



MEMORANDUM

Date: November 30, 2012

To: John H. Armstrong, MD, FACS, Surgeon General & Secretary

From: James D. Boyd, C.P.A., M.B.A., Inspector General

Subject: DOH Cell Phone Usage

Objective

Department of Health (DOH or Department) executive management requested the Office of Inspector General determine the number of state-issued cell phones currently in use throughout the Department and to develop proposed criteria for issuing and using such a device by employees, focusing on documenting the need for the device itself and various device features (such as texting, internet, etc.).

Summary of Conclusions

Given the current movement in all aspects of business is towards maximizing the ability of employees to be able to conduct work anywhere, anytime and in real time, the use of mobile devices has become an increasing necessity. This is evident as the demand for smart phones, tablets and other portable computing devices, which provide for a comprehensive ability to communicate and access information, have become among the most in-demand products on the market today.

The government sector is also rapidly embracing this movement as a means of providing the public with improved quality of services and ensuring the ability to meet expectations in an environment with a shrinking workforce. However, it is important to address the risks that exist with issuing these technological devices to employees. Some risks include: employee misuse, information security, public records availability, asset management and fiscal accountability.

Non-business activities that utilize state-issued technology devices cannot be managed solely by restricting the issuance of these devices alone. Each of the numerous service features available on the various devices require collaboration of business and technology experts to help ensure risks are managed at an acceptable level. The solution is to manage the risks that exist through adequate controls that will govern the issuance and use of these devices.

In order to adequately address the risks associated with these devices and yet still embrace the current overall movement of an increasingly mobile society and workforce, we recommend management consider the following:

In the short term:

- Enhance the *Assignment of Mobile Device* form required for acquisition of a state-issued mobile technology device (including cell phones) to require specific justification for not only the device itself, but for any of the service features the device would provide (such as texting, internet access, pictures and video, DOH systems access, etc).
- Approval to issue a device should be provided by a senior level of management over the particular business unit (such as Deputy Secretary or Division Director level) that would ensure an independent body approves the request based upon need and justification provided.
- Require all current DOH employees issued a mobile technology device to complete a new *Assignment of Mobile Device* form (following revision) that would include specific justification for the device itself and features of the device tied to their job duties. Any features not needed should be turned off (if possible) and any devices rarely used, not used for an extended period of time, or do not tie to job duties should be relinquished back to DOH.

In the long term:

- Tie the request for acquisition of a mobile technology device to an individual's *Position Description*, which should clearly acknowledge the position may require the use of a mobile technology device in the performance of the job duties. The *Position Description* should then be attached to any documentation requesting approval of a mobile device.
- Develop a mobile device policy which defines the term 'mobile device' for the Department, addresses usage standards, security standards, device configuration standards, data storage standards, etc. Policy may disallow all service features deemed too risky or unmanageable or may prescribe the Department programs that have been approved to utilize specific service features. The design of administrative controls should be a collaborative effort with input from the various Department programs areas and technology experts.
- Increase awareness and education related to mobile device usage.
- Revise the definition of "Information Technology Assets" in DOH Policy 250-11-12, which is currently outdated.
- Ensure all mobile technology devices be entered into the Asset Management System.

- Require that assignment of all issued mobile technology devices be re-approved on a set periodic basis to ensure the need for each device and the features of the device are still necessary.

The information below provides additional supporting information and specific details of the recommendations noted above.

Status of DOH Cell Phone Usage and Costs

Sprint and Verizon are the two primary state-term contracts under which mobile technology communication services can be acquired. Currently, there are a total of **4,790** DOH mobile devices with active service from these two carriers. From July 1, 2011 to present, **DOH spent a total of \$1,910,074.62** on all mobile technology services. Each carrier has various service plans and ways they bundle services. There are separate costs for each feature such as texting, tethering, and picture and video. The following tables detail the current device usage, available plans and associated costs, top units by expended dollars from July 1, 2011 to present and top units by reimbursed dollars for non-business usage for fiscal year (FY) 2011-2012:

Current DOH Usage		Device and Feature Charges Available Through State-Term Contracts	
Verizon Wireless		(all charges monthly)	
Total Non-Smart Phones	3,074	Non-Smart Phone (phone only)	\$ 0.05
Total Smart Phones	1,426	Smart Phone	\$ 37.49
<i>Blackberry</i>	<i>1,021</i>	Smart Phone Nationwide	\$ 37.49
<i>iPhone</i>	<i>371</i>	Smart Phone Global	\$ 51.99
<i>Motorola</i>	<i>18</i>	Add on Unlimited Calling	\$ 45.00
<i>HTC</i>	<i>9</i>	Add on Unlimited Nationwide Calling	\$ 65.00
<i>iPad (uses data plans)</i>	<i>6</i>	Tethering - Florida	\$ 10.00
<i>Palm</i>	<i>1</i>	Tethering - Nationwide	\$ 15.00
		Text per 100 messages	\$ 2.99
		Picture and video 250 messages	\$ 5.00
Sprint		(all charges monthly)	
Total Non-Smart Phones	125	Blackberry Bundle w/ 400 minutes	\$ 49.99
Total Smart Phones	165	Blackberry Bundle w/ 1000 minutes	\$ 74.99
<i>Blackberry</i>	<i>163</i>	Custom Blackberry w/ no minutes	\$ 37.49
<i>iPhone</i>	<i>2</i>	Business Essential w/ 400 minutes (non-smart phone)	\$ 29.99
		Business Essential w/ 1000 minutes (non-smart phone)	\$ 44.99
		Business Essential w/ no minutes (non-smart phone)	\$ 18.75

Source: Sprint and Verizon Wireless

Top DOH Units By Expended Dollars for Non-Business Use (July 1, 2011 to present)			
Disease Control	\$ 110,378.68	Polk CHD	\$ 56,224.30
Palm Beach CHD	\$ 102,323.58	Information Technology	\$ 55,450.45
Miami-Dade CHD	\$ 100,220.54	Duval CHD	\$ 54,111.56
Division of CMS	\$ 95,004.13	Sarasota CHD	\$ 48,085.63
Broward CHD	\$ 87,767.21	Medical Quality Assurance	\$ 45,451.13
State Surgeon General	\$ 83,408.17	Deputy State Health Officer	\$ 44,198.43
Orange CHD	\$ 63,985.85	Pinellas CHD	\$ 42,857.08
Hillsborough CHD	\$ 58,052.97	Escambia CHD	\$ 41,081.23
Family Health	\$ 57,924.60	Volusia CHD	\$ 40,957.70

Source: DOH Division of Administration: P-Cards. Policy and Systems Group

On occasion, DOH employees have used state-issued mobile devices to make or receive personal calls, texts, etc. While this practice is discouraged, current policy does provide that an employee should reimburse the Department for any personal or non-business use of their state-issued mobile device. During FY 2011-2012, DOH employees **reimbursed funds in the amount of \$54,696** for personal or non-business mobile device use.

Top DOH Units By Reimbursed Amount for Non-Business Use in FY 2011-12			
Hillsborough CHD	\$ 5,991.78	Emergency Operations	\$ 1,440.52
Palm Beach CHD	\$ 4,148.19	Martin CHD	\$ 1,281.33
Children's Medical Services	\$ 3,826.39	Duval CHD	\$ 1,267.16
Dade CHD	\$ 3,366.31	Indian River CHD	\$ 1,118.15
Sarasota CHD	\$ 3,304.54	Osceola CHD	\$ 994.22
Disease Control	\$ 2,437.28	Polk CHD	\$ 990.90
Environmental Health	\$ 1,850.01	Volusia CHD	\$ 943.71
Broward CHD	\$ 1,604.30	Escambia CHD	\$ 910.87
Pinellas CHD	\$ 1,447.09	Hardee CHD	\$ 834.93

Source: DOH Division of Administration: P-Cards. Policy and Systems Group

Due to various reasons such as device design and service package plans, service features such as texting, and picture and video cannot be disabled by the carrier on smart phones. However, these service features may be disabled by the carrier on non-smart phones (basic cell phones). In order to control these service feature sets, technical device configuration controls may be implemented on the smart phone device itself through utilization of mobile device management (MDM) techniques (Please see **Attachment 4** for more information on MDM). When preventative technical controls are not present (e.g. cannot turn off texting on a device); administrative controls should be instituted within a mobile device policy to control specific functions and activities. This helps support acceptable use of mobile devices and ensures enforceability when Department staff use mobile devices inappropriately.

Specifics of Short-Term Management Considerations

To help ensure DOH's mobile device needs are met in a controlled, fiscally responsible and auditable fashion we recommend the current *Assignment of Mobile Device (Attachment 2)* form within DOHP 56-86-10, *Cell Phone Bill Verification System* be redesigned and the surrounding business processes revised in following manner:

- 1) Rename the *Assignment of Mobile Device* form with a more accurate description such as "*Mobile Technology Approval Form.*"
- 2) Designate one executive or senior level manager to approve requests for mobile technology devices for each primary DOH business unit, specifically all county health departments (CHDs), all Children's Medical Services offices and either each Division or all of Headquarters.
- 3) Within the newly created "*Mobile Technology Approval Form*", insert checkboxes for technology device features such as: texting, internet, tethering, picture and video and data

services, etc. For each checkbox selected, a justification communicating “why” the feature is needed for the position to execute its responsibilities must be provided.

- 4) Revise DOHP 56-86-10, *Cell Phone Bill Verification System* procedures to require all staff assigned and approved for a DOH mobile technology device to complete the *Application and Acknowledgement Form for Mobile Communications Equipment (Attachment 3)*, which is to be signed by the user to acknowledge their request for a mobile technology device and their acceptance of responsibility for use of that device. The form should be reviewed, renamed and revised as appropriate to ensure it outlines acceptable mobile device usage and consequences, based upon the concerns of DOH management.
- 5) Route a package containing all completed forms mentioned above to the designated executive or senior level manager for final approval.
- 6) Upon approval, route the forms to Finance and Accounting for service acquisition and setup in the Cell Phone Bill Verification System.
- 7) Consider including the appropriate Division of Information Technology entity in the process flow to ensure appropriate device configuration as per security policies.
- 8) Consider revising policies to allow personal or non-business use of Department owned mobile devices only in the event of an emergency.

Specifics of Long-Term Management Consideration

The considerations above are business process changes that can be acted upon immediately to help ensure mobile devices are only issued to staff with a business need. However, the overall framework for the Department’s mobile computing environment needs to be examined to ensure the appropriate systems of control are in place to mitigate the risk of mobile devices to an acceptable level. A mobile workforce has become a necessity for efficient and effective government. As government identifies new efficiencies in offering a mobile workforce, the quantity of mobile devices will likely increase in the future. Furthermore, the Department should consider that state-wide surveys indicate that many state employees¹ utilize their personal devices for business purposes.

We recommend the following considerations be addressed over the long term through collaboration of IT, Finance and Accounting and various business entities with mobile workforce needs. These recommendations will help ensure the Department has the appropriate controls in place to minimize the many risks inherent with mobile computing and communications:

- 1) Remove the “Phone Assignment Criteria” box from the *Assignment of Mobile Device* form and place on each *Position Description* (PD). This box should be renamed to more

¹ Office of the Chief Inspector General, *Survey Results of Information Technology Mobile Computing in Florida’s State Government*

accurately describe its purpose. One recommendation may be “Technology Justification Criteria”. This would then be the catalyst to document that the position does have the need for mobile technology devices. (Please see **Attachment 2** for a view of the Phone Assignment Criteria box below).

The PD will document individual position business needs by indicating travel requirements, emergency preparedness responsibilities, physical security responsibilities, hazardous working conditions, necessity for time-sensitive responses and/or communications and other position mobility requirements. Aligning technology needs associated with the position responsibilities eliminates the need for management judgment in prequalifying a position for a technology purchase and/or assignment. Furthermore, it helps ensure the technology stays with the position and not the individual user.

Once the PD has been changed to include this information, the PD should also be attached to the package that goes to the executive or senior management level for approval when acquiring a new device or a new service.

- 2) DOH through a collaborative management effort should draft a mobile device policy to:
 - Define the term ‘mobile device’ for the Department;
 - Address usage standards to include texting, and pictures and video for the entire Department and/or specific programs taking into consideration security and public record concerns;
 - Establish security standards and guidelines;
 - Establish device configuration standards and guidelines; and
 - Establish data storage standards and guidelines, etc.
- 3) Design and implement a mobile workforce education and awareness program to ensure all users are fully informed of the risks and controls surrounding mobile device usage, as well as give “real life” examples of what “not to do” and how to handle various scenarios and situations.
- 4) The short-term methodology above should be expanded beyond cell phones to determine feasibility for all mobile devices such as tablets and laptops for network connectivity (e.g. VPN, email, etc.)
- 5) Revise the definition of Information Technology (IT) Assets in DOHP 250-11-12, *Management of State Property*. The current definition is outdated and does not address all current technologies.
- 6) To ensure DOH has the ability to track mobile devices, design and implement detective monitoring controls to ensure all “IT Assets” are entered into the Property Management System [also referred to as the “Asset Management System” (AMS)].

- 7) Require that all issued mobile technology device be re-approved on a set periodic basis (e.g. yearly, bi-annually, etc.) to ensure the need for the device and the features of the device are still necessary.
- 8) A report issued on April 30, 2012 by the Office of the Chief Inspector General, *Survey Results of Information Technology Mobile Computing in Florida's State Government (Attachment 1)*, reflects that mobile computing has the potential to provide great benefits and efficiencies in government agencies. However, utilization of mobile computing and other mobile communication devices inherently introduces addition risks, including:
 - unauthorized access to networks,
 - loss or compromise of data, and
 - degraded network operations

This is especially important as the benefits of bring your own device (BYOD) is explored as a potentially feasible business solution to maximize cost savings.

Department management should review both the "*Survey Results of Information Technology Mobile Computing in Florida's State Government*" and the draft "*Guidelines on Mobile Devices in Government*" (**Attachment 4**) to familiarize themselves with the threats, vulnerabilities, risks, controls, and compensating controls before designing and/or revising the Departments mobile workforce framework.

Additional Reports To Be Issued Related to Mobile Devices

Currently, the DOH Office of Inspector General is conducting a comprehensive review to evaluate whether select security controls for handheld mobile computing device, laptops and mobile storage devices sufficiently mitigate risks. This review will specifically determine if controls adequately safeguard the confidentiality, integrity and availability of Department data and information technology resources, as well as determine the Department's level of compliance with select mobile device requirements within Chapter 71A-1, Florida Administrative Code, *Florida Information Technology Resource Security Policies and Standards*.

Closing Remarks

Please let us know if you have any questions or thoughts. We are also available to explain or expand upon any of the ideas presented in this document.

EXECUTIVE OFFICE OF THE GOVERNOR



OFFICE OF THE CHIEF INSPECTOR GENERAL



SURVEY RESULTS OF INFORMATION TECHNOLOGY MOBILE COMPUTING IN FLORIDA'S STATE GOVERNMENT

REPORT NUMBER 2012-13

APRIL 30, 2012



RICK SCOTT
GOVERNOR

STATE OF FLORIDA
Office of the Governor

THE CAPITOL
TALLAHASSEE, FLORIDA 32399-0001

www.flgov.com
850-488-7146
850-487-0801 fax

April 30, 2012

The Honorable Rick Scott
Governor of Florida
The Capitol, PL 05
Tallahassee, FL 32399-0001

Dear Governor Scott:

Enclosed is Report Number 2012-13 titled "Survey Results of Information Technology Mobile Computing in Florida's State Government." The report includes the results of the enterprise-wide surveys we conducted and our recommendations. We also developed an Information Technology Mobile Computing Assessment Toolkit for use by the agencies in evaluating internal controls to determine if they sufficiently mitigate the risks associated with agency-owned and managed mobile devices.

I am available to discuss this report with you at your convenience.

Sincerely,

A handwritten signature in blue ink that reads "Melinda M. Miguel".

Melinda M. Miguel
Chief Inspector General

Enclosure

cc: Stephen MacNamara, Chief of Staff
David Martin, Auditor General

Table of Contents

Table of Contents i

Executive Summary i

Background and Introduction 1

State of Mobile Computing – Survey Results 1

State of Mobile Computing Controls..... 2

Considerations for Mobile Computing in Florida’s Government Enterprise 3

Mobile Computing Evaluation Toolkit 5

Conclusion 7

About the Team..... 7

Appendix A – Participating Agencies..... 8

Appendix B – Survey Results Charts 9

Appendix C – Sample Acknowledgement Form 14

Executive Summary

In 2011, the Center for Digital Government¹ (CDG) stated the following about the benefits of mobile computing:²

Far from being an expense, mobile equipment is in many cases more than paying for itself by increasing the amount and quality of work employees can do in the field, reducing government task process time from weeks to days or hours, shortening response time to customers, cutting travel, decreasing equipment expenses and eliminating occupancy costs.

While mobile computing has the potential to provide great benefits to State of Florida government agencies, the practice also presents potential risks to data if not properly managed. The potential risks include unauthorized access to networks, loss or compromise of data and degraded network operations.

While mobile computing has the potential to provide great benefits to the State of Florida, the practice also presents potential risks if not properly managed.

Recognizing these potential risks,³ the Executive Office of the Governor's Office of the Chief Inspector General initiated an assessment⁴ of survey results of the state of mobile computing within the enterprise⁵ and associated management controls. The objectives were to identify mobile computing trends within Florida's state government, identify best practices and assess the effectiveness of the enterprise mobile computing governance framework.

Chief Information Officers (CIO) and 25,960 agency staff from 23 state agencies were surveyed⁶ to solicit information about mobile device controls, guidance, configurations, training and the storage of confidential or exempt information on agency-owned and personally-owned mobile devices.

¹ The Center for Digital Government is a national research and advisory institute on information technology policies and best practices in state and local government. Excerpt is from *A Guide to Mobility in Government*, a supplemental report within the January 2011 issue of Public CIO magazine.

² Mobile computing is the ability to use computing capability without a pre-defined location and/or connection to a network to publish and/or subscribe to information.

³ In June 2011, the Governor's Chief Inspector General issued the State of Florida Inspectors General, Enterprise Audit Plan for Fiscal Year 2011-2012. Through a risk assessment Mobile Computing was identified as a priority.

⁴ The term *assessment* as used in this report refers to the analysis of the survey results only and not additional testing or audit procedures.

⁵ The term *enterprise* as used in this report refers to State of Florida government agencies, particularly those that are under the jurisdiction of the Executive Branch.

⁶ See Appendix A for a list of participating agencies.

The survey responses revealed that agency-owned mobile computing devices⁷ are the devices primarily used within the enterprise and a trend has begun with the use of personally-owned devices. Mobile devices such as smartphones, tablets, and cellphones are being tested and implemented by CIOs to improve business operations, ensure continuity of operations, and reduce costs. Survey results are included as Appendix B.

CIOs and 25,960 agency staff from 23 state agencies were surveyed.

While state agencies have increasingly embraced the many benefits of mobile devices, the governance of mobile devices has not caught up with the growing utilization of these devices. According to the survey, mobile computing governance issues include the following:

- **Mobile Device Usage** - Employees indicated they are using personally-owned devices without the knowledge or approval of their agency.
- **Controls and Guidance** - CIOs indicated that agency controls and guidance⁸ for personally-owned mobile devices are lacking.
- **Data Protection** - CIOs also indicated a lack of data protection, meaning the enterprise may be vulnerable to breaches of confidentiality and integrity due to the access, transmission, storage and disposal of sensitive information.

Based on this assessment, the following actions should be considered to minimize enterprise risk:

- Agencies should establish specific needs-based criteria for determining which employees should be provided agency-owned mobile devices or allowed to use personally-owned devices for state business purposes. This assessment should, at a minimum, consider the following criteria – travel time, availability, network access and emergency response needs.
- Agencies should ensure that mobile device technologies are identified and tested before being deployed for state business purposes. Ideally, agencies should work together to ensure this process is performed efficiently and without undue duplication.
- Agencies should ensure cost-effective procurement of mobile devices and leverage the purchasing power of the enterprise through the Department of Management Services state term contracts for mobile devices and services.⁹

⁷ Mobile computing device – a portable device that can store and/or process data (e.g., laptop, personal digital assistant, certain media players, flash drives/external hard drives, and cellphones.)

⁸ Controls and guidance might include training, authorization, acknowledgement forms and procedures.

- A workgroup of audit, information technology (IT) and legal professionals should evaluate the mobile workforce to ensure that the legal requirements of record retention and public records laws are fully addressed.
- CIO's should adopt application development standards that ensure new system development accommodates mobile computing while minimizing mobile computing risks. Enterprise-wide technologies and agency-specific applications should be developed or modified and integrated with system platforms to accommodate mobile computing.

To assist the enterprise with mitigating the risks identified through this assessment, an IT Mobile Assessment Toolkit¹⁰ was developed by the assessment team. The toolkit is a Microsoft Excel workbook that utilizes IT criteria from Rule 71A-1, Florida Administrative Code (F.A.C.) and the Control Objectives for Information and Related Technology (COBIT) 4.1, created by the Information Systems and Control Association (ISACA)¹¹ to evaluate agency mobile computing controls. Agency CIOs or Inspectors General Offices are encouraged to further evaluate the mobile computing environment within their agency using the toolkit.

⁹ Mobile device services include services which secure, monitor, manage and support mobile devices deployed across mobile operators, service providers and enterprises.

¹⁰ Available on the Florida Inspector's General Webpage, FloridaOIG.com:

http://www.floridaoig.com/library/enterprise/it_mobile_tech/Mobile_Devices_Toolkit.xls

¹¹ ISACA is an independent, nonprofit, global association. ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. ISACA publishes *Control Objectives for Information and Related Technology* (COBIT). COBIT provides a framework of control objectives, management guidelines, and maturity models. COBIT version 4.1 was utilized as a best practice reference during this assessment.

Background and Introduction

The State of Florida has increased the use of agency-owned¹² and personally-owned¹³ mobile devices to provide greater mobility, increase productivity, reduce process time, increase customer responsiveness and reduce the need for travel. The use of these devices is known as mobile computing. Although mobile computing devices¹⁴ have the potential to provide great benefits to the enterprise,¹⁵ their use also presents potential risks and threats if not properly managed. The potential risks of mobile computing include unauthorized access to networks, loss or compromise of data and degraded network operations. Specific threats include lost/stolen devices, device misuse, viruses, malware and network-based attacks.

The State of Florida Inspectors General Enterprise Audit Plan for Fiscal Year 2011-2012¹⁶ identified mobile computing as an enterprise priority due to the potential risks mentioned above. As a result, in accordance with Section 14.32, Florida Statutes (F.S.), the Executive Office of the Governor's Office of the Chief Inspector General initiated an enterprise project to assess the state of mobile computing within Florida's state agencies and associated management controls.

Chief Information Officers (CIOs) and 25,960 agency staff from 23 state agencies were surveyed¹⁷ to solicit information about mobile device controls, guidance, configurations, training and the storage of confidential or exempt information on agency-owned and personally-owned mobile devices.

State of Mobile Computing – Survey Results

Ten of 23 CIOs (43%) surveyed stated their agency only authorizes the use of agency-owned mobile devices. Thirteen of the CIOs (57%) surveyed stated that their agency authorizes both agency-owned and personally-owned devices.

Improved operations, reduced costs, and improved emergency responses were the primary reasons their agency management authorized and implemented mobile devices. Eighty-five percent (85%) of the CIOs from agencies who authorize personally-owned devices cited the ability to reduce costs as their primary reason for authorizing their use. The majority of CIOs indicated they are in the process of testing or implementing tablets¹⁸ and smartphones.¹⁹

¹² Devices owned and managed by the agency.

¹³ Devices owned by the employee.

¹⁴ Mobile computing device – a portable device that can store and/or process data (e.g., laptop, personal digital assistant, certain media players, flash drives/external hard drives, and cellphones).

¹⁵ For the purposes of this assessment, enterprise refers to State of Florida government agencies, particularly those that are under the jurisdiction of the Executive Branch.

¹⁶ State of Florida Inspectors General, Enterprise Audit Plan for Fiscal Year 2011-2012, pp. 1-2.

¹⁷ See Appendix A for a list of participating agencies.

¹⁸ Tablet - a complete computer contained in a touch screen. Tablet computers can be specialized for Internet use only or as a general-purpose personal computer.

More than half of the employee respondents (16,577) indicated they are using mobile computing devices for work-related purposes. Forty-two percent (42%) of employees responded they use agency-owned mobile devices, while 22% responded they use personally-owned mobile devices for work-related purposes.

The overall survey results for the CIOs and employees revealed a trend of an increasing use of personally-owned devices.

Employees responded that the most prevalently used agency-owned devices are laptops, cellphones, and flash drives and the most prevalently used personally-owned devices are smartphones, laptops, and cellphones. Moreover, 44% of employee respondents stated that they would be willing to use their personally-owned devices for work-related purposes.

The overall survey results for the CIOs and employees revealed a trend of an increasing use of personally-owned devices. The trend of using personally-owned mobile devices is likely to continue in Florida’s government agencies as a result of employee preference/willingness and a desire of agency management to reduce costs. This trend is expected to be driven by information technology (IT) consolidation initiatives, workforce reductions, and management initiatives to maximize effectiveness and efficiency within each agency.

State of Mobile Computing Controls

The current state of mobile computing in Florida’s government enterprise necessitates a strong governance framework for mobile devices. However, **agencies have implemented mobile device controls over time to address agency-specific concerns and objectives without the benefit of an enterprise-wide, comprehensive mobile computing governance framework.**

Both CIO and employee survey responses revealed that enterprise governance of mobile devices has not caught up with the growing utilization of these devices. Three significant issues were identified from the survey responses:

- **Mobile Device Usage** – Employees indicated they are using personally-owned devices without the knowledge or approval of their agency. Thirteen agency CIOs (57%) responded that they authorize the use of personally-owned devices. In contrast, employee survey results indicated all 23 agencies have employees using both agency-owned and personally-owned mobile devices.

¹⁹ Smartphone - a high-end mobile phone built on a mobile computing platform, with advanced computing and connectivity ability.

- **Controls and Guidance** – CIOs indicated that agency controls and guidance²⁰ for personally-owned mobile devices are lacking.²¹ The need for more guidance was summarized by one CIO who stated:

“More could be done to train employees on the risks associated with mobile devices. Currently, policies and procedures are distributed that contain more than just mobile policies and the users sign that they have read and understand the policies. Actual training on the policies is done yearly but contains little specific to mobile devices. There are no physical controls in place to prevent the storage of sensitive data that are under the control of the agency or the data centers, so training is tantamount (sic) to the success of the agency in enforcing mobile policies.”

- **Data Protection** – CIOs were asked whether their agency had controls for storing confidential or exempt information on mobile devices. Regarding personally-owned devices, the majority of CIOs (77%) indicated that they either did not know (54%) or did not answer (23%) the question. Regarding agency-owned devices, 45% of the CIOs did not answer the question and 5% did not know.²² With the increasing use of personally-owned devices in the enterprise, CIOs responses or lack thereof are concerning because it may be indicative of a potential risk relative to the storing of confidential and exempt information on mobile devices.



Agencies have implemented mobile device controls over time to address agency-specific concerns and objectives without the benefit of an enterprise-wide, comprehensive mobile computing governance framework.

Considerations for Mobile Computing in Florida’s Government Enterprise

In November 2010, the Agency for Enterprise Information Technology (AEIT) implemented Rule 71A-1, Florida Administrative Code (F.A.C.), entitled *Florida Information Technology Resource Security Policies and Standards*. The purpose of this rule is to document a framework of information security best practices for state agencies, define minimum standards to be used by state agencies to categorize information and information resources, and define minimum security controls for information and information resources. The rule also defines policies and standards for mobile computing practices. These policies and standards are applicable to the Executive Branch agencies and are designed to help ensure that networks and data are

²⁰ Controls and guidance include training, authorization and acknowledgement forms and procedures.

²¹ See Figure 7 of Appendix B.

²² See Figure 8 of Appendix B.

protected. Rule 71A-1, F.A.C., stipulates that each agency develop procedures and configuration requirements to facilitate the management of mobile computing.

To comply with Rule 71A-1, F.A.C., CIOs have implemented some of the following best practices within their respective agencies:

- Mobile device encryption;
- Network security and access controls;
- Mobile device management systems;
- Implementation of a Network Access Control system;²³
- Standardization of the procurement and security configuration processes;
- Password controls;
- Adherence to federal and international security frameworks such as NIST²⁴ and ISO;²⁵ and
- SANS²⁶ best practices.

However, in order to fully comply with Rule 71A-1, F.A.C., each agency's mobile device strategy should include policies/procedures, acknowledgement forms,²⁷ employee training, and logical controls,²⁸ to ensure that potential risks of mobile computing are addressed and managed appropriately. Mobile device policies should not be based on specific evolving technologies but rather on strategies to control user behavior (i.e. education and monitoring) and to address information confidentiality, integrity, and availability when accessing data or distributing government information.

Based on this assessment,²⁹ the following actions should be considered to minimize enterprise risk:

- Agencies should establish specific needs-based criteria for determining which employees should be provided agency-owned mobile devices or allowed to use

²³ Network Access Control (NAC) is an approach to computer network security which restricts access to the network to only authorized devices.

²⁴ NIST – National Institute of Technology Standards is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

²⁵ ISO – International Organization of Standardization is a network of national standards institutes that is responsible for developing and publishing international information systems standards for public and private sector entities.

²⁶ SANS – The SysAdmin, Audit, Network, Security Institute is a cooperative research and education organization that serves as the largest source for information security training and security certification in the world.

²⁷ Acknowledgement forms - a document that is signed by a party to indicate a clear understanding of information (such as standards, policies, procedures, or guidelines). See Appendix C for a sample acknowledgement form.

²⁸ Logical controls - tools used for identification, authentication, authorization, and accountability in computer information systems.

²⁹ The term *assessment* as used in this report refers to the analysis of the survey results only and not additional testing or audit procedures.

personally-owned devices for state business purposes. This assessment should, at a minimum consider the following criteria – travel time, availability, network access and emergency response needs.

- Agencies should ensure that mobile device technologies are identified and tested before being deployed for state business purposes. Ideally, agencies should work together to ensure this process is performed efficiently and without undue duplication.
- Agencies should ensure cost-effective procurement of mobile devices and leverage the state's purchasing power through the Department of Management Services state term contracts for mobile devices and services.³⁰
- A workgroup of audit, IT and legal professionals should evaluate the mobile workforce to ensure that the legal requirements of record retention and public records laws are fully addressed.
- CIO's should adopt application development standards that ensure new system development accommodates mobile computing while minimizing mobile computing risks. Enterprise-wide technologies and agency-specific applications should be developed or modified and integrated with system platforms to accommodate mobile computing.

Mobile Computing Evaluation Toolkit

The assessment team developed an IT Mobile Assessment Toolkit for use by agencies in evaluating agency controls to determine if they sufficiently mitigate the risks associated with agency-owned and managed mobile devices. The toolkit is a Microsoft Excel workbook that utilizes criteria from Rule 71A-1, F.A.C. and the Control Objectives for Information and Related Technology (COBIT) 4.1,³¹ created by the Information Systems and Control Association (ISACA) to evaluate agency mobile computing controls. Specifically, the toolkit provides a framework of control objectives organized by impact zone (i.e. high level subjects) to determine if agency controls safeguard the confidentiality, integrity, and availability of data and information technology resources. The

An IT Mobile Assessment Toolkit and instructions were created by the assessment team to evaluate agency mobile computing controls.

³⁰ Mobile device services includes services which secure, monitor, manage and support mobile devices deployed across mobile operators, service providers and enterprises.

³¹ ISACA is an independent, nonprofit, global association. ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. ISACA publishes *Control Objectives for Information and Related Technology* (COBIT). COBIT provides a framework of control objectives, management guidelines, and maturity models. COBIT version 4.1 was utilized as a best practice reference during this assessment.

toolkit is available on the Florida Inspector's General Webpage, FloridaOIG.com: http://www.floridaoig.com/library/enterprise/it_mobile_tech/Mobile_Devices_Toolkit.xls.

To utilize the toolkit, the assessor will complete the assessment utilizing interviews of individuals performing tasks to satisfy the policy statements, best practices, and regulatory requirements. Once complete, the appropriate management will confirm the accuracy of the assessment. The assessor will incorporate corrections/revisions within the assessment as necessitated through management's confirmation process. An automatically calculated percentage will gauge the impact magnitude of the control objectives and scoring will be provided in summary form in the final report.

Figure 1 – The toolkit includes criteria from 71A, F.A.C. and COBIT 4.1.

ID	Criteria / Guidance	71A F.A.C. Reference	COBIT 4.1 Reference (ITAM)	Doc	Ctrl	Total	%Comp	Compliance Rating
1	The Security Program and supporting policies have been defined to support a controlled implementation of mobile devices.	71A-1.003(1)	DS5.2	1	3	4	67%	Partially Addressed
2	Policy requires a risk assessment before a device is approved for use and a risk assessment update at least annually to determine that new threats are assessed and new technologies considered for deployment.		PO4.8	3	3	6	100%	Addressed
3	Policy requires a centrally managed asset management system for appropriate devices.		DS9.1	0	1	1	17%	Not Addressed
4	Policy defines the types of permitted mobile devices. For example: <ul style="list-style-type: none"> - Smartphones - Laptops, notebooks and netbooks - PDAs - USB devices for storage (thumb drives and MP3/4 devices) and for connectivity (Wi-Fi, Bluetooth, etc.) - Digital cameras 		PO3.4	2	2	4	67%	Partially Addressed
5	Policy addresses the approved applications by device based on data classification and data loss risk.		PO2.3 PO4.9	3	3	6	100%	Addressed

Figure 2 – The toolkit includes the scoring models shown below for policies and procedures as well as controls.

Scoring	
Documentation (Policy and Procedures)	Controls
0 = NO (Documented policy, procedure, or other guidance does not exist)	0 = NO (Controls do not exist)
1 = DEV (Documented policy, procedure, or other guidance is in development 'e.g. draft form')	1 = DEV (Controls are in development 'e.g. current initiative in progress')
2 = PAR (The existing policy, procedure, or other guidance partially addresses the requirement)	2 = PAR (The controls partially address the requirement)
3 = YES (The existing documented policy, procedure, or other guidance is fully implemented and meets the requirement)	3 = YES (Controls are fully implemented and appear to adequately address the requirement)
NA = Not Applicable (Will be used when a requirement does not apply to a specific rule, criteria, or device)	NA = Not Applicable (Will be used when a requirement does not apply to a specific rule, criteria, or device)

Agency CIOs and/or Inspectors General Offices should consider assessing their mobile computing environment using the toolkit as it will allow each agency to further analyze

their specific survey results³² and validate information obtained from their agency's Information Technology Risk Assessment.³³

Conclusion

With proper governance, state agencies can continue to benefit from mobile computing and maintain control of enterprise data. This project has presented agencies with the opportunity to address common vulnerabilities that have been identified throughout State of Florida government agencies. The risks of mobile computing need to be considered and applicable controls applied throughout agencies as the State of Florida continues to rely on technology-based initiatives to accomplish the missions of state government.

About the Team

The IT Mobile Technology assessment team was assembled by the Governor's Chief Inspector General, Melinda Miguel and overseen by Deputy Chief Inspector General, Dawn Case. The team was directed by Joe Maleszewski and Kris Sullivan from the Department of Transportation and consisted of IT auditors from the following agencies: Department of Transportation, Department of Health, and Department of Children and Families. The auditors that participated in the project were Katifani Crum, Karen Calhoun, Michelle Weaver, and Shandyka Strivelli. Technical assistance was provided by Matthew Wells from the Department of Transportation.

³² Each agency was provided their survey results in January 2012.

³³ In accordance with Section 282.318, F.S. each agency is required to "conduct, and update every 3 years, a comprehensive risk analysis to determine the security threats to the data, information, and information technology resources." This analysis, which requires the evaluation of each agency's security posture with requirements of Rule Chapter 71A-1, F.A.C., is reviewed for reasonableness by each agency's Inspector General. It is scheduled for 2012, and is currently being conducted throughout the enterprise.

Appendix A – Participating Agencies

1. Agency for Enterprise Information Technology
2. Agency for Health Care Administration
3. Agency for Persons with Disabilities
4. Department of Business and Professional Regulations
5. Department of Children and Families
6. Department of Corrections
7. Department of Education
8. Department of Elder Affairs
9. Department of Environmental Protection
10. Department of Health
11. Department of Highway Safety and Motor Vehicles
12. Department of Juvenile Justice
13. Department of Lottery
14. Department of Management Services
15. Department of Revenue
16. Department of State
17. Department of Transportation
18. Department of Veterans Affairs
19. Division of Emergency Management
20. Executive Office of the Governor
21. Fish and Wildlife Conservation Commission
22. Florida Department of Law Enforcement
23. Public Service Commission

Appendix B – Survey Results Charts

The IT Mobile Computing surveys were created to determine the following:

- How agency employees are currently using mobile computing.
- What areas of potential risk exist in the enterprise in regards to confidentiality, integrity, and availability.
- Mobile computing best practices that are being used within state agencies.
- CIO's and employee's opinions on the impact of mobile computing on security.

Below are charts of results from the CIO and employee surveys that have been referenced within this report. A complete set of CIO and employee survey results can be accessed at www.floridaoig.com.

- Figure 1 – Devices Authorized within State Agencies
- Figure 2 – Reasons Devices are Authorized within State Agencies
- Figure 3 – Mobile Devices Being Piloted, Tested, or Implemented within State Agencies
- Figure 4 – Mobile Devices Used by Employees
- Figure 5 – Employees Currently Using Personally-owned Devices
- Figure 6 – Employees Willing to Use Personally-owned Devices
- Figure 7 – Number of CIOs with Governance for Mobile Devices
- Figure 8 – Confidential Information Stored on Mobile Devices

Figure 1 - CIO's indicated that both agency-owned and personally-owned devices were utilized within state agencies.

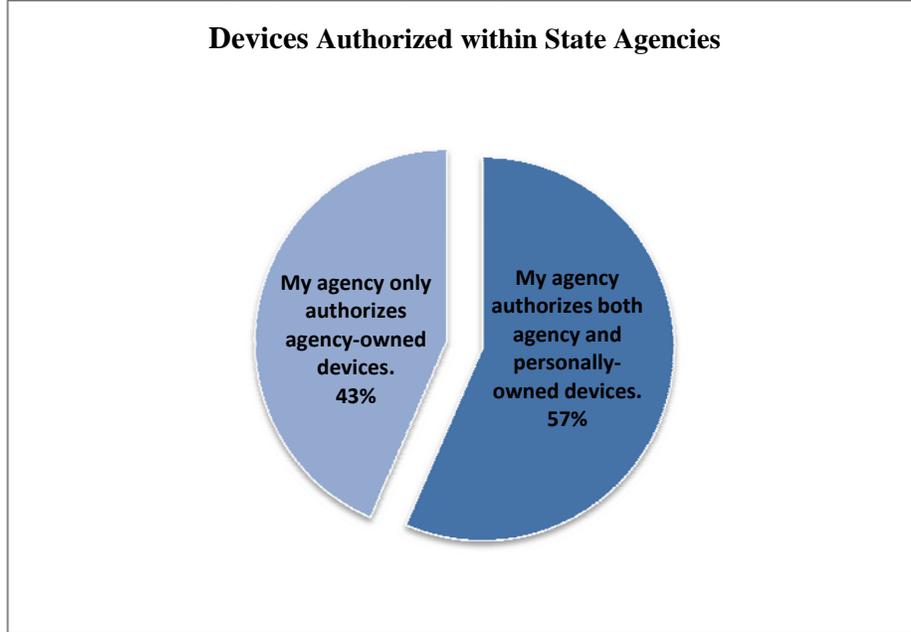


Figure 2 – CIOs cited the following reasons for authorizing agency-owned and personally-owned devices.

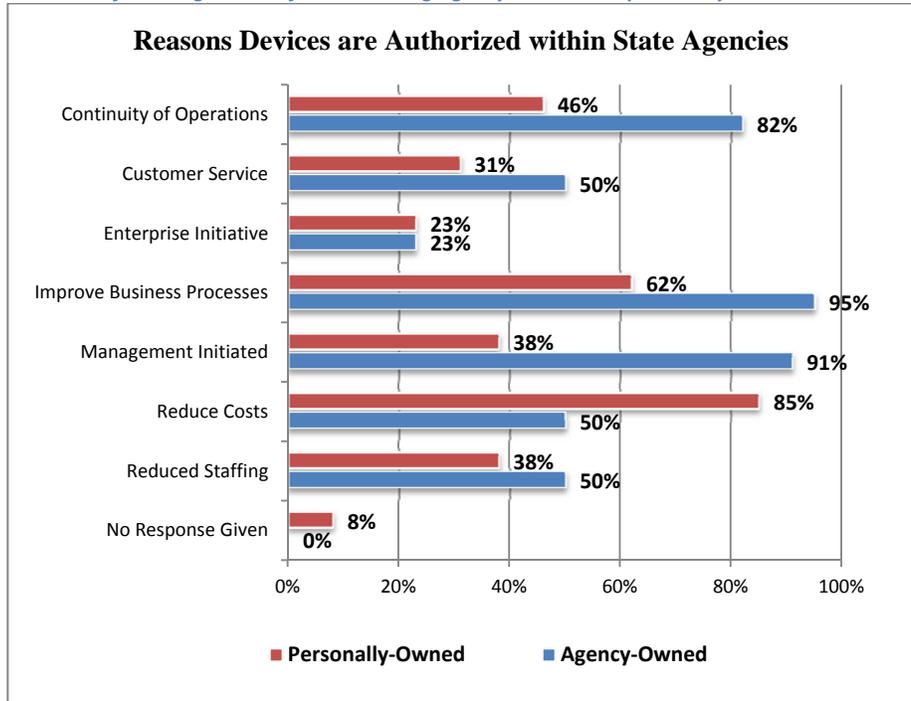


Figure 3 – CIOs indicated they are piloting, testing or implementing the following types of devices.

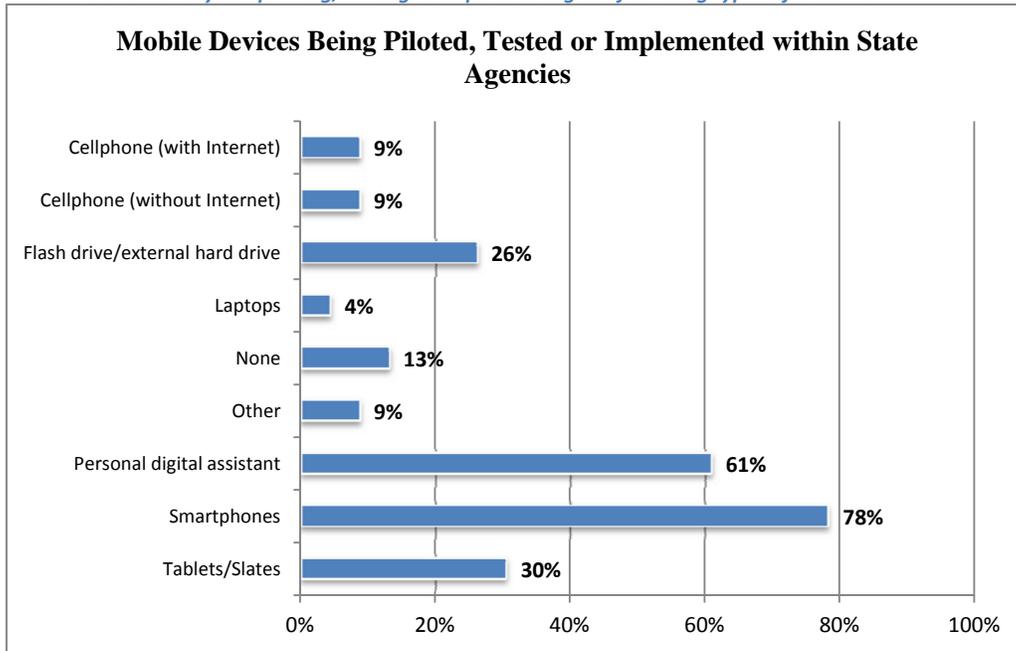


Figure 4 – Employees indicated they use agency-owned and personally-owned devices for work-related purposes. To obtain the percentage of employees using agency-owned devices (42%), “Agency-owned Only” and “Agency-owned and Personally-owned” should be added together. To obtain the percentage of employees using personally-owned devices (22%), “Personally-owned Only” and “Agency-owned and Personally-owned” should be added together.

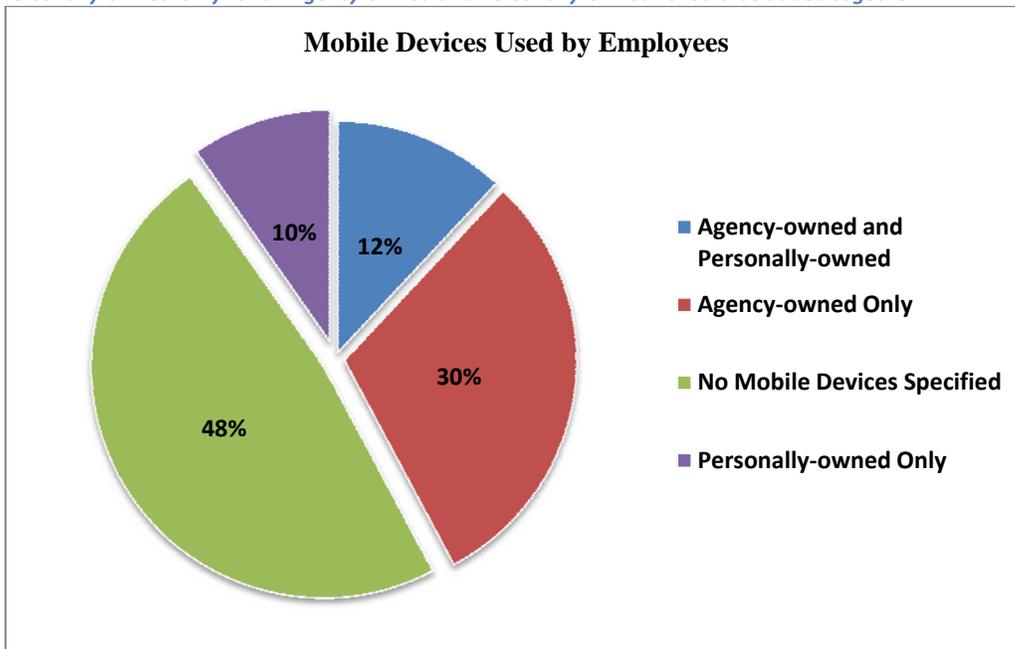


Figure 5 – Twenty-two percent of employees indicated they use personally-owned devices for work-related purposes.

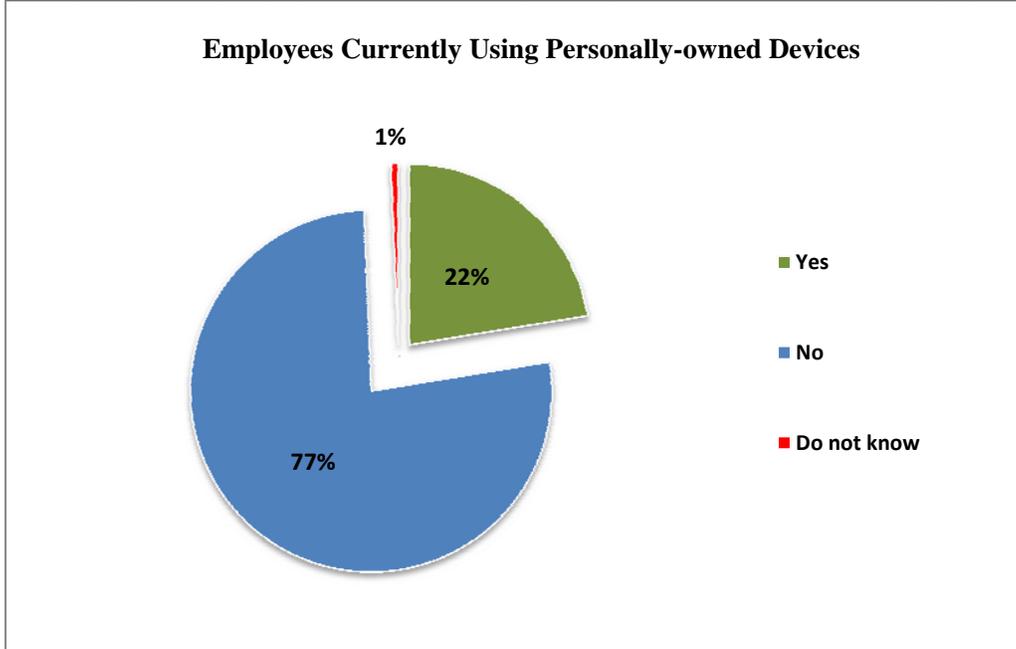


Figure 6 – Forty-four percent of employees are willing to use personally-owned devices for work-related purposes.

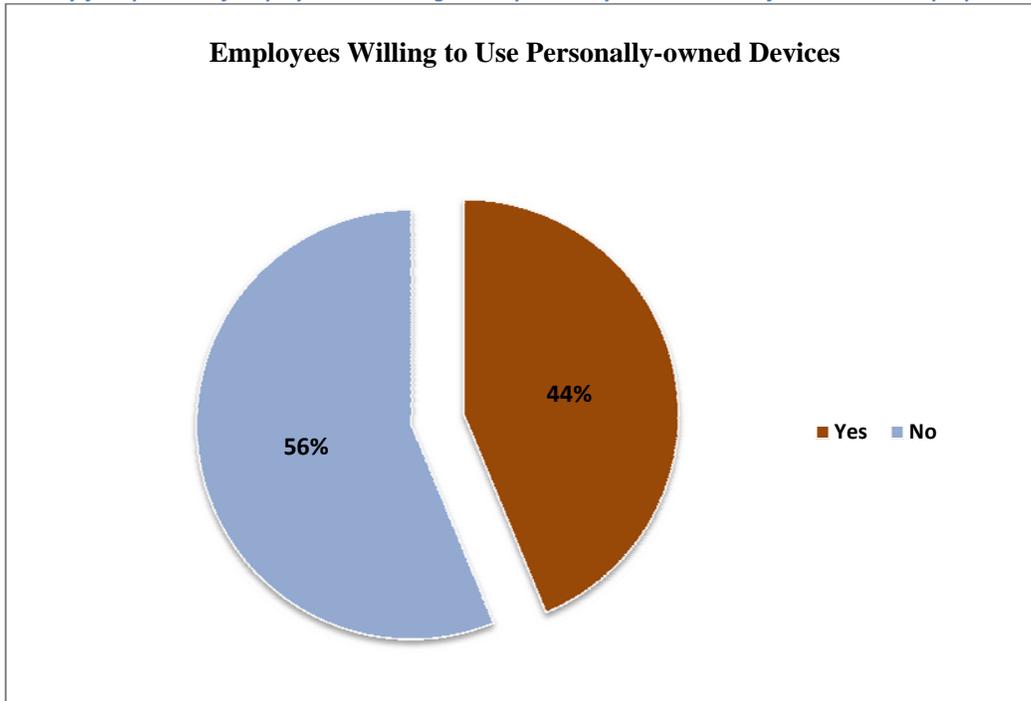
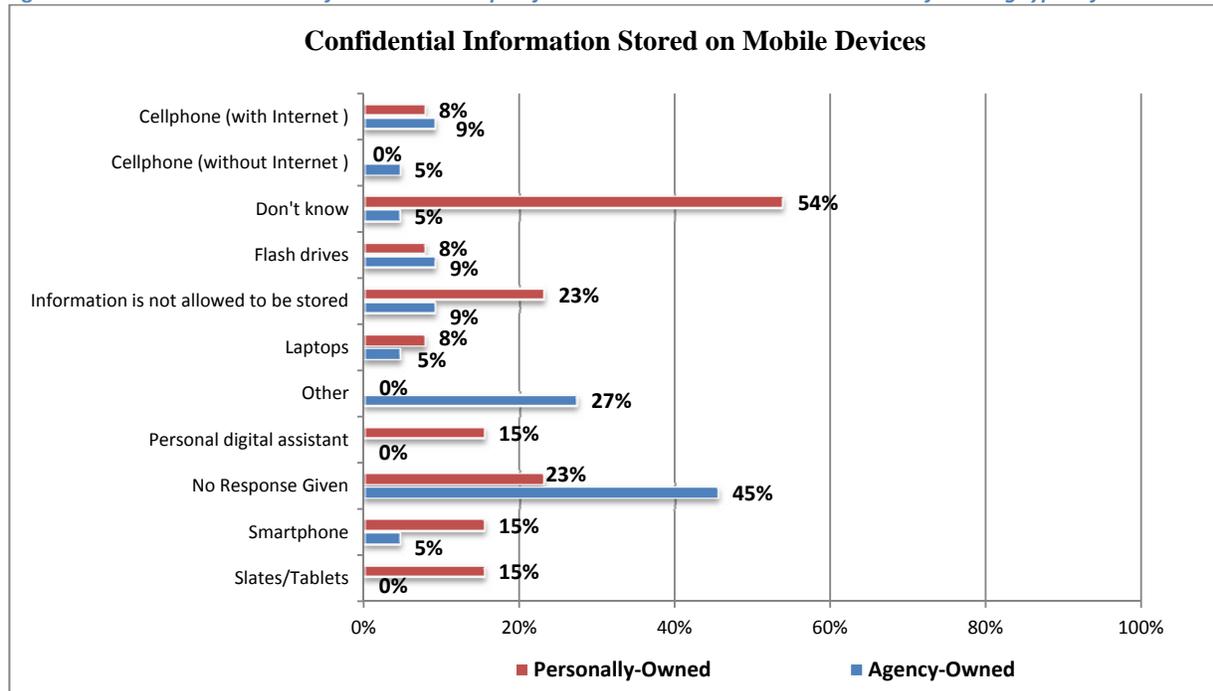


Figure 7 – CIOs indicated that the following types of governance were being utilized within their agencies. The total number of CIOs who responded to this question was 23.

Number of CIOs with Governance for Mobile Devices

Types of Governance	Type of Device	Laptop	Tablet/Slate	Smartphone	Cellphone	Personal digital assistant	Flash drive/external hard drive
Policies	Agency-owned	21	11	20	11	2	14
	Personally-owned	5	5	9	3	1	4
Procedures	Agency-owned	19	9	18	10	2	13
	Personally-owned	3	4	6	1	0	1
Training	Agency-owned	13	7	12	4	2	9
	Personally-owned	1	1	2	1	0	0
Usage Forms	Agency-owned	14	4	10	5	1	6
	Personally-owned	4	4	6	3	0	0
Other	Agency-owned	1	2	1	1	0	1
	Personally-owned	0	0	0	0	0	0
None	Agency-owned	0	1	0	2	1	1
	Personally-owned	3	2	2	4	4	3

Figure 8 – CIOs indicated that confidential or exempt information is allowed to be stored on the following types of devices.



Appendix C – Sample Acknowledgement Form

STATE OF FLORIDA DEPARTMENT OF TRANSPORTATION
**REQUEST TO USE PERSONALLY OWNED COMPUTER
OR MOBILE COMPUTING DEVICE**

Acknowledgment of Security Use and Responsibilities

The purpose of this document is to request to use a personally owned computer or mobile computing device (referred to as "device") to conduct Department related business and the inherent responsibilities associated with such use.

The user will be required to complete **Form No. 325-060-05, FDOT Computer Security Access Request** through the Automated Access Request Form (AARF) system to indicate the type of network connection to be used for the device (ActiveSync, Virtual Private Network, Wi-Fi, Citrix, etc.). Certain types of network access for personally owned devices may be restricted due to security concerns. Access will only be granted through the use of appropriate Department logon credentials, such as an approved USERID and PASSWORD.

Use of personally owned devices is governed by Department policy **Security and Use of Information Technology Resources, Including E-mail, Internet, and Anti-virus Software (Topic No. 001-325-060)**. By signing this document, the owner acknowledges that they have read and understand this policy.

By requesting to use my personally owned device to conduct Department related business, I acknowledge and understand the following provisions:

1. The Department is not responsible for protecting, replacing or repairing my device.
2. I will ensure that my device is properly protected, using anti-virus software with the latest updates and definitions, including real time protection, if available. The Department is **not** responsible for supplying anti-virus software.
3. I will ensure that data exchanged with the Department does not contain viruses or malware.
4. I will ensure that the latest operating system updates are applied to my device, including all applicable security patches.
5. I will ensure that all Department documents or other Department business information stored or maintained on the device will be copied to a Department system or service to meet public records requirements.
6. I will not store any Department confidential or exempt information on my device.
7. All devices connected to the Department's network and systems and used for business purposes will be subject to audit and inspection in the event of a department investigation or public records request.
8. If my device is lost or stolen, I will immediately report it to FDOT Computer Security Administration (email: FDOT Security).
9. If my employment is terminated with the Department, or I choose to temporarily or permanently transfer the ownership of my device, or it is reported lost or stolen, I agree to authorize the Department to remove all of the Department related software, data, e-mail, or any other Department related information from my device.
10. I will comply with state and federal regulations, both existing and future, relating to information technology security and not use this access in any improper or unauthorized manner. Failure to comply may lead to disciplinary action up to and including termination of employment or termination of contracts.
11. If I am eligible to receive overtime pay, I will not use my device to conduct any Department business, including review of Department electronic mail, except during my scheduled work hours, unless I have obtained prior written permission from my supervisor. I understand that any violation of this requirement may result in disciplinary action, including dismissal from my employment with the Department.

I have read and understand the provisions listed above and acknowledge my acceptance by signing below.

Employee Signature

Date

Printed Name



To promote accountability, integrity, and efficiency in government, the Offices of Inspector General audit the programs, activities, and functions of their respective state agency.

This report and other enterprise reports can be obtained from the Office of the Chief Inspector General by telephone (850-717-9264) or by mail (2103 The Capitol, Tallahassee, Florida 32399).

Appendix A



Assignment of Mobile Device Form

User Information

User Name _____ (Smith, Jonathan) E-Mail _____

DOH Network ID _____ (Smith,JX) Training Date _____

User Signature _____ Signature Date _____

I understand that I have thirty (30) days to complete the User Training from the date signed.

Account Information

Account Number _____ (64-37-68-10-XXX) Device Type _____

Account Name _____ (CHD, CMS, or Office) Service Plan _____

Phone Assignment Criteria (please check all that apply)

Managers whose position requires above average travel, have significant program responsibilities, and whose access to a BlackBerry while out of office or not on station would be of significant benefit to the organization; or

Essential staff whose position requires above average travel, have significant program responsibilities, whose access to a BlackBerry while out of office or not on station would be of significant benefit to the organization; and who have the endorsement of their supervisors; or

Staff assigned significant emergency preparedness responsibilities; or

Staff whose duties involve protecting the physical safety of the general public and/or other employees; or

Staff whose duties require additional protection for the employee in potentially hazardous working conditions; or

Staff whose duties directly impact DOH's capability to provide a time-sensitive response to a request for medical care and/or executive and legislative inquiries; or

Staff whose duties require routine mobility, but must be available to respond quickly to email alerts and tasks from automated systems or supervisors.

To assign a mobile device to a user an Assignment of Mobile Device form must be completed properly authorized and emailed to DL.F&A.CPBVS_admins. This form must also be attached to any requisition ordering a mobile device.

(MUST BE APPROVED BY DIVISION DIRECTOR, OFFICE DIRECTOR, COUNTY DIRECTOR/ADMINISTRATOR OR HIGHER)

Supervisor _____ Date _____ Signature _____

Account Manager _____ Date _____ Signature _____

Approved By _____ Date _____ Signature _____

Appendix C



APPLICATION AND ACKNOWLEDGEMENT FORM FOR MOBILE COMMUNICATIONS EQUIPMENT

I, _____, hereby acknowledge my request for: (Print name)

- Cellular Phone - Limited / Unlimited Plan*
Pager (Please circle one)
Lap Top Computer
Personal Digital Device

Justification:

I have read the policies/procedures related to the acquisition and use of Mobile Communications Equipment (MCE), and I agree to abide by the procedures described therein. I further agree to the following:

- 1. The MCE assigned to me, will be used by only me, and will be used primarily for business purposes.
2. If I misuse the MCE, I will be subject to disciplinary action set forth in the department's Discipline Policy, DOHP 60-8-09.
3. I am responsible for the care and usage of the MCE assigned to me. I understand that I am responsible for any damage occurring to this equipment that is determined to be negligence.
4. I will surrender my MCE upon retirement, termination, or upon request of an authorized representative of the department.
5. I will report loss or theft of the MCE to my immediate supervisor, the Service Communications Provider if applicable and the Information Technology Office at (850) 922-7599.

* Division Director or CHD director/administrator's signature is required only if "Unlimited Plan" is selected.

Submit the Application and Acknowledgement form to your designated property custodian.

Applicant's Signature
Date
Phone Number and Extension

Supervisor's Signature
Supervisor's Name (Please Print)
Date

Division Director/
CHD Director/Administrator's Name (Please Print)

Division Director/
CHD Director/Administrator's Signature

Guidelines on Mobile Devices in Government



Recommendations of the
Agency for Enterprise Information Technology

March 2012

DRAFT

Table of Contents

EXECUTIVE SUMMARY	4
1. INTRODUCTION	5
1.1 AUTHORITY.....	5
1.2 SCOPE.....	5
1.3 AUDIENCE	5
2. MOBILE DEVICE TECHNOLOGY OVERVIEW	6
2.1 WHAT ARE MOBILE DEVICES	6
3. SECURITY CONCERNS	7
3.1 COMMON RISKS.....	7
3.2 THREATS	7
3.3 Risks and Threats of Privately-Owned Devices	8
4. RECOMMENDATIONS FOR SECURING MOBILE DEVICES	8
4.1 SECURITY CONTROLS	8
4.2 TECHNICAL CONTROLS	9
TABLE 1 Mobile Device Technical Controls.....	10
5. REFERENCES	11
APPENDIX A - GLOSSARY.....	12
Appendix B – Mobile Device Vulnerabilities and Threats	16
Appendix C - Things to Consider Before Building Your Mobile Device Policy.....	18
Appendix D - Mobile Devices Policy Framework	19

Those who contributed to this guidance:

- **Tom Scott**
- **Karen Calhoun**
- **Mike Clickner**
- **Michelle Weaver**
- **Katifani Crum**
- **Janet Jones**
- **Becky Lackey**

DRAFT

EXECUTIVE SUMMARY

Technology advances during the past 20 years have impacted every facet of the information lifecycle – from how it is collected, to how it is stored, to how it is delivered to businesses, managers, workers, and citizens. Years ago, workers carried pagers that alerted them to call the office for information. Now the information is delivered directly to us and until recently, that delivery was limited to the standard office-issued Blackberry.

Today, more and more people carry smartphones that are more powerful than their work devices and provide anytime access to e-mail, applications (apps), the Internet, and more. Tablet devices (iPads, Xooms, etc.) have similar capabilities and can store even more data. The State of Florida needs to capitalize on the proliferation of these consumer technologies but, at the same time ensure it remains sensitive to the responsibility to protect sensitive state agency information.

While many other states and some Florida agencies strictly forbid the use of mobile devices for work, many other entities are developing policies and solutions that can safely accommodate them. With shrinking state budgets and the ever-growing use of these devices, it makes sound business sense for Florida to embrace the trend and turn it into an advantage. However, the state must take steps to control the higher security risks to the enterprise that come with these tools.

The Florida Information Technology Resource Security Policies and Standards (Ch. 71A-1, F.A.C.) which was promulgated on November 15, 2010, includes security parameters for state use of mobile devices. The business decision to allow personal devices to be used for work is an agency decision that should be considered based on evaluation of risks, benefits, and costs. Furthermore, it is the Agency's responsibility to ensure compliance with the minimum security policies and standards defined 71A-1, F.A.C. to help ensure the agency networks and citizens' data is protected. In instances where an Agency is unable to comply with 71A-1, F.A.C. they may employ compensating controls if the agency documents the analysis results and senior management documents the acceptance of the associated risk. Additional security controls and safeguards that exceed the policies and standards outlined in 71A-1 may be implemented based upon your Agency's risks, authoritative regulations, or security posture.

1. INTRODUCTION

These guidelines propose strategies to more securely use mobile device technologies, mitigate risks, and provide guidance and recommendations to State agencies. The guidelines include recommendations for the creation of a government-wide policy for mobile device technologies that addresses best practices, training, policy controls, and technical controls. Mobile device policies should not be based on specific evolving technologies but rather focus on strategies to control user behavior and to address information confidentiality, integrity, and availability when accessing data or distributing government information. Policies and procedures should be created and updated regularly to address rapid changes in the mobile device environment.

1.1 AUTHORITY

This document is issued pursuant to Chapter 282.318, Florida Statutes, “Enterprise Security of Data and Information Technology Act,” and Florida Administrative Code Rule 71A-1, “Florida Information Technology Resource Security Policies and Standards.”

The Office of Information Security within the Agency for Enterprise Information Technology is statutorily responsible for establishing rules and publishing guidelines for ensuring an appropriate level of security for all data and information technology resources for executive branch agencies.

1.2 SCOPE

These guidelines are intended to help ensure that data accessed via agency-owned and agency-managed mobile devices is secure and that these devices are appropriately managed by outlining “best practices” for their use within Florida state government. While a third category of devices known as privately-owned devices does exist, the risks associated with these devices will only be discussed briefly in Section 3.3 as it is a best practice for agencies to not authorize these devices within their organizations.

This document should be used by organizations to enhance enterprise security by reducing security incidents related to the use of mobile devices. These guidelines present generic principles that may be applied to a variety of organizations and IT infrastructures. The primary tenets of Information Security (Confidentiality, Integrity & Availability) must all be considered when evaluating appropriate security controls related to mobile devices.

1.3 AUDIENCE

This guideline has been prepared for use by State of Florida agencies. The intended audience for this document includes the following:

- ✓ Agency Heads and Senior Management
- ✓ Agency Chief Information Officers
- ✓ Agency Communication Directors and other staff with communication responsibilities
- ✓ Security professionals, including Agency Information Security Managers, other security officers, security administrators, auditors, and others with information technology security responsibilities
- ✓ System and network administrators involved in supporting the security of mobile devices

2. MOBILE DEVICE TECHNOLOGY OVERVIEW

Mobile devices come in many different forms. Many of the risks associated with mobile devices exist because of their biggest benefit: portability. Security managers will need to consider organizational culture, available technology, and governance when creating their mobile device strategy. Mobile devices transport data via wireless networks, which are typically less secure than wired networks. Additionally, many of the mobile devices have storage capability, thus the information gathered from either the interception of data in transit or theft or loss of a mobile device can result in the compromise of sensitive and proprietary information if unencrypted.

Creating an agency mobile device strategy that includes the needed policies/procedures, acknowledgement forms, employee training, and applicable technical controls will help ensure that relevant risks are accounted for and managed appropriately.

2.1 WHAT ARE MOBILE DEVICES

- ✓ Full-featured mobile phones with personal computer-like functionality, or “smartphones”
- ✓ Laptops and netbooks
- ✓ Tablet computers
- ✓ Portable digital assistants (PDAs)
- ✓ Portable Universal Serial Bus (USB) devices for storage (such as “thumb drives” and MP3 devices) and for connectivity (such as Wi-Fi, Bluetooth and HSDPA/UMTS/EDGE/GPRS modem cards)
- ✓ Digital cameras

- ✓ Radio frequency identification (RFID) and mobile RFID (M-RFID) devices for data storage, identification and asset management
- ✓ Infrared-enabled (IrDA) devices such as printers and smart cards (ISACA Doc)

3. SECURITY CONCERNS

The rapid adoption of smartphones, tablets and other mobile devices has added to the risk organizations face when trying to secure critical information technology resources. A single mobile device can allow users to both connect to business as well as personal information resources. Educating the State of Florida workforce on the acceptable uses of mobile devices when accessing business information will assist in managing these risks.

In Florida, agencies subject to federal standards such as HIPAA (Health Insurance Portability and Accountability Act) security or other compliance standards such as PCI (Payment Card Industry) and CJIS (Criminal Justice Information System) could be subject to monetary penalties if certain data is released to unauthorized persons. Also, Florida Statutes addresses breaches of information and actions agencies must take when breaches occur in sections 282.318 and 817.5681.

3.1 COMMON RISKS

- ✓ Breaches of confidentiality and integrity due to the access, transmission, storage and disposal of sensitive information.
- ✓ The loss of availability to critical systems as a result of using an unsecured mobile device.
- ✓ Malware and virus propagation on mobile devices.

3.2 THREATS

Although mobile devices allow agencies to further leverage existing resources and offer highly valued benefits, it is important to understand that these benefits can be realized only if the agency recognizes and addresses the additional associated vulnerabilities and threats.

Deployment of mobile devices and their inherent capabilities can present a significant amount of risk to the overall agency security framework. Mobile devices create numerous vulnerabilities to agencies that make them more susceptible to malicious attacks as well as non-malicious internal threats. The table below presents some known vulnerabilities and associated threats that need to be understood when dealing with mobile devices and the risks they pose to agencies.

Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive

information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. For more information, refer to Appendix B-Mobile Device Vulnerabilities and Threats.

3.3 Risks and Threats of Privately-Owned Devices

Privately-owned devices pose some of the greatest risks to Florida's IT infrastructure and data. All of the risks and threats outlined in this document (particularly in the section entitled Appendix B-Mobile Device Vulnerabilities and Threats) are inherent to privately-owned devices. Moreover, Florida's open-government stance as it relates to data (particularly the Florida Statute 286.011 known as the Sunshine Law) may lead to potential violations of employee's rights that could arise from trying to access, retrieve, or remove agency data from devices that are not owned or managed by the agency. These unique legal implications associated with privately-owned devices are in and of themselves also risks and threats to agencies and should be vetted with each agency's Executive Management in conjunction with the agency's Office of General Counsel. Agencies should be aware that the best way to protect data from breaches associated with privately-owned devices is through the application of compensating controls and user education.

In particular, a primary compensating control is to not allow these devices to access the enterprise IT infrastructure through any other means than secure connection (such as VPN or OWA for email-clients) and agencies should explicitly state this in policies and procedures. Any exceptions should be authorized by Executive Management and documented. This practice cannot by itself ensure that employees do not attempt to access agency data through a privately-owned device. Therefore, agencies should apply a secondary compensating control by training employees on the risks that result from the utilization of privately-owned devices. Each employee's understanding of the agency's standards regarding all mobile device types (and the disciplinary actions associated with these standards) should be documented using an acknowledgement form/agreement or by acknowledging the agency's security policy.

4. RECOMMENDATIONS FOR SECURING MOBILE DEVICES

This section provides a series of topics that are important for agencies to consider when creating mobile device policies. In order to facilitate policy-creation discussions that strongly emphasize security, agencies are encouraged to review each topic with appropriate staff. Mobile devices usually are not under the full physical control of the agency. Agencies will need to consider organizational culture, available technology, and governance when creating their mobile device strategy. The ultimate legality and appropriateness of any final document is the responsibility of each individual agency.

4.1 SECURITY CONTROLS

- ✓ Creating an agency mobile device strategy that includes the needed policies/procedures, employee training, and applicable technical controls will help ensure that relevant risks are accounted for and managed appropriately. This portion of the guidelines is directed towards the state agency that is utilizing mobile devices to carry out the mission of the agency.
- ✓ Protecting data on mobile devices is accomplished in the same manner as protecting data in the agency – through people, processes, and technology.
- ✓ People - We need to educate people on the importance of agency data and the specific things workers must do to protect that information. Workers need to understand that ultimately, the data – whether it resides in a database or in an email on their personal smartphone – is State data, not personal data. If their role involves confidential or exempt information, workers must know their responsibilities and processes specific to using that information.
- ✓ Processes - Agencies need to document the specific processes and configurations they use to support smartphones and other mobile devices.
- ✓ Technology - We need to use technology to monitor devices and make sure configurations are in compliance with standards, and remotely wipe devices if they are stolen or lost. We need to monitor State networks as well to ensure only approved devices connect. There are a number of technical controls that can be implemented to help reduce the security risks that are inherent when using mobile devices. Moreover, finding the right balance—maintaining the integrity and security of the network while allowing easy access to the applications users need to be more productive—will give organizations a competitive advantage in the coming years.¹

4.2 TECHNICAL CONTROLS

Listed in Table 1 are examples of the risks and the technical controls/solutions agencies can implement to mitigate the risk appropriately?

¹ (Carrier, 2010)

TABLE 1 Mobile Device Technical Controls

Risk	Control	Solutions	Compensating Controls
<p>Data in creation – user Interaction with apps and any vulnerability they may have to Malware (viruses, data leakage, and rogue apps) must be minimized.</p>	<p>Use up-to-date anti-malware software on all agency owned and/or agency-managed mobile devices.</p>	<p>Mobile device provided malware solution or third party malware solution.</p>	<p>If no malware solution is available you can do the following:</p> <p>Provide an agency mobile device that is secure.</p> <p>Accept the risk.</p> <p>Restrict the network connection of this mobile device on the network.</p>
<p>Data at rest on device - the ability to protect resident data on the device is imperative, and includes requirements for complex passwords, strong authentication to apps, on-board data encryption.</p>	<p>All agency owned and/or agency-managed mobile devices used with exempt, or confidential information shall require encryption so information is unusable in the event of loss or theft.</p> <p>All agency owned and/or agency-managed mobile computing devices shall require user authentication and have enabled a screensaver secured with a complex password and with the automatic activation feature set at no more than 15 minutes.</p> <p>All agency owned and/or agency-managed mobile computing devices shall require the firewall setting to be enabled by default.</p>	<p>Mobile device encryption solution or third party encryption solution.</p> <p>Mobile device password/screensaver solution or third party password/screensaver solution.</p> <p>Mobile device firewall solution or third party solution.</p>	<p>If no encryption/password/firewall solution is available you can do the following:</p> <p>Provide an agency mobile device that is secure.</p> <p>Restrict the network connection of this mobile device on the network.</p> <p>Accept the risk.</p>
<p>Mobile device physical security – mobile devices must be secured at all times</p>	<p>Mobile device users shall be responsible for securing their mobile devices at all times</p>	<p>Mobile device users will never leave their device unattended for any period of time.</p>	<p>No compensating control for this.</p>

Attachment 4

<p>Data in transit – mobile devices are meant to be connected. Safeguarding data transmission involves encryption and VPN enforcement.</p>	<p>Mobile device users shall/should be connecting to the internal network via a secure connection such as VPN, IP security (IPSec) or Secure Socket Layers (SSL)</p>	<p>Implement an enterprise secure connection solution.</p>	<p>If no enterprise secure connection solution is available you can do the following:</p> <p>Contract with a third party to provide the secure connection.</p> <p>Accept the risks.</p> <p>Restrict the mobile device from transmitting any sensitive or confidential information.</p>
<p>No automated device configuration, settings, remote control for tracking, data wipe, password resets, security updates, and patching.</p>	<p>Each agency should implement a central management solution or manual management solution for all agency owned or agency-managed mobile devices. This management solution should be used for mobile standard device configuration settings, remote control for location tracking, data wipe-out, password resets, security updates, software patching and encryption. This management solution should be used to facilitate device management from installation to retirement.</p>	<p>Central mobile device management solution.</p> <p>Manual mobile device management solution.</p>	<p>Use a manual process of managing the mobile devices or accept the risks.</p>

5. REFERENCES

- Agency for Enterprise Information Technology, Office of Information Security Chapter=71A-1. (n.d.). *FLORIDA INFORMATION TECHNOLOGY RESOURCE SECURITY POLICIES AND STANDARDS*. Retrieved from Florida Administrative Weekly & Florida Administrative Code: <https://www.flrules.org/gateway/ChapterHome.asp?Chapter=71A-1>
- Basso, M., & Simpson, R. (2010). *Critical Capabilities for Enterprise Wireless E-Mail Software*. Gartner Research.
- Carrier, M. (2010, Summer). *iPhone Life Magazine*. Retrieved May 2011, from Managing Personal Devices in the Enterprise: <http://www.iphonelife.com/issues/2010Summer/ManagingPersonalDevices>
- Fisher, E. (2011, January 13). *5 Reasons to Support ActiveSync from Personal Devices*. Retrieved March 2011, from The Email ADMIN: <http://www.theemailadmin.com/2011/01/5-reasons-to-support-activesync-from-personal-devices/>

- Microsoft. (n.d.). *Exchange Server TechCenter*. Retrieved from Microsoft TechNet: <http://technet.microsoft.com/en-us/library/aa996058%28EXCHG.80%29.aspx>
- Ponemon Institute, LLC. (2011, March). *2010 Annual Study: U.S. Coast of a Data Breach*. Retrieved April 2011, from Ponemon Institute: http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach
- Vijayan, J. (2010, August 25). *Computerworld*. Retrieved April 2011, from Infected USB drive blamed for '08 military cyber breach: http://www.computerworld.com/s/article/9181939/Infected_USB_drive_blamed_for_08_military_cyber_breach

APPENDIX A - GLOSSARY

Availability - the principle that authorized users have timely and reliable access to information and information technology resources.

Agency-managed device – A device not owned by the agency, but which the agency ensures the hardware and software used is in compliance with agency standards.

Agency-owned device – A device owned by the agency, which the agency ensures the hardware and software used is in compliance with agency standards.

Anti-malware software – software that detects and removes malicious software from a computer or network stream.

Authentication – The process of verifying that a user is who he or she purports to be. Techniques fall into one of three categories:

- (a) Something the user knows, such as a password or PIN;
- (b) Something the user has, such as a smartcard or ATM card; and
- (c) Something that is part of the user, such as a fingerprint or the iris of the eye.

Chief Information Officer – the person appointed by the agency head that coordinates and manages the agency information technology functions and responsibilities.

CDROM - (Compact Disc Read Only Memory) a compact disc format used to store programs and data files holding either 650MB or 700MB.

Compensating Control – a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control that provides an equivalent or greater level of protection for an information system and the information processed, stored, or transmitted by that system.

Confidential information and/or confidential data - information not subject to inspection by the public that may be released only to those persons and entities designated in Florida statute; information designated as confidential under provisions of federal law or rule.

Confidentiality - the principle that information is accessible only to those authorized.

Directly connect [to the agency internal network] - a device that is joined to and becomes an extension of the agency's internal network. Dial-up and Virtual Private Network (VPN) connections to the agency are considered to be directly connected.

DVD - a digital disc on which images, sounds, or data may be recorded for reproduction by a player connected as to a TV, stereo, or computer; specifically, such a disc on which a film is commercially recorded.

Encryption - the reversible process of transforming readable text into unreadable text (cipher text).

Firewall - a technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts

Integrity - the principle that assures information remains intact, correct, authentic, accurate and complete. Integrity involves preventing unauthorized and improper creation, modification, or destruction of information.

Information technology resources – a broad term that describes a set of technology related assets. While in some cases the term includes items such as people and maintenance, as used in this rule, this term means computer hardware, software, networks, devices, connections, applications, and data.

Integrity- The principle that assures information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information.

Laptop - a microcomputer small and light enough to sit on the user's lap and containing, in a single unit, a keyboard, LCD screen, microprocessor, and, usually, a rechargeable battery.

Malware - malicious software; a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Mobile computing device - a portable device that can process data (e.g., laptop, personal digital assistant, certain media players and cell phones

Mobile device - a general term describing both mobile computing and mobile storage devices.

Mobile device management (MDM) – centrally secures monitors, manages and supports mobile devices deployed across service providers and enterprises. Central functionality includes:

Attachment 4

- Firmware over the air updates
- Diagnostics
- Remote Configuration and Provisioning
- Security
- Backup/Restore
- Network Usage and Support
- Mobile asset tracking and management
- Remote Lock and Wipe
- Device Provisioning
- Software Installation
- Troubleshooting and Diagnostic Tools
- Policy Application
- Logging and Reporting
- Remote Control and Administration
- GPS tracking

Mobile storage device - portable data storage media including external hard drives, thumb drives, floppy disks, recordable compact discs (CD-R/RW), recordable digital videodiscs (DVD-R/RW), or tape drives that may be easily attached to and detached from computing devices.

Mobile Device - is a generic term used to refer to a variety of devices (A portable electronic device, including smartphones, PDAs, laptops, USB drives, DVD/CD ROM, netbooks/notebooks/) that allow people to access data and information from where ever they are.

Netbook - A subnotebook computer used for e-mail and general Web surfing, netbooks have screens in the 8"-10" range but are not suited for intensive tasks such as editing video and large images

Notebook - A laptop computer that weighs in a range from five to seven pounds. The term originated when laptops were routinely more than 10 pounds, and those that became lighter were placed in a special "notebook" category. In practice, notebooks and laptops are synonymous.

PDA - personal digital assistant (PDA), also known as a palmtop computer, or personal data assistant, is a mobile device that functions as a personal information manager. Current PDAs often have the ability to connect to the Internet. A PDA has an electronic visual display, enabling it to include a web browser, but some newer models also have audio capabilities, enabling them to be used as mobile phones or portable media players. Many PDAs can access the Internet, intranets or extranets via Wi-Fi or Wireless Wide Area Networks. Many PDAs employ touch screen technology.

Personal firewall - software installed on a computer or device which helps protect that system against unauthorized incoming or outgoing network traffic.

Privately-owned device - a device not purchased with agency funds; a device owned by a person or other non-agency entity and not configured, maintained, or tracked by the agency. Also known as an employee-owned device.

Attachment 4

Remote access - any access to an agency's internal network through a network, device, or medium that is not controlled by the agency (such as the Internet, public phone line, wireless carriers, or other external connectivity). A virtual private network client connection is an example of remote access.

Remote Wipe - Use of software to destroy data on a mobile device remotely.

Risk - the likelihood that a threat will occur and the potential impact of the threat.

Smartphone - A smartphone is a high-end mobile phone built on a mobile computing platform, with advanced computing and connectivity ability. Today's models also serve to combine the functions of portable media players, low-end compact digital cameras, pocket video cameras, and GPS navigation units. Smartphones typically also include high-resolution touch screens, web browsers that can access and properly display standard web pages rather than just mobile-optimized sites, and high-speed data access via Wi-Fi and mobile broadband.

USB Drive - A flash memory card that plugs into the computer's USB port. Small enough to hook onto a keychain, it emulates a small disk drive and allows data to be easily transferred from one machine to another.

Wireless Network - refers to any type of computer network that is not connected by cables of any kind.

Virtual Private Network (VPN) - a communications network tunneled through another communications network.

Appendix B – Mobile Device Vulnerabilities and Threats

Vulnerabilities and Threats		
Vulnerability	Threat	Risk
<i>Agency information travels across wireless networks, which are often less secure than wired networks.</i>	Malicious outsiders can do harm to the agency. (DOS attack, eavesdropping, unauthorized access)	Information interception resulting in a breach of sensitive data, agency reputation, loss of adherence to regulation, possible fraud, and legal action.
<i>Mobile devices provide users with the opportunity to leave agency boundaries and thereby eliminate many security controls needed to safely conduct business and access applications.</i>	Mobile devices cross boundaries and network perimeters, carrying malware, and can bring this malware into the agency network.	Malware propagation, which may result in data leakage, data corruption and unavailability of necessary data.
<i>Bluetooth technology is very convenient for many users to have hands-free conversations; however, it is often left on and then is discoverable.</i>	Hackers can discover the device and launch an attack.	Device corruption, lost data, call interception, possible exposure of sensitive information.
<i>Unencrypted confidential or sensitive information stored on or transmitted by the device is beyond the control of the agency.</i>	In the event that a malicious outsider intercepts data in transit or steals a device, or if the employee loses the device, the data are readable and usable.	Information interception resulting in a breach of confidential or sensitive data, agency reputation, loss of adherence to regulation, possible fraud, and legal action.
<i>Lost data on any mobile device may affect employee productivity or introduce a business disruption.</i>	Mobile devices may be lost or stolen due to their portability. Data on these devices are not always backed up.	Workers dependent on mobile devices unable to work in the event of broken, lost or stolen devices, and data that are not backed up.
<i>The device has no authentication requirements applied.</i>	In the event that the device is lost or stolen, outsiders can access the device and all of its data.	Data exposure, resulting in damage to the agency, inability to audit, liability and regulation issues.
<i>The agency is not managing the device and addressing the human element or device control issues like entry, configuration, software currency, end of service, and malware.</i>	If no mobile device strategy exists, employees may choose to bring in their own, unsecured devices and take actions inconsistent with agency policy. While these devices may not connect to the virtual private network (VPN), they may interact with e-mail or store sensitive documents.	Data leakage, malware propagation, unknown data loss in the case of device loss or theft. (**)
<i>The device allows for installation of unsigned agency and third-party applications.</i>	Applications may carry malware that propagates trojans or viruses; the applications may also transform the device into a gateway for malicious outsiders to enter the agency network.	Malware propagation, data leakage, intrusion on agency network.
<i>The employees' persons' or personal/physical information privacy not assured.</i>	Malicious or unsolicited outsiders can do harm (physical/economic/social) to the employee or agency, or agency device management could affect personal information.	Loss of or invasion of privacy, legal action resulting from a lack of legal vetting at implementation. (*)
<i>The agency is not poised to hold personnel accountable or adequately conduct investigations (forensics).</i>	Responsible agency personnel unable to enforce policy/procedure/rule/law. Personnel not held accountable (they are public record custodians).	Failed or weak investigations, incomplete public records or subpoena requests, legal action resulting from a lack of legal vetting at implementation. (*)

Attachment 4

<i>The agency does not have an on-going security training program to keep staff aware of threats and trained to address associated security issues.</i>	Malicious or unsolicited outsiders can do harm, data could be leaked or lost, malware propagated.	The agency is unable to defend and control its local network and wireless-accessible resources. (**)
---	---	--

* Agency public records policies and legal counsel should be consulted when addressing any public record or private data concern.

** Device clearing/wiping and/or disposal must be covered in policy and procedure for all devices, regardless of ownership.

*** Agency policies and procedures, with legal counsel oversight, should address acceptable use of non-Agency resources like Twitter, Facebook, or texting on mobile devices.

DRAFT

Appendix C - Things to Consider Before Building Your Mobile Device Policy

- Who will be eligible to use a mobile device?
- Who will support mobile devices?
- What types of devices will be allowed device types (agency-owned devices, agency-managed devices, and/or privately-owned devices)?
- How will device configurations be maintained, updated, and enforced?
- What procurement methods will be used to acquire devices and accessories? Will financial assistance be made available to employees for agency-managed mobile devices?
- Will employees have to reimburse the agency for usage other than that related to State business?
- Within the existing agency IT architecture, what systems/applications/services are allowed on mobile devices?
- How will agency-issued mobile devices be included in your asset management program?
- What tasks or activities will be allowed on the devices?
- How will this policy impact other guidance within your agency?
- What types of authentication and encryption must be present on the devices?
- How can data be securely stored and transmitted?
- Where will data be backed up?
- What will be the mobile device life cycle process (especially termination of use and disposal)?
- What are the legal ramifications of your proposed mobile device program? What are your agency's rights over your data?
- What is your organizations stance on employee privacy on mobile devices?
- Will mobile devices be restricted from certain areas of the agency?
- Will audio recording of meetings using mobile devices is prohibited?
- Will agency-provided devices and network services be allowed access to personal social media services?
- How will the policy impact public records requests?
- Are there any special legal requirements that are unique to your agency that need to be included in the policy?
- What processes and procedures will need to be put in place to enforce the policy?

Appendix D - Mobile Devices Policy Framework

Background

The State of Florida government information technology resources are valuable assets to its citizens; the confidentiality, integrity, and availability of those resources must be protected. The use of mobile devices poses risks to the information they contain, as well as to the devices themselves. Use of mobile devices on non-agency networks poses risks to agency information technology resources upon subsequent connection to the agency network. Therefore, guidance and practices must be in place to secure the data that is accessible via these devices and non-agency networks.

Purpose

The purpose of this mobile device policy is to protect company data and ensure the availability of company computing resources. This policy applies to all salaried employees, outside consultants, partners, and anybody representing a partner. This policy applies to the use of agency-provided mobile devices, agency-managed mobile devices, and privately-owned devices accessing agency information systems and data. Mobile devices should be used on an as-authorized basis for State business.

Authority

Sections 282.318, Florida Statutes (F.S.)

Rule Chapter 71A-1, Florida Administrative Code (F.A.C.)

Reference

(Please reference any other relevant policies/procedures for your agency here)

Policy Objective

To outline appropriate security controls in order to mitigate the security risks presented by using mobile devices.

Policy

Employees are required to adhere to standards that meet or exceed those listed below. Moreover, employees should have no expectation of privacy with respect to the contents of agency-owned and agency-managed information technology resources. Deviations from this policy require a written approval for an exception from the agency head, in consultation with the State Office of Information Security. This policy covers the use of (choose which ones applies): agency-owned devices, agency-managed devices, and/or privately-owned devices. The agency will monitor for unauthorized information technology resources connected to the agency internal network. Failure to comply with this policy may result in access being revoked and disciplinary action, up to and including dismissal.

1. Mobile Device Standards

- 1.1 Mobile devices used for agency business should be authorized by executive management or his/her designee.
- 1.2 Agency-owned mobile devices will be issued to and used by only agency-authorized users.
- 1.3 No privately-owned devices (e.g., MP3 players, thumb drives, printers) should be connected to agency information technology resources without documented agency authorization.
- 1.4 Mobile device users should read and sign an acceptable use statement and/or acknowledgement form for mobile devices.
- 1.4 Applicable security and privacy laws, regulations, executive orders, and policies in the agency facility apply when using or connecting to agency information technology resources from outside the agency facility.
- 1.5 Mobile device should be tracked by the agency and agencies are accountable for mobile devices.
- 1.6 Wireless access into the agency internal network should require user-authentication.
- 1.7 Only agency-owned or agency-managed information mobile device should connect to the agency internal network.
- 1.8 Only agency-approved wireless devices, services, and technologies should be connected to the agency internal network.
- 1.9 Procedures for obtaining remote access should be completed before such access is utilized from a mobile device.
- 1.10 Users should remotely connect computing devices to the agency internal network only through agency-approved, secured remote access methods.
- 1.11 Remote access client connections should not be shared; they are to be used only by the authorized user.
- 1.12 Agency-owned and managed mobile devices should be configured and maintained according to agency standards.
- 1.13 Mobile devices connecting to the agency network should use current and up-to-date anti-malware software.
- 1.14 Mobile devices should activate an agency-approved personal firewall when connected to a non-agency network (where technology permits).
- 1.15 Only agency-approved software should be installed on agency-owned mobile devices.
- 1.16 Mobile devices should require user authentication. All passwords should be unreadable during transmission and storage using appropriate encryption technology (where technology permits).
- 1.17 Mobile devices should be have enabled a screensaver secured with a complex password and with the automatic activation feature set at no more than 15 minutes (where technology permits).
- 1.18 Users should remotely connect mobile devices directly to the agency network only through agency-approved, secured remote access methods.
- 1.19 Only agency-owned or agency-managed mobile storage devices are authorized to store agency data.
- 1.20 To prevent loss of data, agency data stored on mobile devices should be backed up. Users should comply with the agency's backup procedures. Backing up to data stores not owned by the agency is prohibited.
- 1.21 Confidential data should be accessible only to authorized individuals.

Attachment 4

1.22 Mobile devices used to access confidential or exempt information require encryption. Confidential data should not be stored on a mobile device that does not have encryption capabilities.

1.23 Confidential data should be encrypted when transmitted over a network.

1.24 Mobile storage devices with confidential agency data should have encryption technology enabled such that all content resides encrypted.

1.25 Users should take reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage. An employee should maintain adequate physical protection of her/his mobile device, and should not leave the items unattended in public areas, airports, automobiles, in plain sight of others; or in any place where a non-authorized person could have access.

1.26 Users should report theft of mobile devices immediately to the appropriate agency personnel in accordance with the agency's reporting procedures.

1.27 When devices are lost or stolen, the agency reserves the right to execute a remote wipe to remove all data.

1.28 Employees should adhere to the agency's guidelines for acceptable use of email and other messaging resources.

DRAFT