DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2017M-146

Florida Union Free School District

Information Technology

NOVEMBER 2017

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

Contents

Report Highlights

Florida Union Free School District

Audit Objective

Determine whether internal controls over information technology (IT) are appropriately designed and operating effectively.

Key Findings

- Employees do not comply with the District's acceptable use policy.
- Controls over personal, private and sensitive information (PPSI) collected, processed, transmitted and stored have not been developed.
- The District does not have service level agreements for services provided by OUBOCES and MHRIC which could lead to confusion over roles and responsibilities of each party.

Key Recommendations

- Review and monitor employees' computer use to ensure compliance with the District's acceptable use policy.
- Inventory, classify and develop controls over PPSI maintained and collected by the District.
- Ensure that all IT services are provided based on a formal service level agreement.
- Address the IT recommendations communicated confidentially.

District officials generally agreed with our recommendations and indicated they planned to take corrective action. Appendix B includes our comment on an issue raised in the District's response letter.

Background

The Florida Union Free School District (District) is located in the Towns of Goshen and Warwick, in Orange County.

The District contracts with Orange-Ulster Board of Cooperative Educational Services (OUBOCES) and the Mid-Hudson Regional Information Center (MHRIC) for IT services.

The District is governed by the Board of Education (Board) which is composed of five elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

Quick Facts	
Number of Schools	2
Estimated Number of Students	824
Number of Employees	216

Audit Period

July 1, 2015 through June 9, 2017

Information Technology Governance

The District uses IT to initiate, process, record and report transactions. It also relies on its IT systems for Internet access, email and maintaining financial, personnel and student records. Therefore, the IT systems and data are valuable District resources. If IT systems are compromised, the results could range from an inconvenience to a catastrophe and could require extensive effort and resources to evaluate and repair.

What is Effective Information Technology Governance?

Effective governance over IT operations includes:

- Cybersecurity training to ensure employees understand IT security policies and procedures and their roles and responsibilities related to IT security.
- Web content filters with monitoring capabilities to ensure compliance with the acceptable use policy.
- Guidelines for collecting, storing, classifying, accessing and disposing of personal, private and sensitive information (PPSI) encountered during the normal course of business.
- Service level agreements (SLAs) that identify the parties to IT service contracts and the roles and responsibilities of contractors.

District Employees and Staff Are Not Provided Cybersecurity Training

The IT security community identifies people as the weakest link in the chain to secure data and systems. District officials cannot protect the confidentiality, integrity and availability of the District's data and computer systems without ensuring that the people who use and manage IT understand the District's IT security policies and procedures and their roles and responsibilities related to IT security.

The District does not provide or require employees to attend any formal cybersecurity awareness training. Such training should center on emerging trends in information theft and other social engineering reminders; limiting the type of PPSI collected, accessed or displayed to that which is essential for the function being performed; malicious software; virus protection; the dangers of downloading files and programs from the Internet; passwords; Wi-Fi security; or how to respond if a virus or an information security breach is detected.

Although District officials told us that training was provided to staff at the start of each school year, the training was focused on school policies and procedures such as shutting down computers, locking workstations and reminding employees to not share passwords. In addition, District officials did not take attendance and were unable to provide evidence that all staff received and were aware of the training.

As a result, District employees are more likely to be unaware of a situation which could compromise District IT assets and security which places the District's IT system at greater risk.

Employees Did Not Comply With the Acceptable Use Policy

Internet browsing increases the likelihood that users will be exposed to some form of malicious software that may compromise data confidentiality. The District's acceptable use policy prohibits the use of District computers for non-educational or illegal purposes.

We reviewed a sample of eight computers which included all Business Office staff with access to financial software and two employees from the Special Education Department with access to student records. Our review of District equipment identified the following types of inappropriate use:

- Vacation rental and airfare purchases.
- Concert venues.
- Social Media (Facebook, Twitter, Pinterest, LinkedIn).
- Shopping (shoes, makeup, clothing, etc.).

We also reviewed employee acknowledgement agreements for the employees tested to determine if they received and were aware of the District's acceptable use policy. Seven employees had acknowledgement forms on file, one employee was missing a signed acknowledgement form from the employee handbook, but had an electronic work history report indicating that the employee handbook was reviewed.

District officials did not monitor employee Internet use and the District's web filter software does not allow officials to review the full content strings of uniform resource identifiers (URLs) for websites visited by employees. Therefore, District officials are not be able to monitor compliance with the acceptable use policy. As a result, inappropriate computer use puts District IT assets at higher risk of exposure to loss, misuse or damage.

PPSI Data Is Not Properly Managed

The District collects and stores data received and produced from its operations, including PPSI, which includes confidential student and employee data. Classifying the PPSI data can help identify the type of security controls appropriate for safeguarding that data.

District officials have not established a classification scheme for PPSI. Therefore, officials have not assigned a security level to the data. District officials do not know what PPSI is retained, where it is located, who has access and how it is disposed of. Further, there are multiple “owners” of the data, each individually responsible for security over various sources of data, who do not have an understanding of the internal controls over IT. District officials excluded the IT Department from developing controls relating to how PPSI is disposed of, who has access rights to it or to identify where the information is stored.

District officials were unable to comment on the previous administration’s past decisions regarding IT. District officials are taking steps to include the IT Department in managing PPSI.

Without the involvement of qualified IT personnel, District officials cannot have adequate assurance that PPSI is effectively and adequately protected from unauthorized access.

No Service Level Agreements for IT Services

In order to protect the District and to avoid potential misunderstandings, there should be a written agreement between the District and the IT service providers - Orange-Ulster Board of Cooperative Educational Services (OUBOCES) and Mid-Hudson Regional Information Center (MHRIC). Such agreements should identify the District’s needs and expectations and should specify the level of service to be provided by the contractors/vendors. The components of an SLA can include identification of the parties to the contract, term/duration of agreement, scope/subject, limitations (what, if anything, is excluded), service level objectives, roles and responsibilities, nonperformance impact, pricing and billing, security procedures, review/update and approvals. Such agreements should establish a mutual understanding of the nature and required level of service to be provided. It is important to have SLAs so parties understand their roles and responsibilities for IT services.

The District does not have any SLAs for IT services that it receives. The Board has not negotiated a formal agreement with the IT service provides identifying the specific services to be provided or the vendor’s responsibilities because it has not considered the benefits of having such agreements. The District does not have a written SLA with OUBOCES or MHRIC, for student information systems, web filtering and data warehousing. Instead, the District chooses its services in a piecemeal fashion by selecting certain services needed for operations. However, the services provided are not are not explained in detail. The lack of detail could lead to confusion in the roles and responsibilities of each party.

What Do We Recommend?

District officials should:

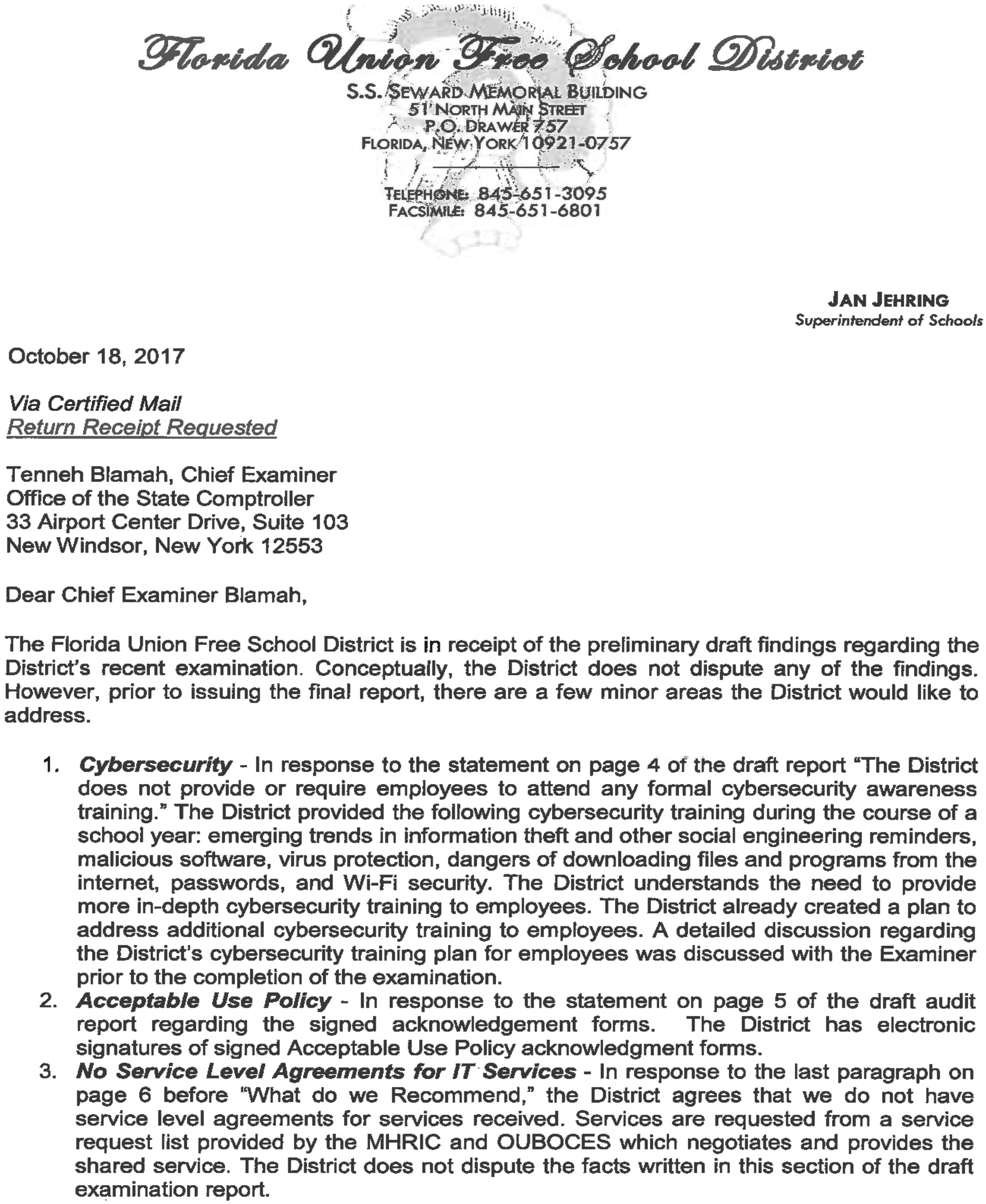
1. Ensure that employees receive formal IT cybersecurity training on an on-going basis that reflects current risks identified by the IT community.

2. Review and monitor employees' computer use to ensure compliance with the District's acceptable use policy.

3. Inventory and classify PPSI and include IT Department staff when developing controls over PPSI collected.

4. Have a SLA for any IT services provided by third-party vendors to ensure the District has an understanding of all services being provided and the roles and responsibilities of all parties.

Appendix A: Response From District Officials



Florida Union Free School District

S.S. Seward Memorial Building
51 North Main Street
P.O. Drawer 757
Florida, New York 10921-0757

Telephone: 845-651-3095
Facsimile: 845-651-6801

Jan Jehring
Superintendent of Schools

October 18, 2017

Via Certified Mail
Return Receipt Requested

Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553

Dear Chief Examiner Blamah,

The Florida Union Free School District is in receipt of the preliminary draft findings regarding the District's recent examination. Conceptually, the District does not dispute any of the findings. However, prior to issuing the final report, there are a few minor areas the District would like to address.

1. ***Cybersecurity*** - In response to the statement on page 4 of the draft report "The District does not provide or require employees to attend any formal cybersecurity awareness training." The District provided the following cybersecurity training during the course of a school year: emerging trends in information theft and other social engineering reminders, malicious software, virus protection, dangers of downloading files and programs from the internet, passwords, and Wi-Fi security. The District understands the need to provide more in-depth cybersecurity training to employees. The District already created a plan to address additional cybersecurity training to employees. A detailed discussion regarding the District's cybersecurity training plan for employees was discussed with the Examiner prior to the completion of the examination.
2. ***Acceptable Use Policy*** - In response to the statement on page 5 of the draft audit report regarding the signed acknowledgement forms. The District has electronic signatures of signed Acceptable Use Policy acknowledgment forms.
3. ***No Service Level Agreements for IT Services*** - In response to the last paragraph on page 6 before "What do we Recommend," the District agrees that we do not have service level agreements for services received. Services are requested from a service request list provided by the MHRIC and OUBOCES which negotiates and provides the shared service. The District does not dispute the facts written in this section of the draft examination report.

See
Note 1
Page 8

The above information was shared with the Examiners during the District's exit conference. Examiners were professional and provided insight and answers to questions. The District will benefit from this thorough examination. The District expects to improve operations based on key findings and recommendations outlined in the draft audit report. Responses to each of the findings will be forthcoming in the District's Corrective Action Plan.

Sincerely,

Jan Jehring
Superintendent of Schools
845-651-3095, extension 40010

Appendix B: OSC Comment on the District's Response

Note 1

Although the District requires employees to acknowledge the acceptable use policy when logging on, it also requires employees to sign a form acknowledging receipt of the employee handbook and agreeing to the policies, including the acceptable use policy. The District did not have a signed form for one employee that we reviewed.

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, we performed the following audit procedures:

- We reviewed Board minutes for resolutions for IT matters and reviewed written Board policies to determine the number and scope of policies officially adopted.
- We interviewed District officials and employees to obtain an understanding of District IT operations.
- We reviewed District records for any IT-related policies and procedures.
- We interviewed District employees to determine what safeguards were in place to protect sensitive data and financial assets.
- We reviewed records for eight employees judgmentally selected based on access privileges to sensitive data and/or software.
- We judgmentally selected a sample of eight computers based on access privileges to sensitive data and/or software and reviewed Internet browsing histories for personal and high-risk activities.
- We analyzed the web browsing history for our sample to identify Internet use and pages that disclosed PPSI.
- We reviewed service-level agreements with the District and vendors to determine the scope of services, reporting requirements, performance indicators and security procedures to be provided to the District.

Our audit also examined the adequacy of certain information technology 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 GAGAS (generally accepted government auditing standards). 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. 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.

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 2116-1(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 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. We encourage the Board to make the CAP available for public review in the Clerk's office.

Appendix D: Resources and Services

Regional Office Directory

http://www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas

http://www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems

http://www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management

http://www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans

http://www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders

http://www.osc.state.ny.us/localgov/lgli/pdf/cybersecurityguide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller

http://www.osc.state.ny.us/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers

http://www.osc.state.ny.us/localgov/researchpubs/index.htm

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics

http://www.osc.state.ny.us/localgov/training/index.htm

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.state.ny.us

www.osc.state.ny.us/localgov

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

NEWBURGH REGIONAL OFFICE –Tenneh Blamah, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel: (845) 567-0858 • Fax: Fax (845) 567-0080 • Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties

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