Lehigh County Pennsylvania

OFFICE OF THE CONTROLLER
Mark Pinsley MBA — COUNTY CONTROLLER
Nanton John CIA,CFE — DEPUTY CONTROLLER

TO: Final Report Distribution

FROM: Mark Pinsley, County Controller

DATE: March 2, 2026

RE: Compliance Audit – Administrative Notice 2019-01
Computer Equipment Inventory as of December 18, 2024

The Controller's office has completed an audit of compliance with Administrative Notice 2019-01. Our audit testing was based on the county computer equipment inventory listing as of December 18, 2024. Our audit report number 26-02 is attached.

The results of our audit are:

- The Office of Information Technology's (IT) management did comply, in all material respects, with the requirements of Administrative Notice 2019-01.

Lehigh County Government Center. 17 South Seventh Street. Allentown. PA 18101-2400
(610) 782-3082
FAX: (610) 871-2897
http://controller.lehighcounty.org

COUNTY OF LEHIGH, PENNSYLVANIA

COMPLIANCE TO ADMINISTRATIVE NOTICE 2019-01

Computer Equipment Inventory
Dated December 18, 2024

REPORT NO. 26-02

COUNTY OF LEHIGH, PENNSYLVANIA
COMPLIANCE TO ADMINISTRATIVE NOTICE 2019-01
COMPUTER EQUIPMENT INVENTORY AS OF DECEMBER 18, 2024

Table of Contents

COUNTY OF LEHIGH, PENNSYLVANIA
COMPLIANCE TO ADMINISTRATIVE NOTICE 2019-01
COMPUTER EQUIPMENT INVENTORY AS OF DECEMBER 18, 2024

Background

Administrative Notice 2019-01, issued on September 1, 2019, outlines computer equipment and software responsibilities assigned to the Office of Information Technology management, to department managers, and to individual users.

According to Administrative Notice 2019-01, "Information Technology will conduct an annual audit of computer equipment within all County offices which will allow for enhanced control of these resources and improve accuracy in tracking all County computer equipment. In addition to this audit, Information Technology personnel will perform random "spot checks" to assure compliance with this Administrative Notice.". As noted in prior audits, the Office of Information Technology completes these "spot checks" when items are brought in for service, or an employee contacts the Help Desk.

Other Administrative Notices referred to in 2019-01 include:

- 2004-2 Use of Computer Systems and Facilities;
- 2001-4 Reporting Missing Personal and County Property

The Office of Information Technology has also issued:

- Administrative Notice 2003-1 – Internet Policy, and
- Administrative Notice 2010-1, Technology Procurement and Project Implementation Policy.

County employees can access the above Administrative Notices on the county intranet under Forms and Documents, Administrative Notices.

The Office of Information Technology is tasked with purchasing, installing, tracking and maintaining over 8,200 technology related items, including: computers, monitors, printers, scanners, projectors and network access points. A summary of the changes in equipment counts from the last two audits are shown below.

Product Type	2021	2022	2024
Access Point	214	214	405
Firewall	5	0	4
LCDTV	23	35	89
Monitor	2,423	2,481	2,820
Printer	819	773	850
Projector/Presentation	40	42	78
Router	9	1	11
Scanner	231	249	295
Server	41	31	7
Switch	71	2	20
Tablet	323	376	446
UPS	0	0	9
Workstation	3611	2927	3249
Grand Total	7,810	7,131	8,283

Robert Kennedy, Chief Information Officer
Office of Information Technology
Lehigh County Government Center
17 South Seventh Street
Allentown, PA 18101-2400

Report on Compliance

Opinion
We have audited Office of Information Technology's compliance with Administrative Code 2019-01, applicable to Office of Information Technology's compliance requirements referred to above that are applicable to computer equipment inventory listing as of December 18, 2024.

In our opinion, Office of Information Technology complied, in all material respects, with the compliance requirements referred to above that are applicable to computer equipment inventory listing as of December 18, 2024.

Basis for Opinion
We conducted our audit of compliance in accordance with auditing standards generally accepted in the United States of America (GAAS); the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States; and Administrative Notice 2019-01. Our responsibilities under those standards are further described in the Auditor's Responsibilities for the Audit of Compliance section of our report.

We are required to be independent of the Office of Information Technology and to meet our other ethical responsibilities in accordance with the relevant ethical requirements relating to our audit. We believe the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion. Our audit does not provide a legal determination of the Office of Information Technology's compliance with the applicable compliance requirements.

Responsibilities of Management for Compliance
Management of Office of Information Technology is responsible for compliance with the requirements referred to above, and for the design, implementation, and maintenance of effective internal control over compliance with the requirements of laws, statutes, regulations, rules, and provisions of contracts or grant agreements applicable to the Office of Information Technology's government programs.

Auditor's Responsibilities for the Audit of Compliance
Our objectives are to obtain reasonable assurance about whether material noncompliance with the applicable compliance requirements occurred, whether due to fraud or error, and to express an opinion on the entity's compliance with the applicable compliance requirements based on the compliance audit. Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit conducted in accordance with GAAS, *Government Auditing Standards*, and Administrative Notice 2019-01 will always detect material noncompliance when it exists.

The risk of not detecting material noncompliance resulting from fraud is higher than for that resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control. Noncompliance with the applicable compliance requirements is considered material if there is a substantial likelihood that, individually or in the aggregate, it would influence the judgment made by a reasonable user of the report on compliance about Office of Information Technology's compliance with the requirements of the government program as a whole.

In performing an audit in accordance with GAAS, *Government Auditing Standards*, and Administrative Notice 2019-01, we:

- Exercise professional judgment and maintain professional skepticism throughout the audit.
- Identify and assess the risks of material noncompliance, whether due to fraud or error, and design and perform audit procedures responsive to those risks. Such procedures include examining, on a test basis, evidence regarding the entity's compliance with applicable compliance requirements and performing such other procedures as the auditor considered necessary in the circumstances.
- Obtain an understanding of Office of Information Technology's internal control over compliance relevant to the audit in order to design audit procedures that are appropriate in the circumstances and to test and report on internal control over compliance in accordance with Administrative Notice 2019-01, but not for the purpose of expressing an opinion on the effectiveness of Office of Information Technology's internal control over compliance. Accordingly, no such opinion is expressed.

We are required to communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and any significant deficiencies and material weaknesses in internal control over compliance that the auditor identified during the audit.

Other Matters
We noted compliance deficiencies or other management issues that are described in the accompanying "Schedule of Prior Audit Findings and Recommendations".

Report on Internal Control Over Compliance
A *deficiency in internal control over compliance* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, noncompliance on a timely basis. A *material weakness* in internal control over compliance is a deficiency, or combination of deficiencies in internal control over compliance, such that there is a reasonable possibility that material noncompliance with a compliance requirement will not be prevented, or detected and corrected, on a timely basis. A *significant deficiency in internal control over compliance* is a deficiency, or a combination of deficiencies, in internal control over compliance that is less severe than a material weakness in internal control over compliance, yet important enough to merit attention by those charged with governance.

Our consideration of internal control over compliance was for the limited purpose described in the "Auditor's Responsibilities for the Audit of Compliance" section above and was not designed to identify all deficiencies in internal control over compliance that might be material weaknesses or significant deficiencies in internal control over compliance. Given these limitations, during our audit we did not identify any deficiencies in internal control over compliance that we consider to be material weaknesses, as defined above. However, material weaknesses or significant deficiencies in internal control over compliance may exist that have not been identified.

Our audit was not designed for the purpose of expressing an opinion on the effectiveness of internal control over compliance. Accordingly, no such opinion is expressed.

Management's Response to the Audit

If provided, the Office of Information Technology's response to our audit is included in this report. We did not audit the Office of Information Technology's response and, accordingly, we do not express an opinion on it.

The purpose of this report on internal control over compliance is solely to describe the scope of our testing of internal control over compliance and the results of that testing based on Administrative Notice 2019-01. Accordingly, this report is not suitable for any other purpose.

This report is intended solely for the information and use of management; Joshua Siegel, County Executive; Phillips Armstrong, Acting County Administrator; Bethany DiMatteo, Acting Chief Fiscal Officer; and the Board of Commissioners and is not intended to be and should not be used by anyone other than these specified parties. However, this report is a matter of public record and its distribution is not limited.

Mark Pinsley
County Controller

February 20, 2026
Allentown, Pennsylvania

Audited by: Daniel Aquilino

xc: Jessica Baraket, Director of Administration
Board of Commissioners
Bethany DiMatteo, Chief Fiscal Officer
Amanda Edge, Information Technology
Robert Kennedy, Chief Information Officer
Joshua Siegel, County Executive
Ed Youwakim, Information Technology

COUNTY OF LEHIGH, PENNSYLVANIA
COMPLIANCE TO ADMINISTRATIVE NOTICE 2019-01
COMPUTER EQUIPMENT INVENTORY AS OF DECEMBER 18, 2024

Schedule of Prior Audit Findings and Recommendations
AUDIT REPORT #23-13 ISSUED JUNE 30, 2023

Departments Not Adequately Tracking Inventory

Conditions:

1. Departments often relocate, reassign, or transfer devices within the department without notifying IT and/or updating their own inventory lists. Failure to consistently monitor devices by both the department and IT, over time increases the likelihood of lost tracking. This control breakdown significantly increases the risk of loss or theft of devices.

   In our audit, we compared what was inventoried by IT to what was physically present at the department's location and found the following discrepancies:
   - 6 of 40 sampled devices were unable to be located at the 911 Center & EMS
   - 10 of 62 sampled devices were unable to be located at Cedarbrook – Fountain Hill.

2. Per Administrative Notice 2019-01, Information Technology personnel is required to perform random "spot checks" to assure compliance with this policy. Currently, random spot checks are only performed when departments seek IT's help with technical support.

Recommendations:

- To ensure effective implementation of inventory monitoring, theft prevention, and compliance with Administrative Notice 2019-01, it is crucial for management to consistently update their inventory lists and promptly notify the IT department of any relocations, reassignments, or transfers of devices. Departments should implement internal control procedures to increase monitoring and tracking efforts, such as quarterly or biannual inventory of devices where feasible.
- IT should consider adopting a spot check schedule and document on-site inventory verification of all departments. This can assist in identifying missing and misplaced IT equipment in a timely manner and facilitate their recovery. During on-site visits, departments should be reminded of their responsibilities and requirements per Administrative Notice 2019-01.

Management's Response: Management did not provide written comments in response to our report. However, as per discussions with Management, it is the intent of the Information Technology Department to follow the Administrative Notice 2019-01 and continue to perform random "spot checks" as they have done in the past. Performing checks on a schedule is not "random".

Current Status: Testing of the 911 Center and Cedarbrook – Fountain Hill during this audit showed improvement in regards to items that were unable to be located during the prior audit. Management has continued to perform annual audits of inventory items, and performs spot checks during these audits, as well as when employees call the Help Desk for assistance.