# LINCS System Security Plan

# NIST SP 800-53 Revision 4

## MA: Maintenance

### MA-1: System Maintenance Policy And Procedures

The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system maintenance 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 maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy [Assignment: organization-defined frequency]; and 2. System maintenance 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 system maintenance 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 in the CivicActions Maintenance (MA) Policy and Procedure document that can be found in the CivicActions Github repository at <https://github.com/CivicActions/compliance-docs>.

##### LINCS

System maintenance policy and procedures are formally documented in the LINCS SSP, which provides the roles and responsibilities as it pertains to software and systems maintennance and updates. The LINCS Technology Project ensures that maintenance controls are developed, disseminated, reviewed, and updated as necessary. Physical and environmental protection is fully inherited from the AWS FedRAMP certified us-east cloud. 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.

### MA-2: Controlled Maintenance

The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.

##### AWS

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

##### LINCS

The LINCS Technology Project schedules, performs, and documents regular maintenance on the software components of all systems, including but not limited to: • Hourly automated snapshot backups • Daily disaster recovery remote backups • Daily Intrusion Detection (OSSEC) / Data Integrity Assurance (AIDE) • As needed HelpDesk support • Twice-monthly OS updates/patches

### MA-4: Nonlocal Maintenance

The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed.

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: non-local maintenance.

#### a

##### CivicActions

System maintenance is done from remote sites as there is no direct access to the server instances in the AWS cloud; this is the government-approved method of doing business. Approval, QA, and monitoring is conducted by the team performing the specific maintenance.

#### b

##### CivicActions

Remote diagnostic tools, such as OSSEC, AIDE, fail2ban and OpenSCAP are used to verify the integrity of files, perform log analysis, monitor login attempts and check for root kits and other vulnerabilies.

#### c

##### CivicActions

All nonlocal maintenance requires the same authentication requirements to perform the maintenance activities as to access the system as defined in controls AC-3 and IA-2. SSH is used to secure all communications between the remote user and the components located in the AWS cloud.

#### d

##### CivicActions

CivicActions records for nonlocal maintenance is managed through JIRA tickets and the Git issue queue as well as normal system logs. CivicActions administrator activity to the system is also logged though the implementation of the AU-2 (Audit Events) and AU-3 (Content of Audit Records).

#### e

##### CivicActions

Any session for internal maintenance activities is terminated when the user completes their session, disconnects from the system, or logs out. In addition, sessions are terminated after 15 minutes of inactivity.

### MA-5: Maintenance Personnel

The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

##### AWS

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

##### CivicActions

Maintenance on the system and applications can only be performed by personnel designated as having internal administrator privileges and responsibilities. Access rights for the internal administrators are assigned and granted access to perform their specific job responsibilities. All physical maintenance requirements are inherited from AWS.

##### LINCS

The Department maintains a list of authorized contract (CivicActions) personnel who perform maintenance and repair activities on the LINCS Technology Project system components, and only these authorized personnel may perform the maintenance. All maintenance personnel have the required personnel security elements in place.