Security Advisories

#### 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: AWS security alerts, advisories, and directives. The AWS host-based intrusion detection system (HIDS) monitors the events of the system boundary.

##### CivicActions

CivicActions utilizes StatusCake for front line monitoring for real-time system status and events of the application. StatusCake can feed to the OpsGenie incident escalation system.

#### c

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: AWS security alerts, advisories, and directives.

##### CivicActions

CivicActions Security disseminates security alerts, advisories, advisories, and directives to all CivicActions internal personnel and client personnel as directed.

#### 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: AWS security alerts, advisories, and directives.

##### CivicActions

CivicActions Security is responsible for ensuring the dissemination and implementation of relevant security alerts and advisories.

### SI-7: Software, Firmware, And Information Integrity

The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: software, firmware, and information integrity.

##### CivicActions

CivicActions employ the GitHub system to monitor source code and version control ensuring system integrity and prevents unauthorized changes. The PHP-authenticator tool is perform a format check on source code prior to entering production. Per implementation of CM-3, any changes to the source code of the system requires the CCB Change Request process. A peer review as part of the Change Request process is conducted to ensure the requested change is verified prior to entering production. CivicActions employs additional integrity checks on production systems as described in SI-4.

### SI-7 (1): Integrity Checks

The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].

##### AWS

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

##### CivicActions

The integrity check implementation of SI-7 is conducted though the GitHub system and verified monthly by redeploying the system codebase from GitHub.

### SI-7 (5): Automated Response To Integrity Violations

The information system automatically [Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguards]] when integrity violations are discovered.

##### CivicActions

The system maintains an audit log of all operations including integrity violations. When an integrity violation occurs, CivicActions Operations will be alerted via email with escalations to text and phone as needed.

### SI-7 (7): Integration Of Detection And Response

The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: integration of detection and response. AWS has deployed OSSEC HIDS to all AWS Enterprise hosts which continuously monitors and alerts for software changes as they occur throughout the AWS platform.

##### CivicActions

CivicActions incident response and configuration capabilities include the detection of unauthorized changes to the system though the IR Plan and CCB Change Request process and the implementation of IR-4 and IR-5. In the event of an unauthorized security change to the system, CivicActions support would roll back to and restore from the most recent authorized database set.

### SI-10: Information Input Validation

The information system checks the validity of [Assignment: organization-defined information inputs].

##### Drupal

All Drupal form input text is subject to format verification and input validation.

### SI-11: Error Handling

The information system: a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defined personnel or roles].

#### 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: error handling.

##### Drupal

Drupal system error logs do not contain passwords, personal information, encryption keys or other sensitive information.

##### LINCS

Drupal in production operation mode does not display application errors to the user but instead displays a predefined page indication that a request cannot be handled as requested and logs all errors to the watchdog.log file.

#### 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: error handling.

##### Drupal

Drupal system error logs are only available to authenticated administrators and viewable within the administrative interface.

### SI-12: Information Handling And Retention

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: information output handling and retention.

##### CivicActions

The CivicActions organization retains all information, system-related information, incident-related information, and system output in accordance with customers’ requirements retention periods and other NIST guidance and standards, Federal policies, procedures, Federal laws and executive orders. Audit records are retained for 365 days.

##### LINCS

LINCS Technology Project representatives and systems administrators receive annual training from the Department regarding information assurance and information handling requirements. These personnel are required to operate the system and handle system data and output in accordance with legal requirements. Personnel training and system guidelines ensure that data and programs are handled appropriately.