



STATE OF ILLINOIS
OFFICE OF THE
AUDITOR GENERAL

Christopher B. Meister, Auditor General

SUMMARY REPORT DIGEST

LEGISLATIVE PRINTING UNIT

State Compliance Examination
For the Two Years Ended June 30, 2025

Release Date: October 15, 2026

FINDINGS THIS AUDIT: 3				AGING SCHEDULE OF REPEATED FINDINGS			
	New	Repeat	Total	Repeated Since	Category 1	Category 2	Category 3
Category 1:	0	0	0	2023		25-2	
Category 2:	1	2	3	2019		25-1	
Category 3:	0	0	0				
TOTAL	1	2	3				
FINDINGS LAST AUDIT: 4							

SYNOPSIS

- (25-2) The Legislative Printing Unit (Unit) did not maintain adequate controls over its commodities inventory.
- (25-3) The Unit had not implemented adequate internal controls related to cybersecurity programs, practices, and control of confidential information.

Category 1:	Findings that are material weaknesses in internal control and/or a qualification on compliance with State laws and regulations (material noncompliance).
Category 2:	Findings that are significant deficiencies in internal control and noncompliance with State laws and regulations.
Category 3:	Findings that have no internal control issues but are in noncompliance with State laws and regulations.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

INADEQUATE CONTROLS OVER COMMODITIES INVENTORY

The Unit did not maintain adequate controls over its commodities inventory.

During testing, we noted the following:

Inadequate segregation of duties over commodities

- The Unit did not have adequate segregation of duties over its commodities inventory function. One person had the ability to receive, maintain, and perform periodic inventory counts of the commodity inventories.

Physical inventory counts did not agree to the Unit's inventory records

- During forwards (list to floor) testing of the Unit's commodities inventory, we noted 7 of 29 (24%) items counted did not match the inventory records, and noted differences could not be reconciled. Differences resulted in inventory being overstated by \$690.
- During backwards (floor to list) testing of the Unit's commodities inventory, we noted 7 of 31 (23%) items counted did not match the inventory records, and noted differences could not be reconciled. Differences resulted in inventory being overstated by \$398 (Finding 2, pages 10–11).

We recommended the Unit implement procedures to maintain accurate records of its commodities inventory. Further, we recommended the Unit should implement procedures to limit one person from having the authority to perform all of the functions associated with a transaction.

Unit officials agreed

Unit officials agreed with our recommendations, noting they will prepare, update, and retain accurate commodities records. Additionally, the Unit noted it will strengthen controls over commodities processes and allow for adequate segregation of duties regarding commodities.

WEAKNESSES IN CYBERSECURITY PROGRAMS AND PRACTICES

The Unit had not implemented adequate internal controls related to cybersecurity programs, practices, and control of confidential information.

During testing, we noted the following:

Inadequate controls over cybersecurity programs and practices

- The Unit did not maintain adequate internal controls related to its cybersecurity programs and practices. Specifically, the Unit had not:
 - Maintained a computer policy or cybersecurity policy;
 - Formally adopted Legislative Information System (LIS) policies and procedures or developed their own policies for:
 - Configuration management;
 - Acceptable use;
 - Access control;
 - Security awareness and training;
 - On-boarding policies for staff and contractors;
 - Backup verification and off-site storage;
 - Reporting security violations and suspected violations;
 - Data maintenance and destruction; or,
 - Tracking control over equipment containing confidential data.

Risk assessments were not performed for the Unit's environment

- Risk Assessments were not performed during Fiscal Year 2024 or Fiscal Year 2025 by the Unit or via the LIS, for the Unit's environment. (Finding 3, pages 12–14).

We recommended the Unit:

- Maintain a computer policy or cybersecurity policy that reflects the Unit's cybersecurity roles and responsibilities;
- Either formally adopt LIS policies and procedures or develop their own policies for configuration management, acceptable use, access control, security awareness and training, on-boarding policies for staff and contractors, backup verification and off-site storage, reporting security violations and suspected violations, data maintenance and destruction, and tracking control over equipment containing confidential data; and,
- Ensure risk assessments are performed annually for the Unit's environment.

Unit officials agreed

Unit officials agreed with our recommendations, noting they will develop and maintain a cybersecurity and computer policy to better define the Unit's Information System (IS) roles and responsibilities. Additionally, the Unit noted it will perform risk assessments annually to identify weaknesses within the agency and work with LIS to formally adopt IS policies and procedures.

OTHER FINDINGS

The remaining finding pertains to inadequate controls over State property. We will review the Unit's progress towards the implementation of our recommendations in our next State compliance examination.

ACCOUNTANT'S OPINION

The accountants conducted a State compliance examination of the Unit for the two years ended June 30, 2025, as required by the Illinois State Auditing Act. The accountants stated the Unit complied, in all material respects, with the requirements described in the report.

This State compliance examination was conducted by the Office of the Auditor General's staff.

SIGNED ORIGINAL ON FILE

DENNIS M. GIBBONS
Division Director

This report is transmitted in accordance with Section 3-14 of the Illinois State Auditing Act.

SIGNED ORIGINAL ON FILE

CHRISTOPHER B. MEISTER
Auditor General

CBM:cgc