DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2022M-67

Union Springs Central School District

Safeguarding of Personal, Private and Sensitive Information on Mobile Computing Devices

SEPTEMBER 2022

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

Contents

Report Highlights

Union Springs Central School District

Audit Objective

Determine whether Union Springs Central School District (District) officials established adequate controls to safeguard personal, private and sensitive information (PPSI) on mobile computing devices (MCDs).

Key Findings

District officials did not adequately safeguard MCDs to help prevent unauthorized access to PPSI. In addition to sensitive information technology (IT) control weaknesses that were communicated confidentially to officials, we found:

- District officials did not establish sufficient procedures, such as establishing a District-wide data classification matrix and inventorying PPSI in their possession, to help ensure the proper safeguarding of PPSI on MCDs.
- Fourteen of the 20 District-owned MCDs we examined contained PPSI that was not adequately safeguarded.

Key Recommendations

District officials and IT staff should:

- Develop comprehensive written procedures to help ensure PPSI on MCDs is adequately protected, which outline proper access, transmission, storage and use of PPSI.
- Establish a data classification matrix that assigns the appropriate security level to each type of data, then conduct an inventory of PPSI stored on electronic devices, and ensure this list is updated on an ongoing basis.

District officials generally agreed with our recommendations and indicated they plan to initiate corrective action.

Background

The District serves the City of Auburn and Towns of Aurelius, Fleming, Ledyard, Scipio and Springport in Cayuga County.

The District is governed by an elected nine-member Board of Education (Board). 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 chief executive officer and is responsible, along with other administrative staff, for day-to-day management under the Board's direction.

The District uses the Central New York Regional Information Center (CNYRIC) for IT services, including support for data privacy and security management. In July 2020 the Board appointed a Chief Technology Officer (CTO) to manage the District's IT environment. The Assistant Superintendent and CTO are appointed as the District's Data Privacy Officers.

Quick Facts	
2021-22 IT Budget	$1.1 million
Staff MCDs	115
Staff	152

Audit Period

July 1, 2020 – February 22, 2022

Safeguarding of Personal, Private and Sensitive Information on Mobile Computing Devices

District officials and staff rely on the District's IT assets for maintaining confidential and sensitive financial and personnel records, email and Internet access. The District relies on MCDs for maintaining financial, personnel and student records, much of which contain PPSI. PPSI is any information to which unauthorized access, disclosure, modification, destruction or use – 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.

District-owned MCDs include laptops and smartphones which function like a personal computer while providing the convenience of portability. The District provides MCDs to certain employees for business purposes in order to facilitate a flexible work environment. For example, these MCDs are used by District officials during non-school hours, while telecommuting or while away from the office. MCDs often provide access to the employees' own work-related data and applications, including email, as well as to protected PPSI that resides in District information systems. Furthermore, District officials allow staff to access their email using personal devices.

Effective policies and procedures for protecting PPSI address various aspects of securing confidential data and limiting access to it.

How Should School District Officials Safeguard MCDs To Help Prevent Unauthorized Access to PPSI?

School district officials are responsible for ensuring that PPSI is properly safeguarded and is used only for business purposes. To fulfill this responsibility, it is essential for the school board to adopt comprehensive written IT security policies to help protect PPSI that is accessed and stored on MCDs. Furthermore, it is the responsibility of school district administrators and IT staff to ensure that the school board's directives are met and that procedures are in place and communicated to staff members who use MCDs. It is also important that school district officials know about all the types of data they possess, access and maintain on MCDs so they can make informed decisions about setting appropriate security levels. To do this, school district officials should maintain an inventory of data stored on their MCDs and parts of the network accessible from MCDs to account for the PPSI they maintain.

Effective policies and procedures for protecting PPSI address various aspects of securing confidential data and limiting access to it. In addition, the school district's policies should define how non-school district MCDs can safely access school district information without jeopardizing PPSI.

As a best practice, all data should be classified and labeled in a consistent manner to help ensure confidentiality, integrity and availability. The data classification process assigns a level of risk to various types of information, which helps management make appropriate decisions about the level of security the data requires. Therefore, it is important that school district officials classify information in a consistent manner to determine the level of security each type of data needs and conduct an inventory of PPSI stored on their devices and network to account for the confidential data maintained. School district officials should update the classification and inventory list annually to reflect any changes. In the event of a data breach, the proper classification and inventorying of PPSI allows school district officials to determine the extent of unauthorized access and take appropriate action.

District Officials Did Not Adequately Safeguard MCDs To Help Prevent Unauthorized Access to PPSI

Officials developed and the Board adopted policies that establish the Board's intent to protect the District's sensitive data by following applicable laws and regulations for handling and storing data. The policies stated that the District will use the National Institute for Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity. However, District administrators and IT staff did not develop specific procedures in accordance with the Board's policy regarding NIST standards, to help protect sensitive data accessed and stored on MCDs from exposure and unauthorized access.

District administrators and IT staff did not develop specific procedures in accordance with the Board's policy regarding NIST standards. …

District officials and staff use MCDs to access or download data, including PPSI, for business purposes. However, given that these portable devices can be lost or stolen, not establishing proper controls to secure these devices increases the risk that unauthorized persons could access and misuse PPSI from a District-owned MCD.

As a result of the lack of comprehensive procedures, we examined for the presence of PPSI on District-owned staff MCDs. School districts typically possess sensitive data such as student information, health records, personal identifying information and bank account information. We examined the hard drives of 20 MCDs and found that 14 (70 percent) contained at least one form of PPSI, with some MCDs having multiple forms of stored PPSI.

It is the responsibility of District officials to determine whether an MCD is the best medium on which to store such information. If such a determination is made, then District officials are responsible for ensuring that adequate safeguards are established, communicated and enforced to help prevent unauthorized access to this information.

Additionally, officials did not ensure they had proper procedures in place to restrict email access to read-only by non-District MCDs (e.g., personal computing devices, smartphones). Officials told us that staff could access their school email on personal devices via a web application; however, District officials had not enabled security settings to prevent staff from downloading and saving sensitive information to personal devices.

Furthermore, officials had not developed a District-wide data classification matrix because they were unaware of what one was or why it was important. As a result, officials had not inventoried the PPSI in their possession and therefore do not know the extent to which it resides on District devices.

Written procedures with clear instructions for staff to follow help ensure that PPSI is not acquired by a person without valid authorization. When officials do not develop and implement comprehensive procedures for these key areas, communicate them to applicable staff and continually monitor and update them as necessary, the risk that unauthorized users could access and misuse confidential data without detection is significantly increased.

Furthermore, without classifying data, and setting appropriate security levels for PPSI, there is an increased risk that PPSI could be inadvertently exposed to unauthorized users. In addition, lack of information about the types and extent of data the District maintains can hamper efforts to properly notify affected parties in the event of a breach.

…[L]ack of information about the types and extent of data the District maintains can hamper efforts to properly notify affected parties in the event of a breach.

What Do We Recommend?

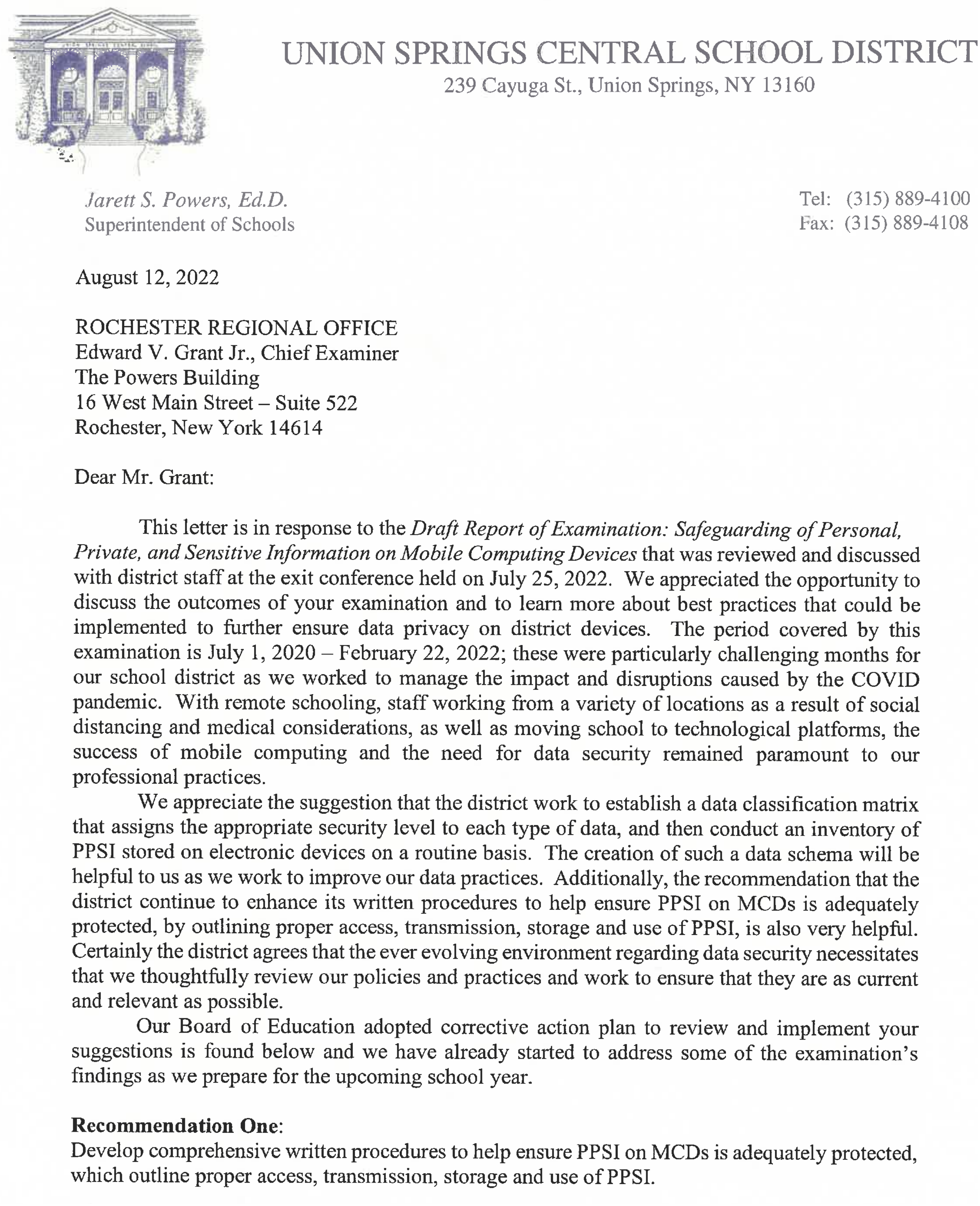
District administrators and IT staff should:

1. Develop written procedures to help ensure PPSI is adequately protected, which outline proper access, transmission, storage and use of PPSI on MCDs.

2. Ensure appropriate security settings are implemented when accessing email using personal devices.

3. Establish a data classification inventory of information the District maintains and assign the appropriate security level to each type of data, then conduct an inventory of PPSI stored to account for the confidential data maintained and ensure this inventory list is updated on an ongoing basis.

Appendix A: Response From District Officials



UNION SPRINGS CENTRAL SCHOOL DISTRICT
239 Cayuga St., Union Springs, NY 13160

Jarett S. Powers, Ed.D.
Superintendent of Schools

Tel: (315) 889-4100
Fax: (315) 889-4108

August 12, 2022

ROCHESTER REGIONAL OFFICE
Edward V. Grant Jr., Chief Examiner
The Powers Building
16 West Main Street – Suite 522
Rochester, New York 14614

Dear Mr. Grant:

This letter is in response to the *Draft Report of Examination: Safeguarding of Personal, Private, and Sensitive Information on Mobile Computing Devices* that was reviewed and discussed with district staff at the exit conference held on July 25, 2022. We appreciated the opportunity to discuss the outcomes of your examination and to learn more about best practices that could be implemented to further ensure data privacy on district devices. The period covered by this examination is July 1, 2020 – February 22, 2022; these were particularly challenging months for our school district as we worked to manage the impact and disruptions caused by the COVID pandemic. With remote schooling, staff working from a variety of locations as a result of social distancing and medical considerations, as well as moving school to technological platforms, the success of mobile computing and the need for data security remained paramount to our professional practices.

We appreciate the suggestion that the district work to establish a data classification matrix that assigns the appropriate security level to each type of data, and then conduct an inventory of PPSI stored on electronic devices on a routine basis. The creation of such a data schema will be helpful to us as we work to improve our data practices. Additionally, the recommendation that the district continue to enhance its written procedures to help ensure PPSI on MCDs is adequately protected, by outlining proper access, transmission, storage and use of PPSI, is also very helpful. Certainly the district agrees that the ever evolving environment regarding data security necessitates that we thoughtfully review our policies and practices and work to ensure that they are as current and relevant as possible.

Our Board of Education adopted corrective action plan to review and implement your suggestions is found below and we have already started to address some of the examination's findings as we prepare for the upcoming school year.

Recommendation One:
Develop comprehensive written procedures to help ensure PPSI on MCDs is adequately protected, which outline proper access, transmission, storage and use of PPSI.

Implementation Plan of Action:
The Union Springs Central School District will continue to refine its policies and procedures to help ensure PPSI on MCDs is adequately protected. The district will develop procedures that more explicitly outline the proper access, transmission, storage and use of PPSI within the school district.

Timeline:
This will be completed by the conclusion of the 2022-2023 school year.

Person Responsible for Implementation:
Board of Education, Superintendent, Director of Operations

Recommendation Two:
Establish a data classification matrix that assigns the appropriate security level to each type of data, then conduct an inventory of PPSI stored on electronic devices, and ensure this list is updated on an ongoing basis.

Implementation Plan of Action:
The Union Springs Central School District will also work to devise and implement a data classification matrix that assigns the appropriate security level to each type of data maintained by the district, as well as conduct an inventory of PPSI stored on district electronic devices, and ensure this data list is updated on an ongoing basis.

Timeline: This will be completed by the conclusion of the 2022-2023 school year.

Person Responsible for Implementation:
Superintendent of Schools, Director of Operations

Thank you for your field staff's energy and thoughtful feedback concerning our district's data security on mobile computing devices. Your team's willingness to engage with us to help us improve our practices is much appreciated.

Respectfully,

Jarett Powers, Ed.D.
Superintendent of Schools

Appendix B: 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 interviewed District officials and staff and reviewed relevant IT policies, regulations, and procedures, as well as security controls in place to gain an understanding of the District's IT environment.
- On February 9, 2022 and February 10, 2022, we reviewed a sample of 20 District-owned MCDs to determine whether PPSI was present on the local hard drive. We selected our sample by obtaining a list of District staff who were issued an MCD and judgmentally selected 11 staff based on their access to PPSI and randomly selected an additional nine staff using a random number generator and selecting two staff each from the elementary, middle and high school, and three staff not specifically assigned to a building.

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. 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 C: 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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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