REPORT OF EXAMINATION | 2021M-192

LaFargeville Central School District

Information Technology

MARCH 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

LaFargeville Central School District

Audit Objective

Determine whether LaFargeville Central School District (District) officials established adequate information technology (IT) controls over physical IT assets and non-student network user account access.

Key Findings

District officials did not establish adequate IT controls over physical IT assets and non-student user account access to the District's network. In addition to sensitive IT control weaknesses that were communicated confidentially to officials, we found:

- 235 IT assets costing $108,462 were not recorded in the District's inventory records, and seven computers, two audio systems, one projector and 10 other electronic components that cost $9,266 could not be found.
- No physical access or environmental controls over the server room.
- Improperly managed network user accounts.
- The District's disaster recovery plan was outdated, inadequate and not tested.

Key Recommendations

- Implement procedures to properly account for physical IT assets throughout the District.
- Establish physical security and environmental controls over the server room.
- Immediately disable unneeded network user accounts and regularly review and update network user accounts for necessity and appropriateness.
- Develop and adopt a written IT contingency plan.

Except as specified in Appendix A, District officials generally agreed with our recommendations. Appendix B includes our comment on an issue raised in the District's response.

Background

The District serves the Towns of Alexandria, Clayton, Le Ray, Orleans, Pamelia and Theresa in Jefferson County. The District operates one school and is governed by an elected five-member Board of Education (Board).

The Board is responsible for managing and controlling the District's financial and educational affairs. The Superintendent of Schools is the District's chief executive officer and is responsible for the District's administration.

District officials and staff rely on the District's IT assets for Internet access, email and maintaining confidential and sensitive financial and personnel records. The District's Technology Coordinator is responsible for monitoring the network and IT assets. The Deputy Treasurer assists the Technology Coordinator in maintaining the District's inventory of physical IT assets.

Quick Facts	
Enabled Non-Student Network User Accounts	169
Students	504
Employees	159
Physical IT Assets Recorded in Inventory Records	1,330 costing $727,000

Audit Period

July 1, 2019 – June 3, 2021

Information Technology

IT assets, including IT systems and data, are valuable resources. If the IT assets are compromised, the results could range from inconvenient to catastrophic and could require extensive efforts and resources to evaluate and repair. While effective controls will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

How Should a District Maintain Its Inventory of Physical IT Assets?

The evolution of IT in the classroom has prompted large increases in school districts' investments in physical IT assets. Maintaining accurate records of IT assets allows school district officials to know what equipment a school district has, where the equipment is located and how much the equipment cost.

A board is responsible for adopting policies and procedures which are part of the internal control structure in providing criteria and guidance over a school district's IT asset inventory. School district officials should keep track of physical IT assets by maintaining a comprehensive, accurate inventory record that is periodically reviewed and updated.

A detailed inventory record should include a description of each item, including make, model and serial number; the name of the person to whom the equipment is assigned, if applicable; the physical location of the asset; and relevant purchase information including acquisition date and cost. Each item also should be immediately affixed with an identification tag and entered into a consolidated inventory record upon receipt.

Equipment should be periodically inventoried to establish its condition and to help ensure none has been misplaced or stolen. When IT assets are planned for disposal, school district officials should ensure access to these assets is physically restricted (e.g., use of gates or locks) to protect them from loss or misuse. Prior to disposal of inventory, officials must ensure that equipment is free of personal, private and sensitive information (PPSI).[1] Inventory records should be updated when assets are disposed of to ensure the records are accurate.

The evolution of IT in the classroom has prompted large increases in school districts' investment in physical IT assets.

The District Did Not Adequately Maintain Its Physical IT Asset Inventory

The District acquires IT assets through cooperative purchasing with the Jefferson-Lewis-Hamilton-Herkimer-Oneida Board of Cooperative Educational Services

1 Personal, private and sensitive information (PPSI) is any information to which unauthorized access, disclosure, modifications, destruction – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers, third parties, or other individuals or entities.

(BOCES) and through direct purchases made by the District. When an IT asset is received from BOCES, it is already tagged with a unique BOCES identification number. The Technology Coordinator adds a District tag to all IT assets that are received by the District (including those from BOCES) and the Deputy Treasurer enters the items into a database (inventory records) that is used to track the assets.

According to District policy, the District is required to tag and record the assets into its inventory records. As of May 2021, the District's inventory records had 1,330 IT assets, including computers, monitors, printers and other audio-visual and computer-related equipment. The disposal of all IT assets requires the Board's approval. IT assets purchased through BOCES also require BOCES approval before disposal.

We found that District officials did not always properly track the District's IT assets.

We found that District officials did not always properly track the District's IT assets. We selected 45 assets that cost the District $115,879 and traced them from the District's inventory records to their physical location. Although we located all 45 assets, 20 of them costing $12,131 were difficult to find because the Technology Coordinator and the Deputy Treasurer designated them in the inventory records as located throughout the building, rather than assigning the asset to a specific numbered classroom or to a staff member.

The Deputy Treasurer told us she did not list a specific location for certain IT assets such as laptops and monitors because they were used by teachers who moved the items from room to room while students remained in the classroom during the COVID-19 pandemic. When the Technology Coordinator and the Deputy Treasurer implemented this strategy due to the COVID-19 pandemic, the District's inventory records should have been updated to show the employee who was assigned the asset in order to provide greater accountability and make it easier for them to be tracked.

We also observed that the District stores a significant amount of surplus and spare computer assets (e.g., computers, laptops, monitors, and printers) in various locations such as the basement, server room and the Technology Coordinator's office. The Technology Coordinator explained that the District plans to dispose of many of these assets; however, these equipment items have not yet been cleared of PPSI. We also found that these items were not properly secured because both the basement and server room doors[2] were not locked. The Technology Coordinator told us the District contracts with a vendor to clear the PPSI from computers and other equipment that store data, on a periodic basis. However, this clearing of PPSI does not occur until the District releases the assets to the vendor for recycling and disposal. Because these IT assets

2 See the section entitled "Access to the Service Room Was Not Adequately Controlled"

were left unsecured, there is a risk the assets could be stolen or that PPSI could be compromised if an unauthorized user were able to gain access to the data. Officials subsequently have taken appropriate action to ensure that both the server room and basement doors are now locked.

We selected an additional sample of 215 spare computers and other IT assets that we observed being stored in various locations. We found that none of the 215 IT assets were recorded in the District's inventory records. According to lists showing cooperative purchases from BOCES (BOCES records[3]), these assets cost $99,196. We also attempted to trace 20 other IT assets that cost $9,266 from the BOCES records to the District's inventory records and their physical location. None of these assets, which included seven computers, seven wireless access points, three control panels, two audio systems and one projector were recorded in the District's inventory records and we could not physically locate any of them.

District officials told us that these 20 assets were likely disposed of three years ago when the District requested their last disposal. However, when we reviewed the prior disposal list that was approved by the Board at that time, we did not see any of these assets on that list. Although District policy also required approval from BOCES to dispose of IT assets, there were also no records to show that the District obtained approval from BOCES to dispose of these assets. Additionally, the District's inventory records did not reflect the date and method of disposition for these assets, which is required by Board policy. Given the lack of inventory and disposal records for these assets, officials cannot be certain that they were not lost, misused or stolen.

The District's inventory records were incomplete because officials did not have an effective process for updating the records when these IT assets were acquired from BOCES. Also, the District did not perform complete periodic physical inventories to help ensure the inventory records were accurate and the assets were on hand.

The Technology Coordinator told us that he and the Deputy Treasurer performed a partial physical inventory of IT assets in January 2021 because they suspected the District's inventory records were not complete and accurate. Prior to this, District officials had not performed a physical inventory in several years. Also, the January physical inventory only included the assets currently being used by District employees and students. It did not include surplus and spare IT assets. As a result, this physical inventory did not disclose that the 215 IT assets set for disposal were not in the inventory records. It also did not uncover the 20 missing IT assets because those assets were not recorded in the inventory records and, therefore, no attempt was made to locate them.

3 Consists of 1,161 devices totaling $725,601 as of January 2021

Without a complete and accurate inventory of computers and other IT assets, District officials cannot be assured that these assets are adequately accounted for and would be detected if lost, stolen, misused or if one of them became obsolete. Further, they do not have enough information to make informed decisions on hardware inventory. In the event of a disaster, the District would be unable to provide its insurance company with an accurate list of assets to replace.

How Should a Server Room Be Physically Controlled?

Physical security controls restrict access to physical IT assets to those who need access and help protect these resources from unauthorized access, intentional or unintentional harm, loss or impairment. Server rooms should be locked, with only necessary IT personnel having access to the room.

Additionally, environmental controls such as a cooling system and temperature controls, smoke detectors, fire alarms and extinguishers and protection from water damage should be used to mitigate the consequences of environmental hazards and help prevent the equipment from being destroyed.

Access to the Server Room Was Not Adequately Controlled

The District's server room is located within a technology classroom. When we performed an initial walk-through of the server room in May 2021, we observed that the door of the room was left open. District officials said the cooling system had been out of service since September 2020, so they had been leaving the door open to maintain a cooler temperature. Because the door was not locked, the servers were accessible by anyone inside the school building. The system was repaired in late June 2021 and we subsequently observed that the door was locked. While there is no fire suppression system in the room, it does have a smoke detector.

These servers house student data applications and other personal information about staff or students. If access to the servers is not controlled, the risk increases that unauthorized access to the students' and staff's personal information could be obtained, and records could be altered or destroyed or the servers could be damaged. This could result in the District expending significant resources in both time and money to correct/repair data and equipment. Furthermore, a lack of fire suppression system in this area leaves the District with an increased risk of not being able to respond to a fire should one occur in the server room.

How Should Officials Properly Manage Network User Accounts?

Network user accounts enable networks, connected computers and certain applications to recognize specific users and processes, allow network administrators to grant appropriate user permissions and provide user

accountability by affiliating network user accounts with specific users and processes. Network user accounts are potential entry points for attackers because, if compromised, they could be used to misuse, modify, corrupt or delete data stored on the network.

School district officials are responsible for restricting network user access to only those network resources and data needed for learning and to complete job duties and responsibilities. This helps ensure data and IT assets are protected from unauthorized use and/or modification. A school district should have written procedures for granting, changing and removing user access to the network.

To minimize the risk of unauthorized access, officials should actively manage network user accounts, including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized. When network user accounts are no longer needed, they should be disabled in a timely manner.

Generic accounts are not linked to individual users and may be needed for certain network services or applications to run properly. For example, generic accounts can be created and used for automated backup or testing processes, training purposes or generic email accounts, such as a service help desk account. Officials should routinely evaluate generic network user accounts and disable those that are not related to a current school district or system need.

Generally, a network administrative account has permissions to monitor and control a network, connected computers and certain applications with the ability to add new users and change users' passwords and permissions. A user with administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes.

Additionally, any program that a user with network administrative permissions runs may inherently run with the same permissions. For example, if malicious software (malware) installed itself on a computer, it could run at a higher privilege under a user account with administrative permissions, which could result in a greater risk of network or computer compromise and/or data loss. Therefore, it is especially important for officials to regularly review administrative accounts and promptly disable them when they are no longer needed.

Cybersecurity risks should be treated as any other hazard a school district may encounter along the way. School district officials should identify the risks, reduce their vulnerabilities and plan for contingencies. This requires an investment of time and resources and a collaborative work environment among the superintendent, the board and the IT department.

A school district should have written procedures for granting, changing and removing user access to the network.

Officials Did Not Properly Manage Network User Accounts

District officials need to improve the management of network user accounts. The District did not have written procedures for granting, changing and removing user access and permissions to the network. Also, we found no established procedures to regularly review the network user accounts to ensure they were needed or written checklists to help ensure access is granted and revoked as appropriate.

With the assistance of the Technology Coordinator, we reviewed all 169 non-student network user accounts to determine the purpose and necessity of each account. We found that 52 of the 169 network user accounts (31 percent) were unneeded. Most of these 52 accounts had not been used for an extended period and the Technology Coordinator agreed that they are no longer needed. Of the 52 unneeded accounts, we found:

- 48 had not been used in over six months; of the 48 accounts, 13 have not been used since 2016 and 13 have never been used,
- 10 had administrative permissions, and
- 30 were generic accounts.

The Technology Coordinator told us that some of these unneeded network user accounts existed because they were used for temporary purposes and never deleted. He also said, due to his work priorities, he has not had the time to review and evaluate all network user accounts for appropriateness and disable those that are no longer needed.

Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, possibly could be used to inappropriately access and view personal information. When network user accounts are not used or monitored, compromised accounts may not be detected timely. The compromise of a network user account with administrative permissions could cause greater damage than the compromise of a lesser-privileged account because administrative accounts have full control over the network. Also, when a District has many network user accounts that must be managed and reviewed, unneeded accounts may make it more difficult to manage network access.

We found that 52 of the 169 network user accounts (31 percent) were unneeded.

What Should an IT Contingency Plan Include?

IT contingency planning refers to the plans, policies, procedures and technical measures that enable the recovery of IT operations after an unexpected incident, such as restoring necessary network operations and replacing or recovering high priority IT assets. It involves analyzing business processes, focusing on minimizing the resulting damage when a disruption or disaster occurs and identifying roles of key individuals and necessary precautions to take to maintain or quickly resume operations.

As part of the contingency planning process and to minimize the risk of data loss or suffering a serious interruption of services, officials should establish a written IT contingency plan that includes guidance on disaster recovery. The plan should address the potential for sudden, unplanned catastrophic events (e.g., inadvertent employee action, ransomware or other malware infection, flood or fire) that could compromise the network and the availability or integrity of the IT system and data. This is particularly important given the ongoing and increasingly sophisticated threat of ransomware attacks.

Typically, an IT contingency plan should address the following key components:

- Roles and responsibilities of key personnel,
- Identifying and prioritizing critical business processes and services,
- Communication protocols with outside parties,
- Technical details concerning how systems and data will be restored,
- Resource requirements necessary to implement the plan,
- Detailed backup procedures, and
- Details concerning how the plan will be periodically tested.

The Disaster Recovery Plan Was Inadequate, Outdated and Not Tested

Although the District does have a written disaster recovery plan (DRP), it was outdated (last updated in 2012), and we found the plan to be inadequate because it did not include all necessary key components of an IT contingency plan. The DRP included one key component which states that all of the District's financial, cafeteria and student data is backed up at the Mohawk Regional Information Center (MORIC) and that the District will call when requesting restoration of the data. It also stated that the District will call MORIC for replacement hardware.

The District is relying on MORIC to perform all backup and restoration of data and the DRP does not include what should be done at the District level such as testing the retrieval of data, verifying the integrity of the backups and the frequency, scope and method of backups. In addition, while the DRP briefly mentions hardware, it does not categorize mission-critical applications or services, nor does it categorize other priority assets. Furthermore, the DRP does not describe the types of threats to the IT system, and it does not contain any detailed technical procedures concerning how systems and data will be restored.

We also found District officials do not periodically review, update or test the existing DRP to ensure its effectiveness. While key personnel who are expected to execute the DRP were provided with a copy of the plan, there is no training

provided to them to ensure that they understand their role in the event of a disaster. The DRP should address the remaining key components to better prepare the District for any potential disruption or disaster.

What Do We Recommend?

The Board and District officials should:

1. Develop and adopt a written IT contingency plan that provides guidance on how the District will recover its critical IT operations in the event of an unexpected incident.
2. Distribute the IT contingency plan to all responsible parties and ensure that it is periodically tested and updated as needed.
3. Ensure that staff are provided IT contingency plan training.

The Technology Coordinator and District officials should:

4. Ensure the District's inventory records include the detail necessary to adequately track and locate a hardware item, including acquisition date, building location, the date and method of disposition, and if applicable, identify room number or employee it was assigned to.
5. Ensure surplus and spare IT equipment is properly secured.
6. Establish written procedures to ensure assets purchased through BOCES are recorded in the inventory records and asset dispositions are properly approved and documented in the records.
7. Update the inventory records to track the 215 IT assets that are not currently in the records.
8. Investigate the 20 missing items to determine whether they were disposed of earlier and if not, attempt to locate them.
9. Ensure that periodic and complete physical inventory counts are conducted and compared to inventory records and take appropriate action to follow-up on differences.
10. Establish physical security and environmental controls over the server room to protect IT systems and resources. Such controls include limiting access to the room, maintaining fire suppression equipment, and ensuring the cooling system and temperature control is running properly.
11. Immediately disable unneeded network user accounts and regularly review and update network user accounts for necessity and appropriateness.

12. Develop written procedures for granting, changing and removing network user access and regularly reviewing the accounts to ensure they are needed.

Appendix A: Response From District Officials

LaFargeville
Central School District

P.O. BOX 138, 20414 SUNRISE AVE. • LAFARGEVILLE, NY 13656
PHONE: 315-658-2241 • FAX 315-658-4223

TRAVIS HOOVER
Superintendent

JAYCEE WELSH
Elementary Principal/CSE Chair

STEVEN NEWCOMBE
Secondary Principal

BOARD OF EDUCATION
Sheryl Wilson, President
Jada Walldroff, Vice Pres.
Matthew W. Duffany
Mary Ford-Waterman
Matthew R. Timerman

Michelle Papin
Clerk

NICOLE PARLIAMENT
Business Manager

Equal Opportunity
Affirmative Action Employer

February 28, 2022

Chief Examiner
Office of the State Comptroller
State Office Building
Room 409
333 E. Washington Street
Syracuse, New York 13202-1428

LaFargeville Central School District
Information Technology Audit
2021M-192

Dear Chief Examiner:

The LaFargeville Central School District is in receipt of the draft Report of Examination for the Information Technology Audit 2021M-192. On behalf of the Board of Education and District Administration, we appreciate the opportunity to respond to the findings of this report.

We agree with the audit findings in the report and plan to have all components of our action plan completed by our March 14 Board of Education Meeting. We would like to point out the following important items:

1. A technology audit was performed only after finding no areas of concern within our budget office procedures.
2. There was no wrong doing by any employee found within this audit and all recommendations are preventative in nature.

See Note 1 Page 12

Respectfully,

Travis Hoover
Superintendent

Appendix B: OSC Comment on the District's Response

Note 1

While we did perform a risk assessment of various District operations prior to selecting our audit objective, we did not perform an in-depth evaluation of the District's budget office procedures. Therefore, we did not draw any conclusions concerning those procedures.

Appendix C: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the District's IT policies and procedures and interviewed District and BOCES officials to gain an understanding of IT operations, specifically those related to maintaining IT asset inventory records; security of the server room; the granting, modification and revocation of network user accounts; and IT contingency planning.
- We used our professional judgment to select 45 IT assets from the District's inventory records to determine whether the assets were tracked properly and located within the District. We selected high dollar value IT assets and assets frequently used that could easily be stolen or could have PPSI stored on them.
- We also selected 215 spare and surplus IT assets stored in various locations such as the basement, server room and the Technology Coordinator's office to determine whether those assets were recorded in BOCES records and also in the District's inventory records. We also selected 20 assets from BOCES records to determine whether they were located in the District and included in the District's inventory records.
- We ran a computerized audit script on the District's domain controller[4] on June 3, 2021. We analyzed the data produced to assess network user accounts, permissions assigned to the accounts and the related security settings applied to the accounts.
- We followed-up with District officials on possible unneeded network user accounts.
- We performed a walk-through of the District's facilities to identify any weaknesses in the physical access security and environmental controls over IT systems and servers to determine whether the District established adequate security controls over these assets.

Our audit also examined the adequacy of certain IT controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to District officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective.

4 The domain controller is a server that controls or manages access to network resources.

We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report,* which you received with the draft audit report. The CAP should be posted on the District's website for public review.

Appendix D: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/local-government

Local Government and School Accountability Help Line: (866) 321-8503

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner

State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428

Tel (315) 428-4192 • Fax (315) 426-2119 • Email: Muni-Syracuse@osc.ny.gov

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller