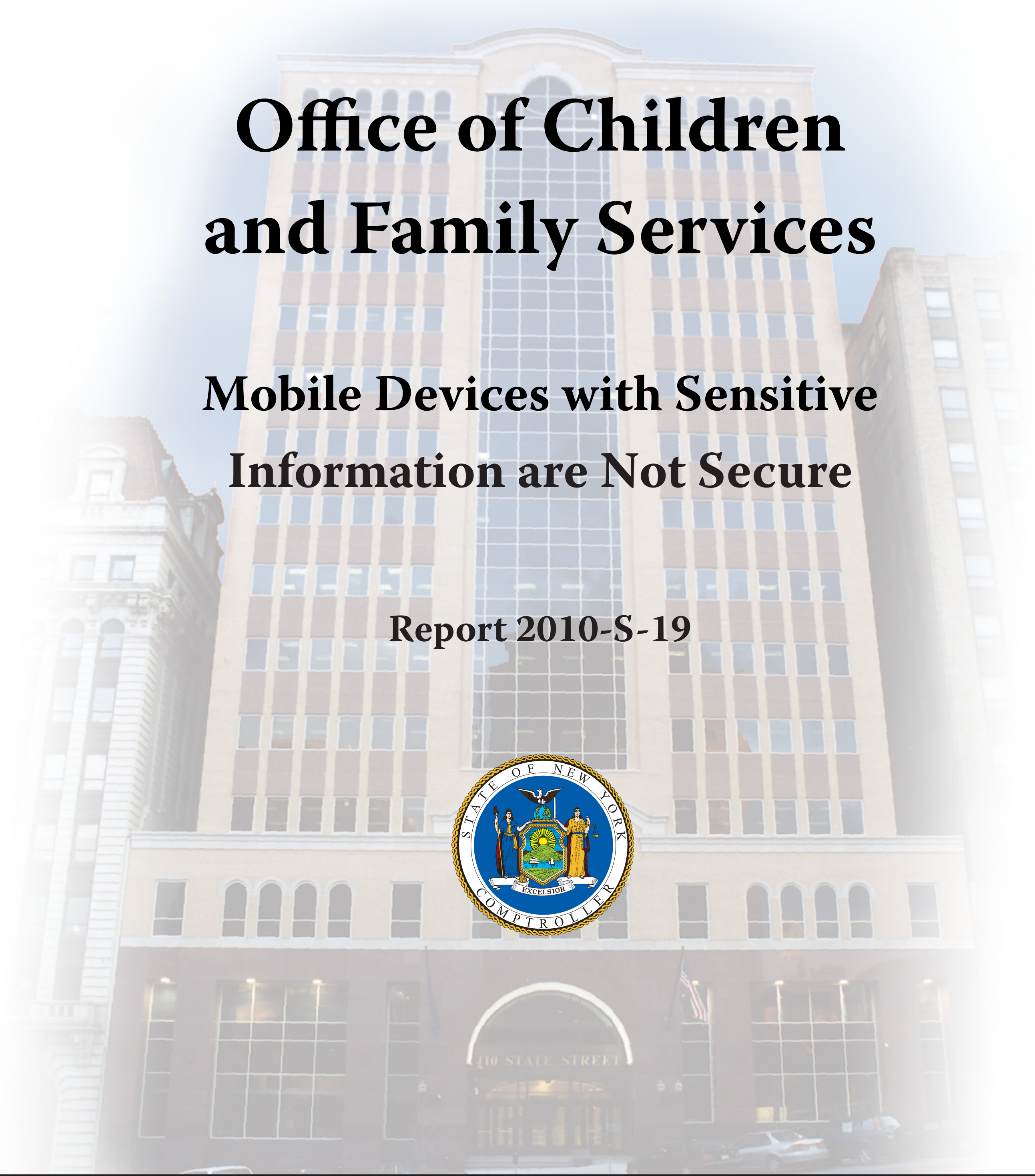
OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF STATE GOVERNMENT ACCOUNTABILITY



Office of Children and Family Services

Mobile Devices with Sensitive Information are Not Secure

Report 2010-S-19

Thomas P. DiNapoli

This page is left intentionally blank.

Table of Contents

This page is left intentionally blank.

State of New York
Office of the State Comptroller

Division of State Government Accountability

August 22, 2011

Ms. Gladys Carrión, Esq.
Commissioner
New York State Office of Children and Family Services
52 Washington Street
Rensselaer, New York 12144

Dear Ms. Carrión:

Following is our report of the Security Controls over Mobile Devices at the Office of Children and Family Services. Confidential child welfare data is at risk. The Local District staff are using unsecured laptops and word-processing keyboards. We were able to access progress notes, pictures of injuries related to case investigations and files related to court petitions and medical requests on unsecured mobile devices.

We urge you and your managers to take action on the report's recommendations and make the needed changes. If you have any questions about this report, please feel free to contact us.

Respectfully submitted,

Office of the State Comptroller
Division of State Government Accountability

This page is left intentionally blank.

State of New York
Office of the State Comptroller

EXECUTIVE SUMMARY

Audit Objective

Do security controls over mobile devices protect sensitive child welfare data from unauthorized access?

Audit Results - Summary

Confidential child welfare data is at risk of being viewed by unauthorized users. We were able to access progress notes, pictures of injuries related to case investigations and files related to court petitions and medical requests.

The Office's Information Security Officer and the Information Security Unit are responsible for the security of this data and should provide guidance and direction to ensure proper security controls are implemented. We found Local District staff are using unsecured laptops and word-processing keyboards. Further, they are storing confidential child welfare information on this equipment. Local District staff are also using the devices in public areas increasing the risk of unauthorized access to confidential information. Numerous word-processing keyboards, which may contain unencrypted confidential data, are missing. Further, information technology staff at some Local Districts are not aware if their mobile devices are encrypted or not. The Information Security Officer has not provided adequate guidance or training to Local District staff regarding the security of child welfare data on mobile devices to ensure all Office-provided laptops are encrypted.

Our report contains six recommendations for the Office and Local Districts to improve controls over mobile devices.

This report, dated August 22, 2011, is available on our website at http://www.ocs.state.ny.us.
Add or update your mailing list address by contacting us at: (518) 474-3271 or
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

This page is left intentionally blank.

Introduction

Background

The Office of Children and Family Services (Office) provides a system of family support, juvenile justice, child care, and child welfare services that promotes the safety and well being of children and adults. The Office funds and supervises 59 Local Districts that provide these services.

Local District staff use a variety of mobile devices including laptops, Blackberries, word-processing keyboards (Quick Pads and Alpha Smarts) and digital voice recorders to help complete their job duties, whether in or away from the office. These devices allow staff to record confidential information such as casework information and progress notes, and store pictures related to investigations, files related to court petitions and medical requests. In addition, staff can use these devices to access the Office's child welfare application, CONNECTIONS, as well as other Office network resources.

According to sections 136, 372(4) and 422(4) of the Social Services Law, information relating to public assistance and care, children, and children's protective services held by public agencies is deemed to be confidential and protected by law. Further, the Office has regulations which specifically set forth procedures for safeguarding this confidential information maintained by the Office, Local Districts and other authorized agencies.

In 2007, the New York State Office of Cyber Security established encryption standards for protecting State data stored on laptops. State agencies were required to implement these Standards by December 31, 2008. Further, the Office of Cyber Security's Cyber Security Policy (Security Policy) states that agencies should take steps to adequately secure data whenever laptops are used. The Security Policy applies to State entities, staff and all users who have access to or manage State information, including outsourced third parties.

The Office previously addressed the security of information stored on laptops. In a report issued to the Governor in 2006 titled: Portable Information Technology Pilot Program Report to the Governor and Legislature, the Office stated "data that can remain on portable devices poses new risks" and "encryption of all remotely stored data is essential." In the same report, the Office stated that they anticipated the deployment of encryption software on laptops that were in the field.

The security over these mobile devices is especially critical in light of a recent report of social security numbers illegally accessed from computers belonging to contractors working for a New York State agency.

Audit Scope and Methodology

We did our performance audit according to generally accepted government auditing standards. We audited selected aspects of the security controls in place over mobile devices for the period April 15, 2010 through November 24, 2010. We sought to determine whether the security controls over mobile devices protect sensitive child welfare data from unauthorized access.

To accomplish our objective, we reviewed Office policies and procedures for securing mobile devices. We interviewed Office and Local District technical staff responsible for mobile devices and operations. We visited 10 of 59 Local Districts. These included Allegany, Fulton, Jefferson, Montgomery, Orange, St. Lawrence, Schoharie, Warren and Westchester Counties and New York City. We judgmentally selected Local Districts based on risks identified from mobile device surveys sent to all Local Districts, as well as inventory reports of encrypted devices received from the State Office for Technology. At each Local District visited, we selected a judgmental sample of mobile devices to review based on the devices available and the inventory listings, where available. We used various tools and techniques to evaluate the security controls, specifically encryption and software update settings, on the devices.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our opinion, these functions do not affect our ability to conduct independent audits of program performance.

Authority

This audit was done according to the State Comptroller's authority as set forth in Article V, section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

Reporting Requirements

We provided a draft copy of this report to Office officials for their review and comment. Their comments were considered when preparing this report and are included at the end of the report. Although Office officials do not agree with all aspects of our findings, they have taken steps to implement the majority of our recommendations. We provided clarification where necessary for the Office. The Office agrees with the two recommendations for Local Districts.

Contributors to the Report

Major contributors to this report include: David R. Hancox, Brian Reilly, Nadine Morrell, Claudia Christodoulou, Jennifer Van Tassel, Corey Harrell and Randy Rose.

This page is left intentionally blank.

We were able to access confidential information, including pictures of injuries related to investigations, progress notes, and files related to court petitions and medical requests, from mobile devices being used by staff at the Local Districts. Furthermore, we found three Local Districts were missing over 100 devices that could contain unencrypted caseworker data.

Local Districts use numerous mobile devices including laptops, word-processing keyboards, digital voice recorders, and Blackberries. Local District staff use these devices to record case information and access the CONNECTIONS application. The Office should require Local Districts to ensure devices that contain child welfare data are secure. Yet we found many devices are not secured from unauthorized access. The Office has provided limited guidance to Local District staff to ensure these devices have adequate security controls. Further, the Office is not aware of all mobile devices the Local Districts are using and, in some cases, Local District IT staff are not aware of their own mobile device inventory.

Mobile Devices Are Not Protected

Local District staff use Office-issued laptops and word-processing keyboards as well as devices they purchase themselves. Laptops issued by the Office are imaged and managed by the Office for Technology. The image includes the operating system and software for the laptop. Local District staff can have the Office for Technology image put on the laptops they purchase as well. The current image includes full disk encryption. However, the Office does not require Local District staff to encrypt laptops without the Office for Technology image. Requiring this would protect the data stored on them from being read by an unauthorized user. The Office does require users, including those at the Local Districts, to implement other security controls such as installing antivirus and firewall software before granting them access to Office networks and/or applications.

During our site visits, we found child welfare data resided on unencrypted mobile devices and is not protected against unauthorized use. These include Quick Pads, Alpha Smarts and laptops with and without the Office for Technology image. There is a high risk an unauthorized user can obtain confidential information from these devices. This risk is further increased since some Local District staff connect the laptops to public wireless networks. We found:

- Unencrypted child welfare information on 14 laptops, some of which are used outside the Local District offices, at two Local Districts: Montgomery and Westchester counties. This information included investigation pictures, case notes, medical requests, police escort requests, school records and court petitions. Pictures on one laptop dated back to October 2009 and another laptop contained over 100 images. Additionally, we identified other laptops that did not have proper security settings in place. Although these devices were encrypted, some were missing security updates and none of the ones we reviewed had screensavers with password protection. The Information Security Officer should be providing guidance and direction to the Local Districts so that all devices being used have appropriate security controls in place.
- Eighteen of 91 Quick Pads at four Local Districts: Jefferson, Orange, and Westchester counties and New York City Administration for Children's Services, contained confidential data about case investigations including names, phone numbers, information about drug use, sexual abuse, and financial information. We also recovered deleted data on two Alpha Smarts at another Local District. We were able to see names, addresses, phone numbers, medical information, and other sensitive information. Data on these devices needs to be overwritten to prevent old data from being recovered. Because Quick Pads and Alpha Smarts are not and cannot be encrypted, an unauthorized user only needs physical access to the device to read the data it contains.
- Twelve percent of the laptops with the Office for Technology image are not encrypted; despite the fact the current version of the image includes full disk encryption. Staff in the Office's Information Security Unit told us some of these might have been issued during the initial pilot in 2006 when encryption was not yet required. However, in a 2006 report communicating the results of the pilot, the Office indicates they anticipated encrypting laptops used in the field. Further, the Standards required the Office to fully encrypt all laptops by December 2008. When we inquired whether the Office had plans to encrypt the remaining laptops, the Information Security Unit did not have a timeline or process to complete this task. Further, they did not have procedures for monitoring the encryption status, as required by the Standards, nor could they provide encryption reports of those devices being used by staff at the Local Districts.

IT staff at some Local Districts do not know whether the devices they purchased, or the devices received from the Office, are encrypted. In some cases, Local District officials do not even know who is using the devices or where they are located. We also found Local Districts' mobile device inventory reports are inaccurate. We found:

- One Local District, the New York City Administration for Children's Services, does not retain an accurate inventory of their laptops. This Local District, which has multiple offices, reported laptops in one location yet they were actually stored in another.
- Two Local Districts: NYC Administration for Children's Services and Warren County, could not tell us the number of Quick Pads they have and they weren't sure where they were located. Three other Local Districts could not locate all of their Quick Pads. One of these Local Districts, Westchester county was missing 121 Quick Pads while the remaining two Local Districts: Orange and St. Lawrence counties were missing 25 Quick Pads.

Most Local Districts are rarely or no longer using the Quick Pads in their inventory. At no time did the Office instruct officials at the Local Districts to return the devices that are not being used. In fact, when an official at Fulton County inquired what should be done with the unused devices, the Office told her to throw them away. Local Districts should be maintaining an inventory of all mobile devices and either return or destroy unused devices. If this is not possible they should, at the very least, ensure all confidential information is removed from them.

We surveyed the Local Districts about the guidance they received from the Office in securing mobile devices. Out of the 55 Local Districts that responded, 18 stated they did not receive any guidance from the Office or only received cable locks for their laptops. The Office does not have a mobile device policy to guide the Local Districts nor does the Office require laptops and other mobile devices be encrypted in any of its other security policies. The Information Security Officer told auditors Local District staff do not store data locally. Further, the Information Security Unit believes Local Districts are not required to comply with the Standards, which require third party laptops containing personal, private, or sensitive State information to be encrypted.

The Information Security Officer should provide sufficient guidance and training to Local Districts to ensure they are using mobile devices in a secure manner. Local District staff are using and accessing child welfare data which is the responsibility of the Office and therefore they must ensure this information is protected. Whether this information is on a device issued by the Office or purchased by the Local District, the Office should implement specific security controls and require encryption of all mobile devices transmitting, accessing, or storing caseworker data as it can prevent unauthorized users from reading data.

The Information Security Officer should develop a mobile device security policy to be followed by all staff that perform child welfare activities. In addition, the regulations regarding safeguarding confidential information maintained by the Office, Local Social Service Districts and other authorized agencies do not address the practices being used in collecting and storing such information on computer systems. The Office needs to amend its regulations to reflect these new circumstances and to require Local Districts to implement security measures to protect confidential information on these systems.

The Information Security Officer stated they are in the process of following up with the Local Districts on the unsecured mobile devices we identified. The Information Security Officer reported the Office completed the following during the course of our audit:

- Facilitated the return of unused QuickPads and AlphaSmarts. Required that any that are used should not store identifying information. In addition, the data that is on them should be deleted on a regular basis.
- Required that any laptop that has not been imaged prior to March 2007 be re-imaged to ensure encryption.
- Required all laptops used in the field to be encrypted to protect confidential data that may be contained on them. In addition, each user is responsible for verifying the encryption status on the laptop they are using. Instructions were provided to demonstrate how to verify encryption.
- Provided guidance to the LAN Administrators of the Local Districts on how to generate encryption reports.

Staff at Westchester County, have also begun to address some of the issues we identified and is replacing the laptops they purchased with newly issued encrypted laptops from the Office. They are also gathering all of their unused QuickPads and returning them to the Office.

Recommendations

To the Office:

1. Regularly communicate with and train staff at Local Districts on securing mobile devices used for child welfare activities.

2. Develop a mobile device security policy to be followed by all staff (Office, Local District, and others) that have access to or manage child welfare information.

3. Ensure all mobile devices provided by the Office are encrypted. Develop procedures for ensuring mobile devices purchased by Local Districts are encrypted.

4. Amend current regulations relating to safeguarding of confidential information to address the use of computer systems to store such information and direct Local Districts to adopt appropriate security measures to protect such information.

To the Local Districts

1. Keep an accurate inventory of mobile devices used for child welfare activities.

2. Encrypt or otherwise properly secure all mobile devices.

This page is left intentionally blank.

Agency Comments

New York State Office of Children & Family Services

www.ocfs.state.ny.us

Andrew M. Cuomo
Governor

Gladys Carrión, Esq.
Commissioner

Capital View Office Park
52 Washington Street
Rensselaer, NY
12144-2796

April 18, 2011

Mr. Brian Reilly
Audit Manager
Division of State Government Accountability
Office of the State Comptroller
110 State Street, 11th Floor
Albany, New York 12236

Dear Mr. Reilly:

This is the Office of Children and Family Services (OCFS) response to the Office of the State Comptroller (OSC) draft audit report, "Office of Children and Family Services: *Mobile Devices with Sensitive Information are not Secure*." OCFS would contend that the title of the report is inaccurate. OCFS has communicated to Local Social Services Districts (Local Districts) and others that the confidentiality of child welfare information is protected by various federal and state laws, and has taken specific and affirmative steps to protect the confidentiality of that information. It is important to note that this report indicates that only 12% of the laptop devices surveyed did not contain full disc encryption and that the vast majority of the laptops were in fact encrypted to protect the confidentiality of the information stored within them.

*
Comment
1

There are two specific themes detailed by OSC in this document which OCFS believes are inaccurate. First, OCFS would like to emphasize that OSC frequently states in this report that "OCFS should ensure" proper security controls and that mobile devices should be used in a secure manner by Local District and voluntary agency staff. OCFS has no way to "ensure" that persons outside of OCFS take proper security measures. OCFS can and has instituted policies and procedures designed to protect the security of confidential information on mobile devices used by Local Districts.

*
Comment
2

The other theme at issue in this report involves the description of the relationship between OCFS and Local Districts. In the last sentence of the first paragraph on page 9 of the draft report OSC, states that OCFS supervises "59 local offices (Local Districts) that assist in providing these services". This statement is incorrect. The local districts are not "local offices" of OCFS, but rather they are independent governmental units with independent legal responsibility and authority in regard to the provision of child welfare and other services. The local districts do not "assist" in providing those services; they actually provide child welfare and other services. The report seems to imply that districts are part of OCFS and fully subject to OCFS control when in fact local districts are independent and, although supervised by OCFS, are not under the control of OCFS.

*
Comment
3

* See State Comptroller's Comments on page 33.

An Equal Opportunity Employer

Response to OSC findings and recommendations:

1. **Regularly Communicate with and train staff at Local Districts on Securing mobile devices used for child welfare activities.**

OCFS disagrees with OSC's characterization of the AlphaSmart and QuickPad devices in the field. When these devices were initially deployed in 2002 and 2003, the intent was for these devices to supplement the ability of caseworkers to enter information into CONNECTIONS, replacing the paper pad that caseworkers would bring with them into the field. These devices have limited utility and while not capable of supporting encryption, were deemed to be more secure than the pad of paper that caseworkers had previously been using.

OCFS provided caseworkers with instructions on how to use and secure these devices, utilizing both a utility password and a "folder/portfolio" password, protecting the document contents within that folder.[1] As with the AlphaSmart, QuickPad folders may be password protected. The ability to password protect these devices made them an improvement over the use of paper in regard to protecting confidentiality. However, with the availability of other portable device technology, including laptop and table computers, the utility of these devices is deemed low, and given their age and inability to support the latest security measures, including encryption. OCFS will be advising Local Districts to return these devices to OCFS for destruction, or to securely destroy these devices and remove them from their active inventories. OCFS has advised, and will continue to advise, Local Districts that under no circumstance should any confidential information be kept on these devices or USB Flash drives unless it is encrypted using an approved encryption method.

*
Comment
4

In November of 2010, OCFS sent a memorandum to all Districts and Voluntary Agencies, reminding them that all laptops are required to have whole disc encryption software, providing instructions to users on how to verify that Point Sec or McAfee encryption exists on their laptops and is functioning properly. Users were told in order to verify a laptop's encryption status, a user simply needs to look for the encryption ICON in the system tray area (where the clock is located). The McAfee ICON looks like a small picture of a monitor. Details can be retrieved for McAfee Encryption by right Clicking the ICON and then clicking status. The Pointsec ICON is a white "P", and a user(s) need to place his or her mouse over the ICON for it to display Pointsec. Details can be retrieved by right clicking the ICON and then clicking "Information".

---

[1] See "QuikPAD IR Word Processing Device Security Password Protection Information" at http://ocfs.state.nyenet/connect/equipment/quickpad_security_password_protection_nypwa.pdf

OCFS agrees that it is important to communicate with and train staff at the Local District level. OCFS sends periodic communications, conducts training and provides Local Districts with security protocols. OCFS addressed confidentiality and encryption with the LAN Administrators at their conference in the fall of 2010. As recently as the New York Public Welfare Association (NYPWA) conference in January 2011, OCFS provided staff with an update on information security and procedures for equipment handling and disposal. OCFS will conduct targeted training to specifically address those counties that indicated that they are receiving no guidance and will direct them to the materials and contact information posted on the OCFS Intranet site for their use. OCFS will also develop and distribute a Mobile Device tip sheet procedure guide for use by Local Districts.

2. **Develop a mobile device security policy to be followed by all staff (Office, Local District, and others) that have access to or manage child welfare information.**

As part of mobile security, OCFS has required laptop devices to be encrypted since the inception of the Portable Information Technology Device pilot, for which funds were appropriated by the State Legislature in 2006/2007.[2] In the 2008 Report to the Legislature on that pilot, OCFS indicated that encryption technology was installed on all portable devices funded through the Technology Device pilot prior to deployment. Since being advised by OSC that some Local District laptop computers in their inventories did not have whole disc encryption, whether due to the devices having been reimaged with an older image, or for a variety of other reasons, OCFS has instituted a project to remediate the issue. Some laptops, due to the portability of the devices, may have predated the Portable Device Technology pilot and may not have been issued with whole disc encryption. Others may not have been connected to the Human Services Enterprise Network (HSEN) in order to have received the latest image from the Office for Technology, containing the latest security controls and patches, including whole disc encryption. OCFS has directed LAN Administrators in Local Districts to assess the laptops in their inventories, verifying that whole disc encryption exists on these devices, and further instructing individual caseworkers on how to verify that the encryption on their laptop devices exists and is functioning properly.

---

[2] See Portable Device Information Technology Pilot Report to the Governor and New York State Legislature, pages 6, 8, and 23.

OCFS, with the assistance of the New York State Chief Information Officer (CIO) and Office for Technology (OFT) has included Full Disk encryption as part of the installation process for laptop computers, beginning with the deployment in March 2007 of "OneImage" (Gen3). Every subsequent Image (currently Gen7) deployed contains an encryption program. The current System Center Configuration Manager (SCCM) OneImage also contains this program as part of the installation for laptop computers. Prior to August, OFT utilized a product called "PointSec Encryption." Beginning in August 2009, CIO/OFT entered into an agreement with McAfee Security for the McAfee encryption suite, replacing PointSec encryption in the installation process.

Recognizing the importance of maintaining the confidentiality of child welfare information, OCFS has initiated a project to verify that all laptops utilized by Local Districts are encrypted, directing all LAN Administrators to have their laptops connected to the HSEN network for at least one hour per month, in order for these devices to receive the latest security updates, including whole disc encryption. The remediation of these devices is ongoing and is expected to be completed by September 30, 2011. In addition, in the event a laptop is not connected to the HSEN at least once every sixty (60) days to receive the latest security updates, OFT has advised OCFS that they will automatically disable these devices preventing them from connecting to the HSEN.

Over the years, OCFS has provided direction, through a variety of Administrative Directives (ADMs), Informational Letters (INFs), Local Commissioners Memorandums (LCMs) and Memorandums of Understanding (MOU) that child welfare information is confidential and is to be protected from wrongful disclosure. To participate in the portable technology project, Local Districts agreed to abide by security and confidentially requirements. As documented in the Portable Information Technology Device pilot, staff is also permitted to access the network through using a Virtual Private Network (VPN), providing them a secure, encrypted tunnel for accessing the State HSEN. Prior to gaining VPN access, staff must be authorized access, pursuant to the Remote Access MOU, which advises staff of their responsibilities to communicate through the VPN in a secure, authorized manner. On April 15, 2011 OCFS sent a letter (see attachment) to all Local Districts reminding them that some portable devices, such as QuickPads and AlphaSmarts, are not capable of supporting encryption, unlike the newer technologies provided by OCFS, and therefore under no circumstances should caseworkers enter confidential information into these devices. OCFS is further requesting these devices be returned to OCFS for destruction or be securely destroyed by the Local Districts. Finally, OCFS is drafting a "Mobile Device Policy," to provide Local District caseworkers with guidance and procedures to be followed for physical and technical security while utilizing portable technology devices in the field.

3. **Ensure all mobile devices provided by the Office are encrypted. Develop procedures for ensuring mobile devices purchased by Local Districts are encrypted.**

As mentioned earlier, OCFS with the assistance of the CIO and OFT, has included Full-Disk encryption as part of the installation process for all new laptop computers. This started with the deployment of "OneImage" (Gen 3) in March 2007. Every subsequent Image (currently Gen7) that has been released for new laptops has contained whole disc encryption. The current System Center Configuration Manager (SCCM) OneImage also includes whole disc encryption as part of the installation for all new laptop computers. Prior to August 2009, OFT utilized a product called "PointSec Encryption". Since August 2009, CIO/OFT has been utilizing the McAfee Security Encryption suite in the installation process. OCFS is also, going forward, requiring that all laptops purchased on behalf of Local Districts receive the McAfee Security Encryption suite prior to being deployed to the field.

OCFS will continue to verify that all laptops utilized by Local Districts are encrypted. For those unencrypted laptops, OCFS has instituted a remediation effort to verify that encryption software is installed, and in fact has shown an improvement in the percentage of encrypted laptops. OCFS expects to complete this effort by September 30, 2011. In addition, in the event a laptop is not connected to the HSEN at least once every sixty (60) days to receive the latest security updates, OFT automatically disables these devices preventing them from connecting to the HSEN. OCFS is also developing guidance to the Local Districts along with a tip sheet to assist Local Districts in verifying that their mobile devices are encrypted.

*
Comment
5

4. **Amend current regulations relating to safeguarding of confidential information to address the use of computer systems to store such information and direct Local Districts to adopt appropriate security measures to protect such information.**

Child welfare information is designated as confidential by New York State law and regulation. OCFS policies, in conformation with regulations described in 18 NYCRR 466.6, require that the security of information in the CONNECTIONS system be maintained by those who use CONNECTIONS. It is unclear to OCFS what specific regulatory recommendations OSC is suggesting with respect to the unspecified "new circumstances" mentioned in the draft report which would improve the confidentiality of child welfare information.

*
Comment
6

* See State Comptroller's Comments on page 33.

The report also includes two recommendations directed to Local Districts:

1. Keep an accurate inventory of mobile devices used for child welfare activities.
2. Encrypt or otherwise properly secure all mobile devices.

OCFS agrees with both of these recommendations directed to Local Districts.

In summary, OCFS will continue to provide guidance to local districts on how to secure information on mobile devices. This response outlines a number of activities OCFS is engaged in to improve the security of Mobile Devices with Sensitive Information. OCFS appreciates the opportunity to respond to this report. Any questions you may have can be directed to Ralph Timber, OCFS Audit Liaison, at (518) 473-0796.

Sincerely,

William T

William T. Gettman, Jr.
Executive Deputy Commissioner
New York State Office of Children and Family Services

Attachments

April 15, 2011

New York State
Office of
Children &
Family
Services

Andrew M. Cuomo
Governor

Gladys Carrión, Esq.
Commissioner

Capital View Office Park

52 Washington Street
Rensselaer, NY
12144-2796

Dear Commissioner,

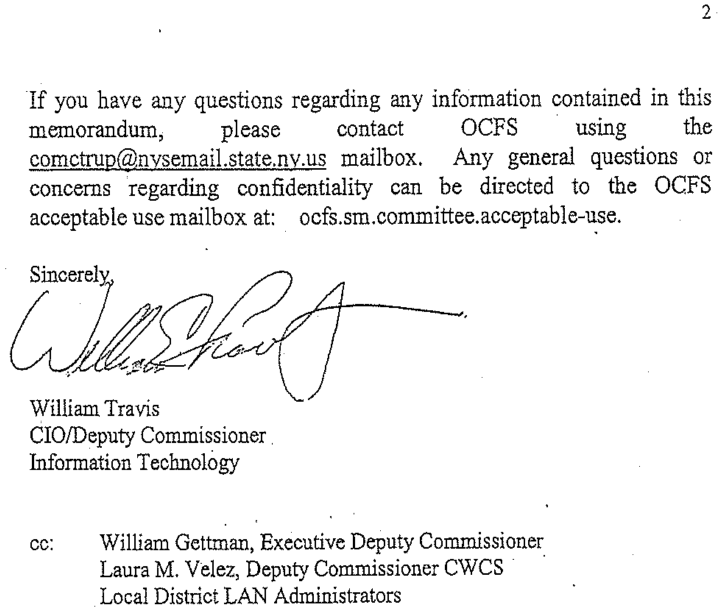
All Local District staff are reminded that all personal, private and sensitive information ("PPSI"), regardless of the form, format or location must be kept confidential and be protected from unauthorized access or disclosure. Each individual employee is responsible for maintaining the confidentiality of PPSI within their control, and adhering to OCFS' policy regarding safeguarding that confidential information.

In 2002 and 2003, OCFS had provided Local Districts with a variety of portable devices, including QuickPads, AlphaSmarts. These devices were intended to assist caseworkers in the field with taking notes which could later be imported into CONNECTIONS. While not capable of supporting encryption, these devices were capable of supporting password protected documents, providing, at the time issued, better security for a caseworker than previously afforded. Over time, additional devices were deployed statewide, including encrypted laptops, tablets, digital pens, and other devices to permit caseworkers and staff to work more efficiently and perform their casework in the field.

Laptops and tablet computers that are capable of supporting encryption are the only devices that should be utilized for entering and storing confidential information. As QuickPads and AlphaSmarts are not capable of supporting encryption, they must not be used for entering or storing such information. Accordingly, these devices are no longer permitted for child welfare casework. Local Districts are to return these devices to OCFS for destruction, or certify in writing that all devices in their possession have been securely destroyed. For guidance on physical destruction, please see Attachment A.

When used in the field, users must use caution and be responsible for the security of authorized portable devices, keeping them attended at all times or physically secured. Additionally, all laptops must be encrypted with full disk encryption prior to storing or transmitting any PPSI or electronic Protected Health Information (e-PHI). In no circumstance should any PPSI or e-PHI be kept on USB Flash or Thumb drives unless it is encrypted. Note: Please refer to the November 2010 CONNECTIONS Weekly Update for a security message requesting users verify that their issued laptops are properly encrypted, see Attachment B.

An Equal Opportunity Employer

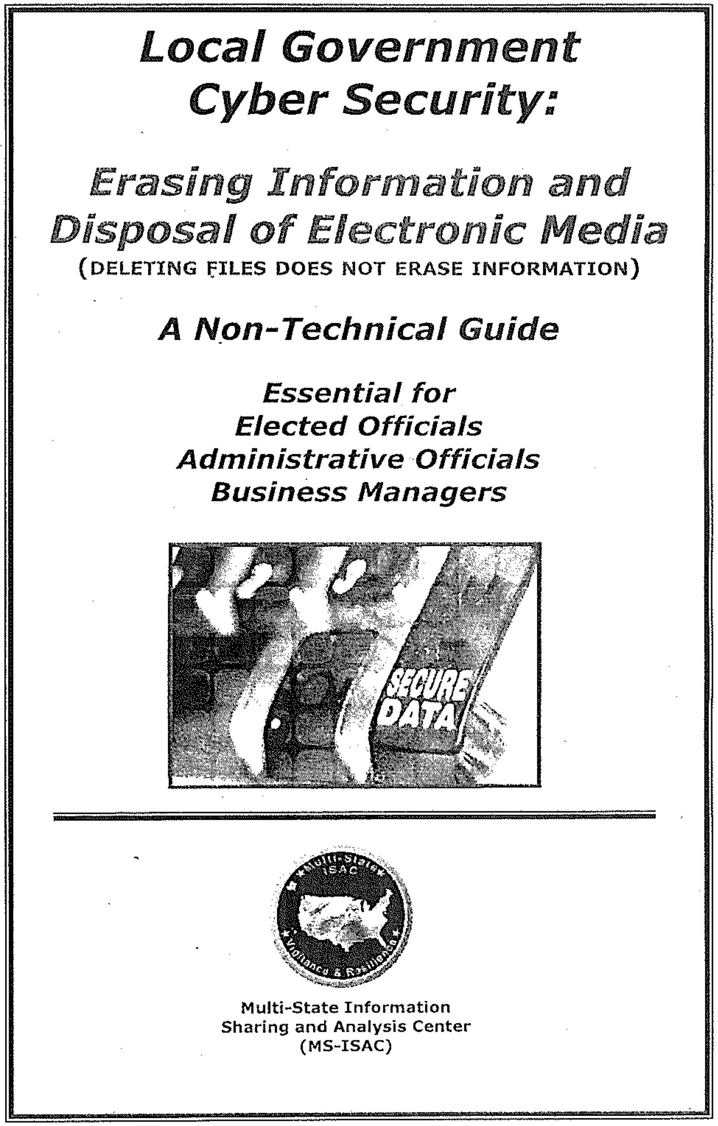


If you have any questions regarding any information contained in this memorandum, please contact OCFS using the comctrup@nysemail.state.ny.us mailbox. Any general questions or concerns regarding confidentiality can be directed to the OCFS acceptable use mailbox at: ocfs.sm.committee.acceptable-use.

Sincerely,

William Travis
CIO/Deputy Commissioner
Information Technology

cc: William Gettman, Executive Deputy Commissioner
Laura M. Velez, Deputy Commissioner CWCS
Local District LAN Administrators



Local Government Cyber Security:

Erasing Information and Disposal of Electronic Media

(DELETING FILES DOES NOT ERASE INFORMATION)

A Non-Technical Guide

Essential for
Elected Officials
Administrative Officials
Business Managers

Multi-State Information
Sharing and Analysis Center
(MS-ISAC)

This appendix is a supplement to the *Local Government Cyber Security: Getting Started Guide,* a non-technical reference essential for elected officials, administrative officials and business managers. This appendix is one of many which is being produced in conjunction with the *Guide* to help those in local governments to further their knowledge and awareness regarding cyber security. For more information, visit: http://www.msisac.org

OTHER CONSIDERATIONS

Returning Media Under Warranty Many hard drives are purchased with a warranty period. When devices fail during the warranty period, the vendor normally requires the return of the defective drive before a warranty replacement is provided. Warranty return of a defective drive includes all the data, documents and information stored on the drive prior to the fatal problems. Since sensitive data could potentially be exposed on a warranty returned defective drive, the organization should resort to physical destruction instead of returning the drive to the vendor. Your vendor may have an option to not return the hard drive.

Audit Trail A log should be maintained of all media that have been disposed. The log should include the date, type of device, manufacturer, serial number (if one exists), sanitation or destruction method used, disposal method such as sold or crushed.

Acknowledgement

Special thank you to Laura Iwan and the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) for their contribution to this paper.

Portions of this article are taken directly from Monthly Cyber Security Tips NEWSLETTER Volume 1, Issue 3, August 2006 edition and reprinted with permission.The full article may be found on the MS-ISAC website, http://www.msisac.org.

Any product-specific resources mentioned in this paper are provided as a general reference only. We do not endorse or promote the advertising of any resources.

Issues

- Environmental concerns may exist with incinerating media.
- Mechanisms need to be implemented to ensure the media is appropriately destroyed. Requiring a contractor to crush the media on site would be an appropriate control.
- Safety concerns include, but are not limited to, the use of safety goggles when using physical destruction techniques.

RECOMMENDED TECHNIQUES FOR DISPOSAL OF ELECTRONIC STORAGE MEDIA Once an organization has decided to dispose of electronic storage media then the following table can be used as a reference of recommended techniques to accomplish the job.

This is not an all inclusive list of devices but a sample of the most commonly used pieces of equipment. Any device used to process information electronically may store information.

Erasure and Disposal Technique Matrix

Media Type	Wipe OR	Degauss OR	Physical Destruction
Computer Hard Drive Network Hard Drive External Drives	●	●	●
Fax Machine Printer Copier	●		●
CDs DVDs			●
USB Drives Thumb Drives Memory Sticks	●		●
Floppy Disks	●	●	●
Tapes	●	●	●
PDAs Cell Phones	●		●

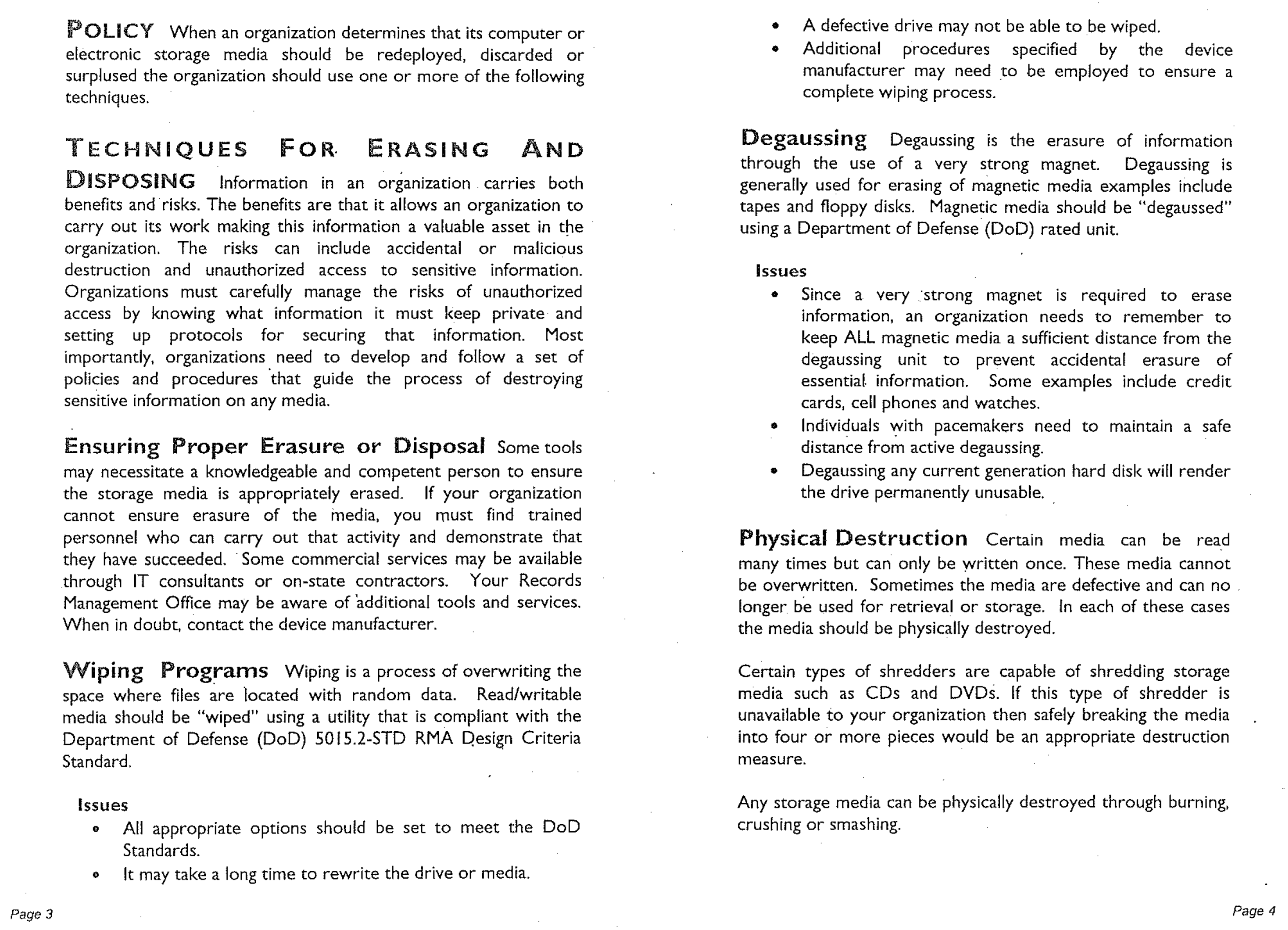
INTRODUCTION The intent of this policy is to describe how to dispose of computers and electronic storage media effectively and prevent the inadvertent disclosure of information that often occurs because of inadequate cleansing and disposal of computers and electronic storage media.

There are many laws that require information be protected. Some examples of these laws are public health laws, privacy laws and the Health Insurance Portability and Accountability Act. Social Security numbers, credit card information, health-related information and trade secrets are examples of sensitive information requiring protection from disclosure. To the extent that electronic media is used to store official records, organizations must also adhere to records management rules, including records retention schedules.

Sensitive documents and data containing personally identifiable information can be stored electronically in multiple formats and locations. For example, the information might first exist on a CD then be copied to the computer's hard drive and subsequently backed up to a tape for disaster recovery purposes. In this example, there are three different storage media to consider: CD, hard drive and backup tape.

Remember: Simply viewing a file with a computer can create a copy of the file on the computer's hard drive.

Deleting files does not erase information. Information that is deleted from a computer may be retrieved by using forensics or other recovery tools. As new computers are purchased, older computers may be redeployed, discarded or surplused. It must be assumed that at some point in time sensitive information may have been stored and is still retrievable from all electronic storage media including computer and network hard drives, external hard drives, CDs, DVDs, floppy disks, tapes, thumb drives, memory sticks, PDAs, cell phones and other storage devices not enumerated here.



POLICY When an organization determines that its computer or electronic storage media should be redeployed, discarded or surplused the organization should use one or more of the following techniques.

TECHNIQUES FOR ERASING AND DISPOSING Information in an organization carries both benefits and risks. The benefits are that it allows an organization to carry out its work making this information a valuable asset in the organization. The risks can include accidental or malicious destruction and unauthorized access to sensitive information. Organizations must carefully manage the risks of unauthorized access by knowing what information it must keep private and setting up protocols for securing that information. Most importantly, organizations need to develop and follow a set of policies and procedures that guide the process of destroying sensitive information on any media.

Ensuring Proper Erasure or Disposal Some tools may necessitate a knowledgeable and competent person to ensure the storage media is appropriately erased. If your organization cannot ensure erasure of the media, you must find trained personnel who can carry out that activity and demonstrate that they have succeeded. Some commercial services may be available through IT consultants or on-state contractors. Your Records Management Office may be aware of additional tools and services. When in doubt, contact the device manufacturer.

Wiping Programs Wiping is a process of overwriting the space where files are located with random data. Read/writable media should be "wiped" using a utility that is compliant with the Department of Defense (DoD) 5015.2-STD RMA Design Criteria Standard.

Issues

- All appropriate options should be set to meet the DoD Standards.
- It may take a long time to rewrite the drive or media.

Page 3

- A defective drive may not be able to be wiped.
- Additional procedures specified by the device manufacturer may need to be employed to ensure a complete wiping process.

Degaussing Degaussing is the erasure of information through the use of a very strong magnet. Degaussing is generally used for erasing of magnetic media examples include tapes and floppy disks. Magnetic media should be "degaussed" using a Department of Defense (DoD) rated unit.

Issues

- Since a very strong magnet is required to erase information, an organization needs to remember to keep ALL magnetic media a sufficient distance from the degaussing unit to prevent accidental erasure of essential information. Some examples include credit cards, cell phones and watches.
- Individuals with pacemakers need to maintain a safe distance from active degaussing.
- Degaussing any current generation hard disk will render the drive permanently unusable.

Physical Destruction Certain media can be read many times but can only be written once. These media cannot be overwritten. Sometimes the media are defective and can no longer be used for retrieval or storage. In each of these cases the media should be physically destroyed.

Certain types of shredders are capable of shredding storage media such as CDs and DVDs. If this type of shredder is unavailable to your organization then safely breaking the media into four or more pieces would be an appropriate destruction measure.

Any storage media can be physically destroyed through burning, crushing or smashing.

Page 4

November CONNECTIONS Security Message

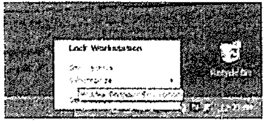
Use of Laptops and Encryption

All laptops used in the field must be encrypted in order to protect confidential data that may be contained on them.

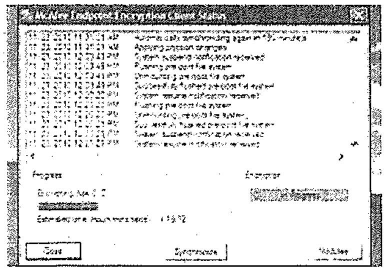
- Each user is responsible to verify the Encryption Status of the laptop they are using.
- In order to verify the encryption on a laptop the user simply needs to look for the encryption ICON in the system tray area (next to where the clock is located) at the bottom right of the screen.
- The McAfee ICON looks like small picture of a monitor. Details can be retrieved for McAfee Encryption by right Clicking the ICON (step 1) and then click status (step 2).
- The Pointsec ICON is a white "P." If you place the mouse over the ICON it will display Pointsec. Details can be retrieved by right clicking the ICON and then click Information.
- Should you encounter an issue where a laptop is not encrypted or you are not sure if the laptop is encrypted, it should immediately be brought to the attention of your LAN Administrator for corrective action.

Reminder: Each user is responsible to make sure that they connect their laptop to the network for 30 minutes each month in order for the laptop to receive updates and patches, and remain on the network. Your attention to this important function assists the agency in keeping data safe while continuing to provide ease of use services to its customers. If you have any questions, please contact your LAN Administrator.

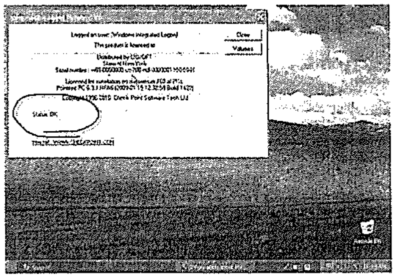
Location of encryption icon for McAfee or PointSec:



McAfee



Pointsec



Please note: If you are using any mobile device that cannot be encrypted, such as an Alpha Smart or Quick Pad, it should never contain any identifying information, such as name or address. Case number can be used to identify the case or family. In addition, the data on the device should be deleted on a regular basis.

If your agency has any OCFS mobile devices that cannot be encrypted that are no longer being used, contact your LAN administrator for him or her to arrange for their return to OCFS.

This page is left intentionally blank.

State Comptroller's Comments

1. The title of the report, *Mobile Devices with Sensitive Information Are Not Secure*, is accurate. We found many mobile devices - laptops, QuickPads and AlphaSmarts - that were not encrypted and/or were not secured that contained sensitive information and were in use at the Local Districts. As a result, we were able to access confidential information, including pictures of injuries related to investigations, progress notes, and files related to court petitions and medical requests from mobile devices being used by staff at the Local Districts. Moreover, we found that three Local Districts were missing over 100 devices that could contain unencrypted caseworker data. We do not find it particularly reassuring to note that 12 percent of the laptop devices surveyed did not contain full disk encryption.

2. We agree the Office cannot monitor the practices and security measures used by all the Local Districts in protecting the security of confidential information. However, as noted in our recommendations, the Office needs to provide guidance to Local Districts by developing a security policy for mobile devices as well as implementing standards and procedures.

3. We changed the reference from Local Offices to Local Districts and we now indicate that they provide child welfare services.

4. Although certain versions of Quick Pads and Alpha Smarts are capable of being password protected, we found none of the devices we reviewed at the Local Districts were password protected. This further indicates there is a need to provide more guidance to the Local Districts on securing devices used to store confidential information.

5. This recommendation pertains to all mobile devices, not just laptops.

6. Regulations 357.5 and 428.10 of Social Services Law set forth procedures for safeguarding confidential information maintained by the Office, Local Social Services Districts and other authorized agencies. In addition, pursuant to sections 136, 372(4) and 422(4) of the Social Services Law, information relating to public assistance and care, children, and children's protective services held by public agencies is deemed to be confidential and protected by law. In accordance with its authority under section 20(3)(d) of the Social Services Law, the Office has promulgated regulations, most notably sections 357.5 and 428.10 (18 NYCRR §§ 357.5,428.10), which specifically set forth procedures for safeguarding this confidential information maintained by the Office, Local Social Service Districts and other authorized agencies. Due to the fact that governmental agencies are now collecting and storing such information on computer systems, the Office needs to amend its regulations to reflect these new circumstances and to require Local Districts to implement security measures to protect confidential information on these systems. The rules of confidentiality apply once information and data are put into their systems (mobile devices).