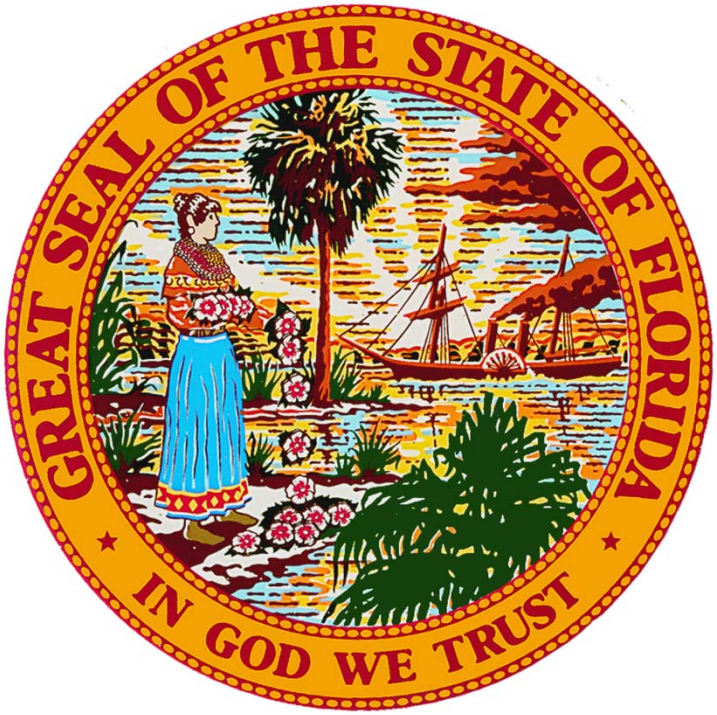
EXECUTIVE OFFICE OF THE GOVERNOR



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

STATE OF FLORIDA

Office of the Governor

THE CAPITOL
TALLAHASSEE, FLORIDA 32399-0001

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

RICK SCOTT
GOVERNOR

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,

Melinda M. Miguel
Chief Inspector General

Enclosure

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

Table of Contents

Executive Summary

In 2011, the Center for Digital Government[1] (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 assessment[4] of survey results of the state of mobile computing within the enterprise[5] 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 surveyed[6] 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 devices[7] 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 guidance[8] 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 Toolkit[10] 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-owned[12] and personally-owned[13] 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 devices[14] 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 2011-2012[16] 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 surveyed[17] 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 tablets[18] 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 guidance[20] 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 NIST[24] and ISO;[25] and
- SANS[26] 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	(IIA)	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%	*Partialy 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: • 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%	*Partialy 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 results[32] 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.*

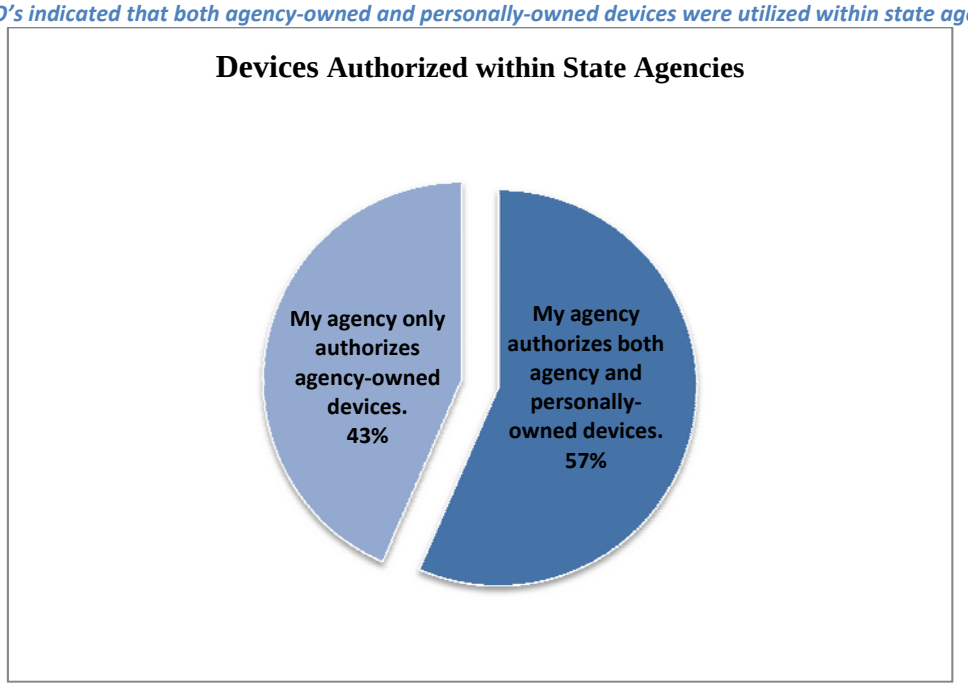


Figure 2 – *CIOs cited the following reasons for authorizing agency-owned and personally-owned devices.*

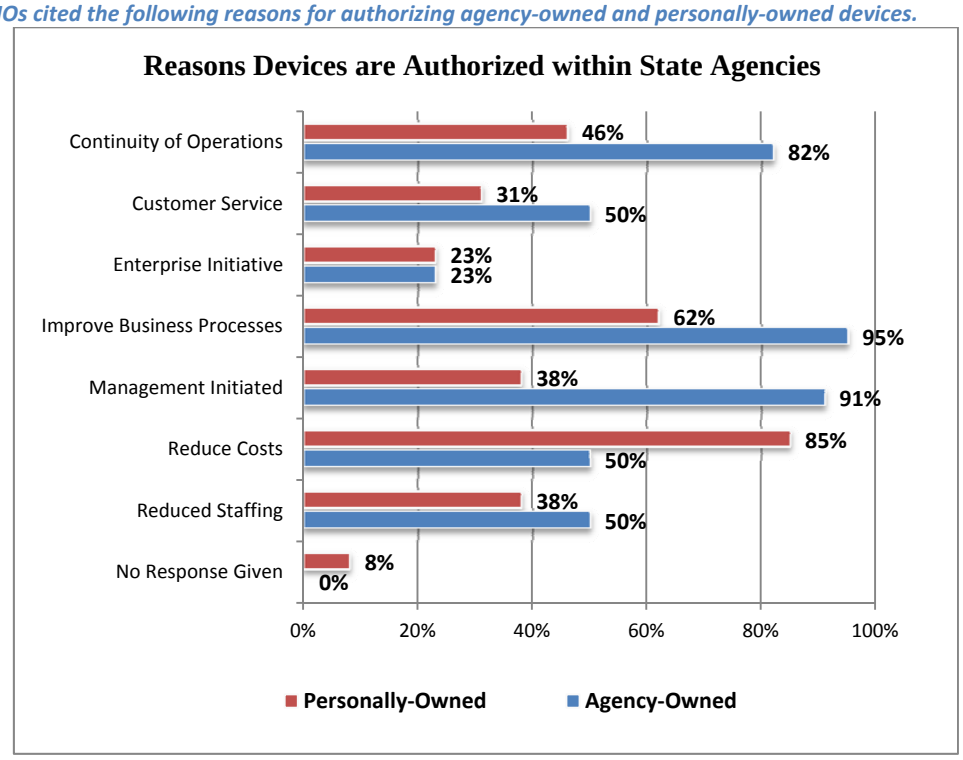


Figure 3 – *CIOs indicated they are piloting, testing or implementing the following types of devices.*

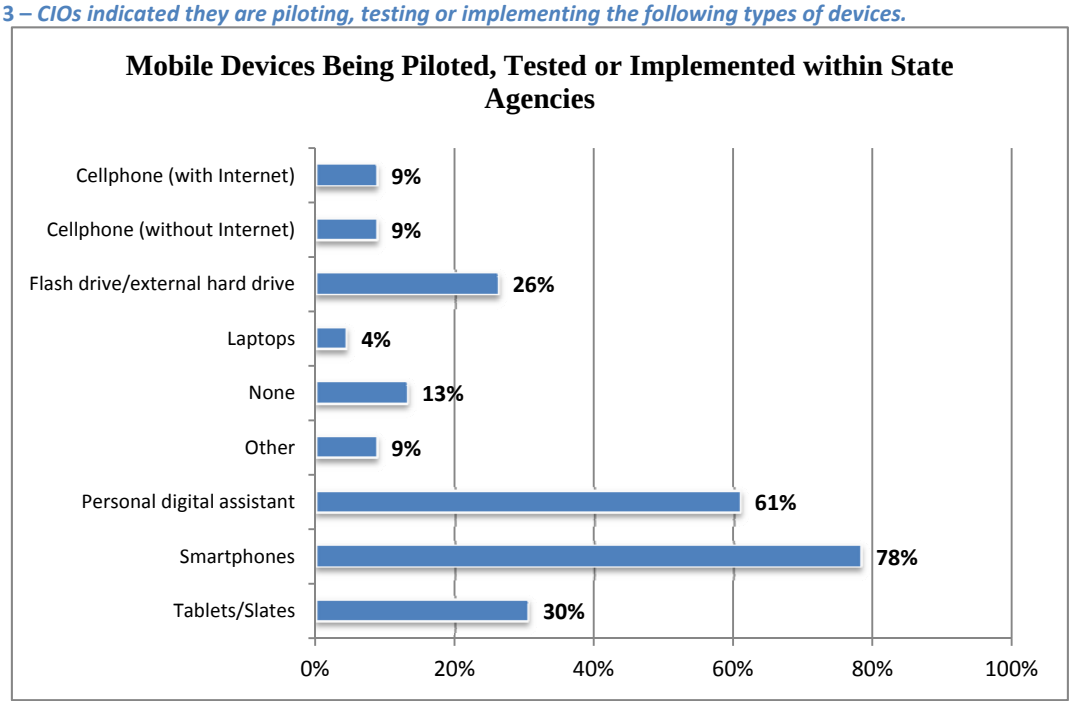


Figure 4 – *Employees indicated they use agency-owned and personally-owned devices for work-related purposes. To obtain the percentage of employees using agency-owned devices (42%), "Agency-owned Only" and "Agency-owned and Personally-owned" should be added together. To obtain the percentage of employees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

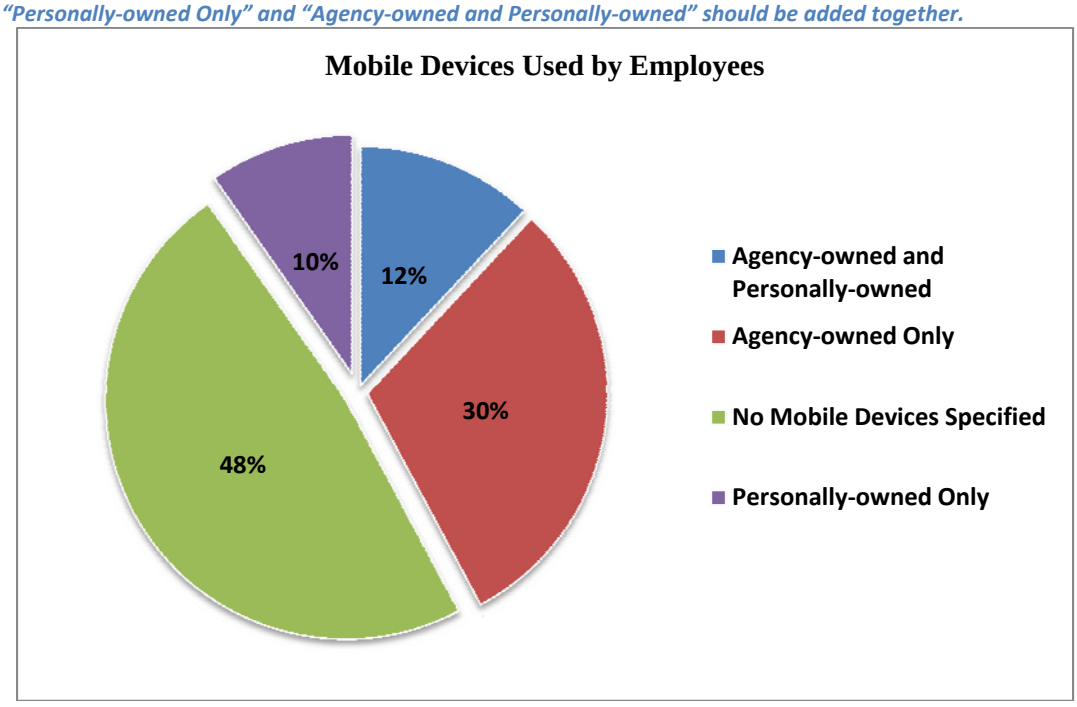


Figure 5 – *Twenty-two percent of employees indicated they use personally-owned devices for work-related purposes.*

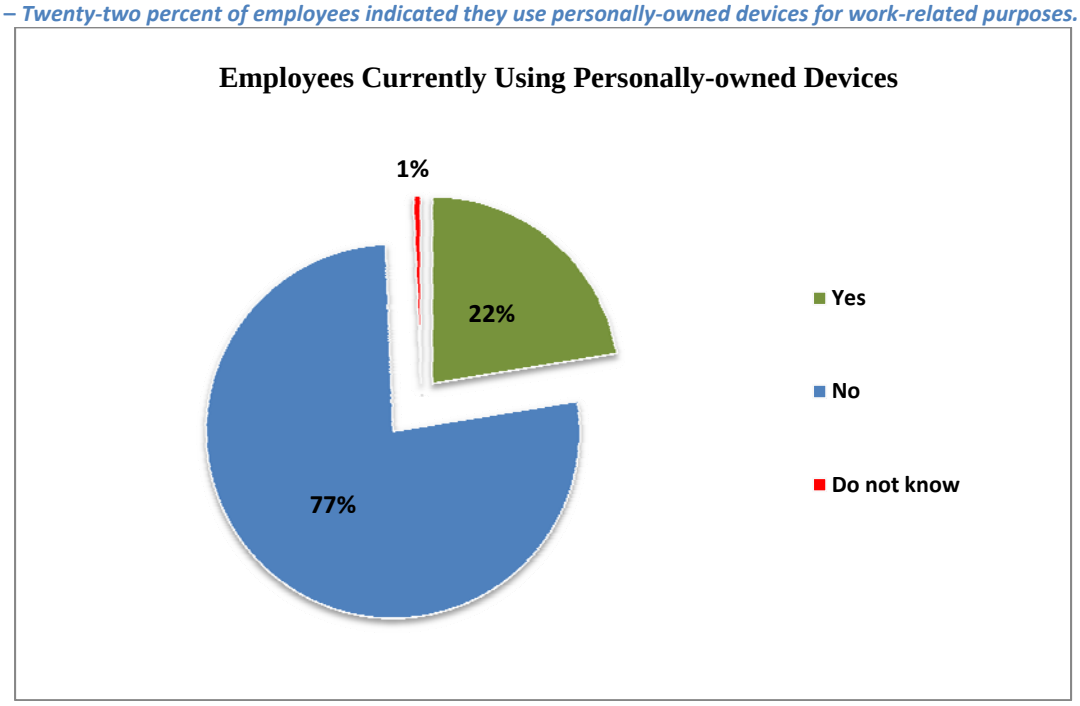


Figure 6 – *Forty-four percent of employees are willing to use personally-owned devices for work-related purposes.*

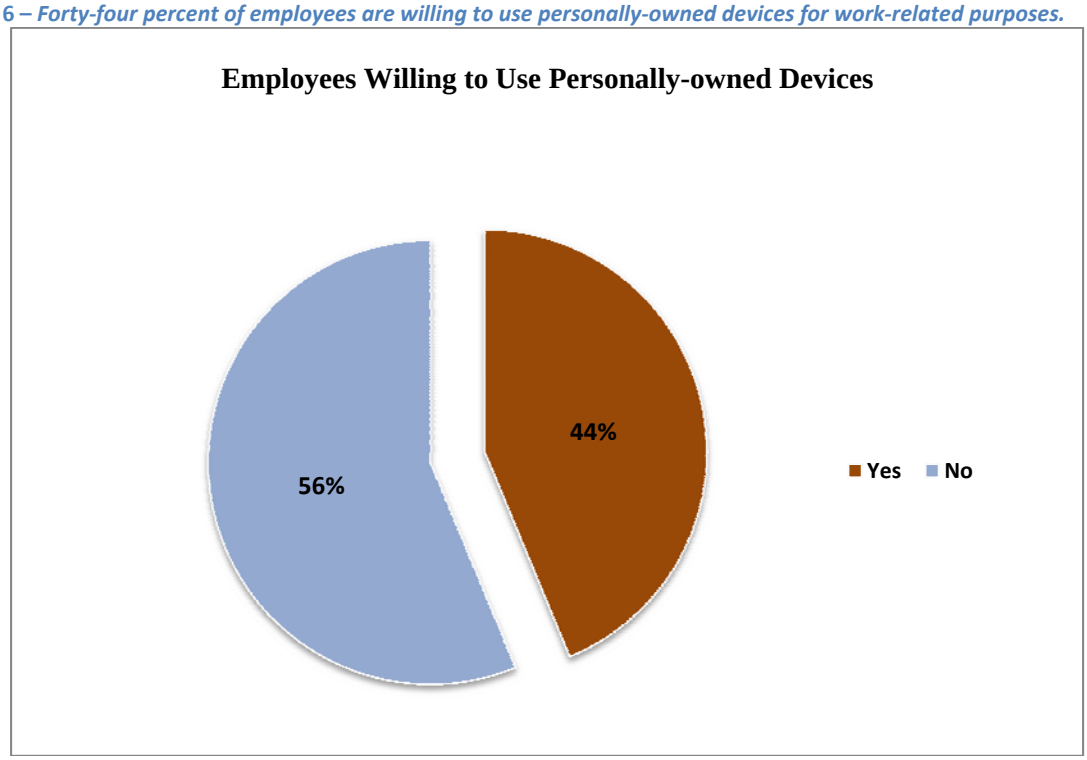
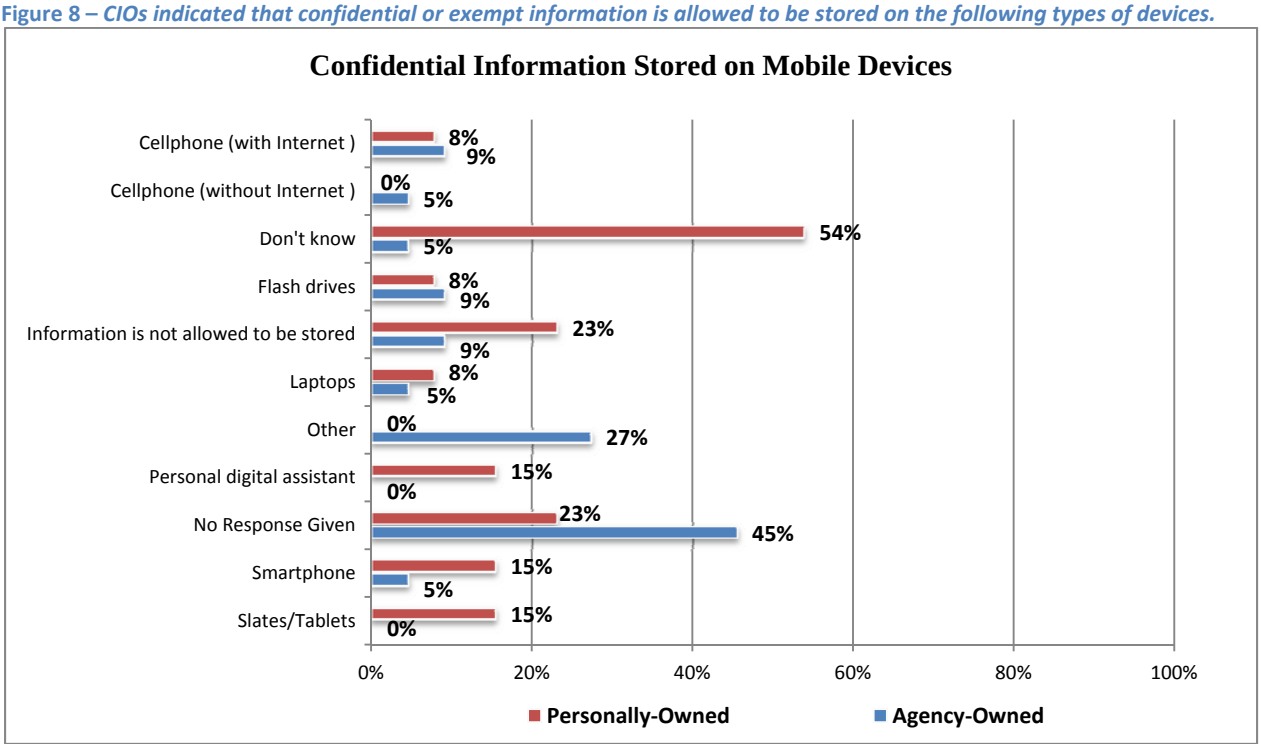


Figure 7 – CIOs indicated that the following types of governance were being utilized within their agencies. The total number of CIOs who responded to this question was 23.

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).