OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Security of Personal, Private, and Sensitive Information (PPSI) in Mobile Computing Devices

2012-MR-2

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

December 2012

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help local government officials manage government resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of local governments statewide, as well as compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations and school district governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard local government assets.

Following is a report of our audit titled Security of Personal, Private, and Sensitive Information (PPSI) in Mobile Computing Devices. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the General Municipal Law.

This audit's results and recommendations are resources for local government officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

Introduction

Background

Regardless of their size or complexity, local governments and school districts (districts) face similar information technology (IT) security risks. Securing technology equipment and electronic storage devices can help to prevent security breaches that can result in the loss of individuals' personal, private, and sensitive information (PPSI). A security breach can be very costly, in monetary terms, to both the individual victims and to the local government entity that may be found liable for the breach. A security breach can also be costly in terms of lost productivity, negative publicity, and residents' loss of confidence in their local government or district.

PPSI is any information to which unauthorized access, disclosure, modification, destruction, or disruption of access or use could severely impact critical functions, employees, customers or third parties, or citizens of New York[1] in general. Private information could include one or more of the following: Social Security number; driver's license number or non-driver ID; account number, credit card number, or debit card number and security code; or access code/password that permits access to an individual's financial account or protected student records.

Districts often provide mobile computing devices (MCDs) to certain employees for business purposes to facilitate work when employees are in meetings, in training, or traveling. MCDs include laptop and tablet computers and other small electronic devices, such as smart phones and personal digital assistants (PDAs), which function like a personal computer while providing the convenience of portability. For example, a PDA combines an organizer (address book, calendar, and to-do lists) and instant messaging with wireless services, such as email, mobile telephone, and web browsing.

These devices are often used by district management personnel, including district officials who need access to specific IT resources during non-duty hours and district officials who are frequently away from the office. Because district officials increasingly use MCDs for business operations, they commonly integrate information systems (e.g., student information systems, email software, etc.) on these devices. MCDs often provide access to

[1] http://www.dhses.ny.gov/ocs/resources/documents/Definitions-Acronyms.pdf

the employees' own work-related data and applications, including email, as well as to protected student records that reside in student information systems. The growing sophistication and capabilities of these devices can introduce security vulnerabilities that did not exist 10 years ago. Therefore, the risks for exposure of student information and other PPSI have increased dramatically.

The widespread use of MCDs also increases the risk that PPSI could be obtained for unauthorized purposes. We found significant variation in the extent to which the districts we audited used MCDs. While some districts issued MCDs only to administrators, other districts also issued MCDs to certain teachers (e.g., special education teachers) and staff; and one district was even moving to a one-to-one laptop computer to student ratio.

Good governance and accountability require a district's board of education to adopt policies and procedures to safeguard PPSI against unauthorized access, misuse, or abuse. In addition, districts must protect PPSI to comply with the requirements of the Family Educational Rights and Privacy Act of 1974 (FERPA).[2] Generally, FERPA requires districts to get written permission from the parent or eligible student to release information from the student's education record[3] to any party, except in limited circumstances identified by statute.

The 12 districts[4] we audited serve approximately 22,630 students and are located within eight counties (Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, and Steuben) in western New York State. Each district, to varying degrees, obtains technology services provided by one of the following four Regional Information Centers[5] (RICs): Monroe #1 BOCES, EduTech, Greater Southern Tier (GST) BOCES, and the Central New York Regional Information Center (CNYRIC). Records show that these districts have distributed a total of approximately 6,130 mobile computing devices. Total budgeted appropriations for these districts for the 2011-12 fiscal year were approximately $402.1 million.

---

[2] FERPA is a Federal law that protects the privacy of student education records, and applies to educational agencies and institutions that receive funds under any program administered by the U.S. Department of Education.

[3] "Directory" information, such as the student's name, address, and date of birth, may be released without written permission.

[4] See Appendix C for details about each individual school district audited.

[5] BOCES Regional Information Centers provide collaborative IT services for the purpose of supporting management, learning, and student achievement.

Objective

The objective of our audit was to determine whether these districts are adequately controlling MCDs to protect confidential information. Our audit addressed the following related question:

- Have district officials adequately safeguarded MCDs to prevent unauthorized access to PPSI?

Scope and Methodology

For the period January 1, 2010, to May 4, 2012,[6] we interviewed district officials and staff and reviewed districts' policies and procedures to identify the controls established to protect PPSI. We also selected and reviewed a sample of mobile computing devices at each school district to identify applicable controls and the presence of PPSI. Our audit identified certain vulnerabilities concerning PPSI. Because of the sensitive nature of certain findings, they are not included in this report but have been communicated confidentially to district officials so they could take corrective action.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit is included in Appendix B of this report.

Comments of District Officials

The results of our audit and recommendations have been discussed with District officials and their comments, which appear in Appendix A, have been considered in preparing this report.

[6] See Appendix C for fieldwork end dates for each audited school district.

PPSI in Mobile Computing Devices

Parents and students rely on officials who are responsible for district operations to ensure that students' personal information is properly safeguarded and is used only for legitimate purposes. To fulfill this responsibility, it is essential that district officials develop comprehensive written IT security policies and procedures designed to protect PPSI in mobile computing devices and other equipment in the IT environment and then ensure that district security procedures are consistently followed. It is also important that district officials know about all the kinds of data they possess so they can make informed decisions about setting appropriate security levels. To do this, district officials can conduct an inventory of PPSI stored on all their electronic equipment to account for the confidential data they maintain.

We found that the majority of the 12 districts did not have adequate security policies and procedures in place, increasing the risk that PPSI could be accessed and misused by unauthorized persons. Further, our tests of a sample of 383 district-owned MCDs found PPSI on 71 (18.5 percent) of these devices. Without proper safeguards in place, any confidential data on these MCDs could be at risk of exposure. We also found that none of the districts had developed a classification scheme or performed an inventory of the PPSI the districts possess. Unless districts know about all the PPSI they maintain, district officials could find it difficult to promptly notify affected students and other parties if a security breach should occur.

Security Policies and Procedures

Effective policies and procedures for protecting PPSI address various aspects of securing confidential data and limiting access to it. Essential measures include the encryption of data so that only the intended recipients can read it. It is important that a district's policies either prohibit the inclusion of PPSI in emails, or require that confidential data be encrypted before it is emailed. Unencrypted messages sent over the Internet could be intercepted, viewed, and used for non-approved purposes. Further, a district's policies should provide for control over remote access (the ability to access district network resources from an off-site location) to define who can access the network remotely and how the district will monitor remote access. In addition, a district's policies should define how non-district MCDs can safely access district information without jeopardizing PPSI. It is also a good practice for districts to establish an information breach notification policy

detailing how district employees would notify affected parties whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

While all 12 districts had acceptable use policies in place for students and staff, none of the districts' policies were comprehensive enough to adequately protect PPSI contained on MCDs. We found that districts lacked formal policies and procedures in the following areas:

- Encryption — Eleven of the 12 districts did not have formal written policies and procedures requiring the encryption of PPSI residing on MCDs. Only the Penfield Central School District had developed and implemented an encryption policy. The policy describes the requirements for encrypting data at rest on mobile devices and the encryption key complexity requirements. When a district does not require the encryption of PPSI on MCDs, this confidential information is at increased risk of unauthorized access if the device were ever lost or stolen.

- Remote Access — Eight of the 12 districts did not have formal written policies or procedures governing remote access. When a district has not adopted and implemented a comprehensive policy to ensure that everyone accessing district resources is in compliance with acceptable use guidelines, district officials do not have full assurance that the district's IT resources and its confidential information are adequately protected.

- PPSI in Email Communications — Eight of the 12 districts either lacked any policies and procedures for protecting PPSI in email communications, or had policies and procedures with vague language that provided inadequate direction for safe emailing practices. MCDs allow district users to access or download data, including PPSI, for legitimate business purposes. However, given that these portable devices can be lost or stolen, the failure to properly secure email increases the risk that unauthorized persons could access and misuse PPSI using a district-owned MCD.

- Non-District MCDs — Eleven of the 12 districts did not have policies and procedures to restrict email access to the district's network resources by non-district MCDs.

One district, Victor Central School District, had adopted a policy that properly limits such connection capability to secure devices. This district's policy serves as a model for other districts to follow because its policy addressed the enabling of basic security settings on personal devices connecting to the district's email server. When a district fails to ensure that all devices connected to its network are secure, there is a higher risk that PPSI maintained on the network could fall into the wrong hands by design (when PPSI is obtained for malicious purposes) or by error (when PPSI is obtained unintentionally).

- Data Breach — Six of the 12 districts did not have data breach policies and procedures that informed staff about procedures to follow in the event of a data breach. The lack of such a policy potentially delays district efforts to notify affected parties that their confidential information may have been acquired by a person without valid authorization.

Table 1: Security Policies and Procedures

School District	Acceptable Use	Encryption	Remote Access	PPSI in Emails	Non-District Hardware	Data Breach
Bath	Y	N	N	N	N	N
Cato-Meridian	Y	N	N	Y	N	Y
East Rochester	Y	N	Y	Y	N	N
Geneseo	Y	N	N	N	N	N
Marcus Whitman (Gorham-Middlesex)	Y	N	N	N	N	Y
Horseheads	Y	N	Y	N	N	Y
Odessa-Montour	Y	N	Y	N	N	Y
Penfield	Y	Y	Y	N	N	N
South Seneca	Y	N	N	N	N	Y
Victor	Y	N	N	Y	Y	Y
Weedsport	Y	N	N	N	N	N
Wheatland-Chili	Y	N	N	Y	N	N

Written procedures with clear instructions for staff to follow help ensure that privileged information is not acquired by a person without valid authorization. Failure to adopt and implement formal written policies and procedures in these key areas, and to continually monitor and update them as necessary, significantly increases the risk that unauthorized users could access and misuse confidential data without detection.

PPSI Testing

Given the lack of written policies and procedures for protecting PPSI on MCDs, we tested for the presence of PPSI on district-owned MCDs used at the 12 school districts during our scope

period. We examined a total of 383 MCDs, which included laptops, smart phones, tablets, and portable media devices (i.e., PDAs and music/media players).

We found that 71 (18.5 percent) of the 383 MCDs at 11 of the 12 districts contained PPSI. We did not identify PPSI on the MCDs we reviewed at the Weedsport Central School District. Further, we identified a total of 111 instances of various types of PPSI on these 71 devices. The PPSI we identified included confidential identification and achievement data about students and staff. These 111 instances include the following: student's password (one); Social Security numbers (seven); driver's license numbers (two); student names and grades (27); personal identifying information, such as name, address, phone numbers, email, and/or date of birth (37); student names and school identification numbers (13); student locker combinations (three); staff member's personal bank statements (one); and students' individualized education programs (IEPs) and/or related observations (20).[7]

While we understand there may at times be a legitimate business need for PPSI to reside on these devices, it is the responsibility of district officials to determine who should have access to sensitive information and whether or not a 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 in place on MCDs to prevent unauthorized access to this information. For example, eight of the nine MCDs (laptops) from Penfield Central School District that contained PPSI had full disk encryption, which would prevent unauthorized access should the MCD become lost or stolen.

Loss or theft of MCDs is also a very real risk. The sample of MCDs we initially selected included three MCDs (from three different districts) that we were unable to examine because one had been stolen and two had been lost. The district had filed a police report in the case of the stolen MCD. The districts had not realized that the other two devices were lost; it only became apparent that these two MCDs were lost when district officials were unable to locate the devices for our audit. Because we were unable to examine these devices, there is no way of knowing whether or not any of these MCDs contained PPSI, and whether

[7] An IEP is privileged information because it is the legal document that defines a child's special education program. An IEP frequently includes parent information, student information, student special needs information, and health information.

adequate controls had been implemented on the devices to protect such information.

The exposure of PPSI to any unauthorized users would constitute a security breach, which could definitely have negative financial consequences for the individual(s) whose private information was accessed. Such exposure could also have a negative financial impact on the district, the custodian of this data, if it were found liable for the unauthorized release of confidential information. The occurrence of security breaches also reduces taxpayers' confidence in a district's ability to safeguard personal information about students and their families.

PPSI Data Classification and Inventory

As a best practice, all information, whether in printed or electronic form, should be classified and labeled in a consistent manner to ensure data confidentiality, integrity, and availability. The data classification process assigns a level of risk to various types of information, which helps management to make appropriate decisions about the level of security the data requires. Therefore, it is important that 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 all their electronic equipment to account for the confidential data maintained. Districts should update the classification and inventory list on an ongoing basis, as appropriate, to reflect any changes. In the event of a data breach, the proper classification and inventorying of PPSI allows district officials to determine the extent of unauthorized access and take appropriate action.

We found that none of the 12 school districts have a written district-wide data classification scheme, and that none of them have inventoried the PPSI in their possession. As a result, they do not know the extent to which PPSI resides in the electronic equipment district employees and students are using on a regular basis. Unless districts classify the data they maintain and set appropriate security levels for PPSI, there is an increased risk that PPSI could be inadvertently exposed to unauthorized users. Further, lack of information about the types and extent of data districts maintain – and where PPSI resides on all the MCDs in use – can hamper efforts to properly notify affected parties in the event of a breach.

Recommendations

1. District officials should adopt formal written policies and procedures to ensure a sound IT environment and to protect PPSI in mobile computing devices. These policies and procedures should include a breach notification policy and procedures that provides directions to employees on actions to take in the event of a data breach.

2. District officials should develop written policies and procedures that outline the proper access, use, and protection of PPSI on MCDs.

3. District officials should complete a classification and inventory of information the district maintains to assign the appropriate security level to each type of data, and then conduct an inventory of PPSI stored on all their electronic equipment to account for the confidential data maintained. Each district should update the classification and inventory list on an ongoing basis, as appropriate, to reflect any changes.

APPENDIX A

RESPONSES FROM DISTRICT OFFICIALS

We provided a draft copy of this global report to each of the 12 school districts we audited and provided each district with an opportunity to respond to the global report. We received response letters from six of the 12 districts, specifically, Horseheads, Marcus Whitman (Gorham-Middlesex), Odessa-Montour, Penfield, Bath, and Weedsport Central School Districts.

District officials generally agreed with our findings and recommendations. The following comments were excerpted from the responses we received. Comments that were specific to findings at a particular district are not included here, but are instead addressed in the district's individual letter report. Our findings at each of the 12 districts, and each district's response to our findings, are contained in the individual letter report addressed to each district.

Overall Comments

Horseheads Central School District

"The District will review and revise its information technology (IT) policies and practices as necessary to ensure proper access, use, and protection of PPSI on mobile devices."

Marcus Whitman (Gorham-Middlesex) Central School District

"The District's Board of Education and Administration are committed to ensuring that District IT operations are conducted in a secure manner."

"We have started work on formalizing policies and procedures around PPSI on Mobile Computing Devices (MCDs)."

Odessa-Montour Central School District

"There needs to be a strengthening between current practices and formal policy/regulation and the District will create policies to match safeguards which are in effect."

Penfield Central School District

"…we appreciate the efforts of the Comptroller's office to ensure the privacy of sensitive information managed by the District and the guidance provided by the subsequent release of the comprehensive document entitled Information Technology Governance."

Bath Central School District

"The District appreciates the opportunity to participate in this process and understands the resulting recommendations are intended to enhance the security of data managed and stored within our environment. The District is hopeful that the State utilizes the data gathered through this process

to evaluate and enhance the support provided for Districts related to developing and maintaining sound IT environments in school districts throughout the state."

Weedsport Central School District

"The recommendations that served as the outcome of the audit will be pursued to the fullest extent."

"It is our goal to develop and implement policies and procedures that ensure the security of personal, private, and sensitive information (PPSI) thereby minimizing the risk of loss or damage through inappropriate access and use of the District's data, hardware, and software systems."

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

The objective of our audit was to determine whether districts' officials have adequately safeguarded mobile computing devices (MCDs) to prevent unauthorized access to PPSI. To select our sampled districts, we classified districts in the 10-county Rochester region according to size (large, medium, and small), based on student enrollment, and identified the RIC that provided each district with IT services. We then stratified our sample by choosing one district of each size from each of the four regional RICs (Monroe #1 BOCES, EduTech, GST BOCES, and the CNYRIC), for a total of 12 districts. Our audit included the following steps relating to that objective:

- We interviewed district officials and staff and reviewed IT policies and procedures to identify the controls established.

- For each district, we reviewed a randomly selected sample of district MCDs to determine if PPSI was present and if proper security features were in place to protect PPSI. We selected our sample by obtaining a list of district MCDs by type, and randomly selected approximately 10 percent from each device type (i.e., tablets, laptops, PDAs, smart phones, and portable media devices) available for use by staff.

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

APPENDIX C

SUMMARY OF DATA FOR AUDITED SCHOOL DISTRICTS

Table 2: Statistics for Sampled School Districts				
School District	**Total Number of MCDs**	**Total District Appropriations in 2011-12 (Millions)**	**Approximate Student Enrollment**	**Fieldwork End Date**
Penfield CSD	1,351	$83.2	4,600	January 17, 2012
Bath CSD	1,676	$33.5	1,700	January 26, 2012
Odessa-Montour CSD	137	$15.1	800	February 8, 2012
Horseheads CSD	497	$69.3	4,400	February 16, 2012
South Seneca CSD	337	$22.0	800	February 28, 2012
Weedsport CSD	70	$17.6	900	March 14, 2012
Cato-Meridian CSD	237	$18.3	1,000	March 28, 2012
Marcus Whitman CSD (Gorham-Middlesex)	143	$28.5	1,300	April 4, 2012
Geneseo CSD	70	$16.9	900	April 19, 2012
Wheatland-Chili CSD	146	$16.5	730	April 24, 2012
East Rochester UFSD	309	$25.2	1,200	April 26, 2012
Victor CSD	1,154	$56.0	4,300	May 4, 2012
Total	**6,127**	**$402.1**	**22,630**	

APPENDIX D

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX E
OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deupty Comptroller
Steven J. Hancox, Deputy Comptroller
Nathaalie N. Carey, Assistant Comptroller

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building - Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE
Robert Meller, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington Counties

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Christopher Ellis, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

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

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street – Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

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

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

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

STATEWIDE AND REGIONAL PROJECTS
Ann C. Singer, Chief Examiner
State Office Building - Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313