Audit of Mobile Devices - Smartphones

May 14, 2021

Mark S. Swann, City Auditor

City of Dallas

Table of Contents

Executive Summary

Objective and Scope

The objectives of this audit were to determine if:

- Directives and guidance address smartphone usage and risk.
- Smartphones are:
  - Justified for use and formally approved prior to issuance.
  - Physically secured on-site and when held by individuals.
  - Configured to mitigate common threats and vulnerabilities.
  - Monitored through a centralized mobile device management system.
- Smartphone charges are verified and reviewed for reasonableness.

The scope of the audit was smartphone usage from June 2020 to March 2021.

What We Recommend

- Update management directives and governance to reflect emerging risks with the use of smartphones.
- Establish minimum default configuration requirements for smartphones.
- Implement a mobile device management system to validate smartphone configurations.
- Develop easy-to-do monitoring and inventory procedures.

Background

The City of Dallas uses a myriad of mobile devices in daily operations and smartphones were chosen as the mobile device for consideration. Smartphones are approved and paid for by the City of Dallas either as *City Owned* or *City Approved* (Bring Your Own Device) as reimbursement through paycheck. For the fiscal years 2019 and 2020, the cost for *City Owned* smartphones was approximately $6,670,000 and *City Approved* (Bring Your Own Device) reimbursements were approximately $859,000.

Smartphone program, provisioning and lifecycle management is decentralized.

What We Found

Opportunities exist to improve smartphone governance, security, and user management. Specifically,

- Improvements are needed to monitor management's expectations for smartphone usage and limiting potential privacy and data breach vulnerabilities.
- Approval and justification processes are dependent upon each department's procedure, and each department's phone coordinator executes based on their understanding.
- Smartphones are generally issued out of the box with no modifications or restrictions on applications installed, hardware usage installation of anti-virus or anti-malware agents, disabling Bluetooth services, or remote disabling features.
- Billing accuracy reasonableness is difficult to determine because the billing process is separate from the activation/ordering process.

Objectives and Conclusions

1. Do the City of Dallas' directives and guidance address smartphone usage and risk?

   Generally, yes. Administrative Directive 4-08, *Mobile Telephone Services* (last effective date March 1, 2004) and *ITS Enterprise Security Standard* (next review date 10/1/2019), which establish the design elements for the smartphone program's execution, are mostly complete. Improvements are needed to monitor management's expectations for smartphone usage and limit potential privacy and data breach vulnerabilities associated with smartphones. See Observation A.

2. Are smartphones justified for use and formally approved prior to issuance?

   Generally, yes. The process for smartphone approvals and justification is partially achieved. Justification is sometimes documented, and approvals come in various formats: verbally, via email, or internal department form. See Observation C.

3. Are smartphones physically secured on-site and when held by individuals?

   Generally, no. Guidance for smartphones on-premises physical security does not exist and off-site physical security is difficult to determine. Departments handle off-site physical security and reporting of stolen smartphones differently, making it difficult for off-site physical security. See Observation B.

4. Are smartphones configured to mitigate common threats and vulnerabilities?

   No. Smartphones are generally issued out of the box with no modifications or restrictions on applications installed, hardware usage installation of anti-virus or anti-malware agents, disabling Bluetooth services, or remote disabling features. See Observation A.

5. Is smartphone usage monitored through a centralized mobile device management system to validate compliance with City of Dallas approved configurations for applications, operating systems, and patch fixes?

   No. The City of Dallas has not configured smartphones with centralized mobile device management agents. See Observation A.

6. Are smartphone charges verified and reviewed for reasonableness?

   Indeterminable. Billing accuracy reasonableness was difficult to determine because the billing process is separate from the activation/ordering process. While the phone coordinators are responsible for initiating a request and activating a phone, they are often not the person who receive the bills. See Observation C.

Audit Results

As required by *City Council Resolution 88-3428,* departments will establish internal controls in accordance with the standards established by the Comptroller General of the United States pursuant to the *Federal Managers' Financial Integrity Act of 1982.* Administrative Directive 4-09, *Internal Control* prescribes the policy for the City to establish and maintain an internal control system. The audit observations listed are offered to assist management in fulfilling their internal control responsibilities.

Observation A: Smartphone Design, Enforcement, and Configuration

The smartphone program's design, enforcement, and configuration does not facilitate monitoring of management's expectations for smartphone usage and limiting potential privacy and data breach vulnerabilities associated with smartphones. As a result, management may unknowingly support multiple payment methods for a single user's smartphone or foster existing data security vulnerabilities.

Design

Administrative Directive 4-08, *Mobile Telephone Services* allows individuals to use smartphones for City of Dallas business activities in two methods. These methods are executed independently of each other without procedures to determine if users participate in both methods. For instance, an employee can obtain smartphones as follows:

- *City Owned:* Employees can obtain smartphone devices and related plans upon approval and authorization, and all user activity is billed directly to the City of Dallas. The purchase, activation, and billing process are executed solely by department management and is referred to as *City Owned.*
- *City Approved* (Bring Your Own Device): Employees can also use their smartphones and receive a reimbursement/ allowance through their paycheck. This process involves the employee's department supervisor, the City Controller's Office, and the Payroll Division and is referred to as *City Approved* and works similar to a "Bring Your Own Device" program.

Smartphones are approved by department management in both methods and the approval and justification process may not confirm that employees assigned a *City Owned* smartphone are not receiving a *City Approved* payroll allowance simultaneously (see Observation C). Since *City Owned* smartphones are allocated to a department and *City Approved* are managed by the Payroll Division without the department's purview, an employee could participate in both methods.

Verification of the Verizon smartphone listing against the Workday inventory demonstrated that 60 of the 768 *City Approved* personnel also had devices and accounts as *City Owned.* The average cost per month of a smartphone plan is $42 and this could mean the cost for the 60 accounts is $30,240 annually. ($42 x 60 x12).

Enforcement

Administrative Directive 4-08, *Mobile Telephone Services,* which establishes the design elements for smartphone program's execution, and the *ITS Enterprise Security Standard,* which is used to carry out these responsibilities, are mostly complete but not consistently enforced.

For instance, Administrative Directive 4-08, *Mobile Telephone Services*, *Section 5.1* states: "…*The City will only provide cell phones which will be shared by two or more employees, any cell phone assigned to one employee will only be allowed via cell phone allowance program regardless of use.*" This requirement does not match actual practices. As of September 2020, there were approximately 3,400 devices identified as payments for smartphones. With 13,000 employees across the City, the Verizon contract accounts for 26 percent (3,400/13,000) of smartphones in use. The number of smartphones on the AT&T Wireless or FirstNet contract could not be obtained to validate the total number of smartphones in use.

Additionally, Administrative Directive 4-08, *Mobile Telephone Services* and the *ITS Enterprise Security Standard* do not include current security elements for an effective smartphone program. Refer to Exhibit 1 on page 5 to identify threats and vulnerabilities that can be mitigated through the use of available technology features or additional direction on usage of smartphones.

Finally, although the *City Approved* process works like a "Bring Your Own Device" program, the City does not have a Bring Your Own Device policy regulating security and usage of *City Approved* smartphones. *City Approved* smartphones do not currently follow the same security requirements as *City Owned* devices. Refer to Exhibit 1 on Page 5 for further details on missing elements.

Exhibit 1:

Table 1 – Threats and Vulnerabilities

Threats and Vulnerabilities	Administrative Directive 4-08, *Mobile Telephone Services* does not:	*ITS Enterprise Security Standard* does not:
Untrusted Applications, Network, and Content	Specify the type of information employees can access from their smartphones. [1]	Specify the type of information that can be accessed, stored, or transmitted.
	Address risks of downloading unapproved applications, using hardware on smartphones, and using untrusted networks and contents.	Establish rules for downloading unapproved applications, use of hardware, use of untrusted networks, and contents.
Physical Security Weakness	Enforce authentication protocols and establish a specific timeframe for reporting lost, stolen, or damaged smartphones used for City business.	Require minimum authentication protocols. The *ITS Enterprise Security Standard* suggests controls, but they are not required.
	Apply remote wiping/locking of smartphones to all smartphones.	Enforce patching of operating systems.
Improper Provisioning, Management, and Deletion	Address limits of personal usage on a device.[1]	Enforce the approval, justification, and acceptable use of smartphones before issuance through the *Mobile Consent Use Form*, *Cell Phone Allowance Authorization Form*, and confirmation of usage requirements.
Inconsistent Standardization	Specify the types of devices, the security requirements, enrollment/registration of *City Owned* and *City Approved* devices for consistent enforcement.	Specify the types of devices, security requirements, enrollment/registration of *City Owned* and *City Approved* devices to encourage standardization for consistent and improved monitoring.

Sources: Administrative Directive 4-08, *Mobile Telephone Services;* ITS Enterprise Security Standard, Section 21, *General Policy for Mobile Computing Devices*

Configuration

Smartphones are generally issued out of the box with no modifications or restrictions on applications installed, hardware usage installation of anti-virus or anti-malware agents, disabling Bluetooth services, or remote disabling features. Furthermore, the City of Dallas has not configured smartphones with centralized mobile device management agents to validate compliance with City of Dallas approved configurations for applications, operating systems, and patch fixes.

[1] **References:** Dallas City Code, Chapter 34, Personnel Rules, Section 34-36, *Rules of Conduct (b) (9) (C)* and Administrative Directive 2-33, *Acceptable Use of City Provided E-Mail and Internet Services.*

A compensating control is the Department of Information and Technology Services provides annual training to all employees regarding cybersecurity risk; however, the frequency of this training might not sufficiently compensate for the configuration limitations.

Criteria

- National Institute of Standards and Technology 800-124, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*
- Administrative Directive 4-08, *Mobile Telephone Services*
- ITS Enterprise Security Standard, Section 21, *General Policy for Mobile Computing Devices*
- Standards for Internal Control in the Federal Government, *Principle 10 - Control Activities*

Assessed Risk Rating:

High

We recommend the **Director of the Department of Information and Technology Services:**

A.1: Update the smartphone program to consider centralized governance of cost evaluation, work improvement benefits through continued use of smartphones (e.g., improved efficiency, faster response to problems), and justification of smartphone usage at the department or employee level (e.g., role, position, business need).

A.2: Revise Administrative Directive 4-08, *Mobile Telephone Services* to include centralized governance of elements listed in Exhibit 1 and any additional due diligence requirements to demonstrate City of Dallas' accountability of smartphone program.

A.3: Formalize the *City Approved* process as a Bring Your Own Device policy and reinforce management's expectations through Administrative Directive 4-08, *Mobile Telephone Services* and the *ITS Enterprise Security Standard*. If necessary, a separate policy should be created to provide clarity to employees and ensure consistent execution.

A.4: Revise the *ITS Enterprise Security Standard* to address daily execution and administration of smartphone device management including monitoring for privacy and security breaches.

A.5 Establish minimum default configuration requirements for smartphones before issuance for both *City Owned* and *City Approved* devices.

A.6: Implement a centralized mobile device management system that incorporates enterprise ID to validate compliance with smartphone configurations for *City Owned* and *City Approved* devices.

A.7: Consider additional training needs based on employees' smartphone program roles and responsibilities.

Observation B: Lifecycle Management

Smartphone procurement, inventory management, physical security, and disposition processes need to improve. Without additional attention, governance of the smartphone program may be diminished.

Procurement

The City of Dallas has several smartphone contracts, and these contracts are not governed to support cost efficiency, transparency, and consistency. Specifically:

- Cost efficiency: There are eight smartphone contracts with approved contract values of $14,155,298 distributed across the Department of Information and Technology Services, Dallas Water Utilities, Library, and City Attorney's Office. Not all of them are managed by the Department of Information and Technology Services. Therefore, the ability to negotiate a low cost for smartphone procurement is diminished.
- Consistency: Three contracts are providing similar cellular devices and programs. The contracts do not stipulate which cell phone plans, accessories, or optional services (hotspots) apply to the City of Dallas or individual departments, making it difficult to determine which pricing factor will be used for invoice verification. Without an established pricing index, the City cannot hold the vendor or user accountable, and excessive charges will go undetected or ignored for extended periods.

Inventory

A central inventory of smartphones is not available. The Department of Information and Technology Services relies on the vendors Verizon, AT&T Wireless Communication, and FirstNet to track inventory details such as username, assigned phone number, city personnel contact information, and type of device. An analysis of all the Verizon inventory as of September 2020 showed the following:

- 477, or 14 percent of the cell phone accounts have generic names such as *SECURITY PH#4*, *Spare,* and *VACANT OSE LINE.*
- 224, or 6 percent have duplicate user assignments.
- 1,621, or 47 percent are for emergency-related departments. According to the Department of Information Technology and Services, all emergency-related departments must be on the FirstNet contract and emergency network. The Dallas Police Department, Department of Dallas Fire-Rescue, Office of Emergency Management, and the Department of Information and Technology Services were identified as emergency-related departments.

Further review of a random sample of 25 accounts on the Verizon September 2020 listing demonstrated that:

- Nine of the contact email addresses are not current, as these employees no longer serve as phone coordinators.

- Eight additional accounts have the same person but with two different email addresses.
- Three of the usernames are generic accounts. The Department of Information and Technology Services provided information for one of the three generic accounts. The generic account *COVID19 ISSUE 21* has 50 smartphones purchased as spare inventory for the Dallas Police Department.

Physical Security

Guidance for smartphones on-premises physical security does not exist and off-site physical security is difficult to determine. Each phone coordinator can store up to ten new smartphones for immediate use and may receive additional smartphones for safekeeping. The physical security of devices on-site may not be ideal due to limited options for the phone coordinator. Also, departments may handle the off-site physical security and reporting of stolen smartphones differently, making it difficult for off-site physical security.

Disposal

Smartphone scrubbing and/or destruction is not in place. There are no procedures that dictate the baseline for data scrubbing and destruction of chips for certain departments/users of smartphones. This procedural weakness could allow malicious insiders to obtain unauthorized information.

Criteria

- National Institute of Standards and Technology 800-124, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*
- Administrative Directive 4-08, *Mobile Telephone Services*
- Administrative Directive 4-05, Contracting Standards and Procedures (Interim), *Section 15.4.1.*
- Standards for Internal Control in the Federal Government, *Principle 10 – Design Control Activities*

Assessed Risk Rating:

High

We recommend the **Director of the Department of Information and Technology Services:**

B.1: Consider centralized governance of procurement of smartphones to support cost efficiency, transparency, and consistency.

B.2: Implement a mobile device management system which would incorporate the use of an enterprise ID to manage inventory, provide continuous monitoring, and enable emergency shut down for device as deemed necessary.

B.3: Minimize on-site storage locations for smartphones to ensure physical security till they are issued, stored for emergencies, or readied for disposal or destruction.

B.4: Conduct physical security inventories of smartphones at least annually or on a rotating basis.

B.5: Establish destruction procedures for smartphones.

Observation C: User Management

Procedures for approval, justification, deletion, and monitoring of user accounts are not consistently performed. Thus, making it difficult to hold employees accountable if violations of procedures occur.

Justification, Approval, and Deletion

The process for smartphone approvals and justification is partially achieved. Justification is sometimes documented, and approvals come in various formats: verbally, via email, or internal department form.

A random sample of 25 personnel smartphone requests determined that 14 requests were not justified for use. Approvals for the same 25 personnel showed that:

- Fifteen requests for approval were not supported with documentation.
- Eight requests had a form but it was not the form subscribed by Administrative Directive 4-08, *Mobile Telephone Services.*
- One approval was completed through email, and supporting documentation was not available.
- One approval was completed retroactively after the issuance of the smartphone.

A complete population review of all smartphone accounts as of September 2020 identified 174 accounts are associated with employees who are no longer with the City. The City of Dallas is paying on average $42 per account and these accounts are estimated to cost $87,700 annually ($42 x 174 x 12).

Invoice Verification

Billing accuracy reasonableness was difficult to determine because the billing process is separate from the activation/ordering process. While the phone coordinators are responsible for initiating a request and activating a phone, they are often not the person who receive the bills. The bills are sent to other financial coordinators who do not know whether the ordered product and billing amounts match.

Monitoring

Annual reviews of smartphones to verify current device assignments are not performed consistently. A survey of six phone coordinators indicated limited monthly reviews are completed, but the reviews are not similar. Some reviews are focused on excessive usage, and other reviews are focused on the number of accounts. Some are knowledge-based on who should be removed from the list of accounts.

Criteria

- Administrative Directive 4-08, *Mobile Telephone Services*
- Standards for Internal Control in the Federal Government, *Principle 10 – Design Control Activities*

Assessed Risk Rating:

Moderate

We recommend the **Director of the Department of Information and Technology Services:**

C1: Ensure an appropriate level of management reviews the approval and justification for smartphone requests before issuance.

C.2: Develop easy-to-do monitoring procedures that phone coordinators can complete to provide a minimum level of assurance of user accounts through a combination of user access reviews related to provisioning, re-provisioning, and the deletion of user accounts (e.g., checklists, unscheduled reviews with the help of the Department of Information and Technology Services).

Appendix A: Background and Methodology

Background

Mobile device is a broad term, and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-124, Section 2.1, *Defining Mobile Device Characteristics* defines mobile devices as:

- Small form factors.
- One/more wireless network interface(s) for network access (Wi-Fi, cellular networking).
- Non-removable data storage.
- An operating system that is not a full-fledged desktop or laptop operating system.
- Applications are available through multiple methods (web browser, downloads, or installation).

Other characteristics of mobile devices include network services (Bluetooth), Global Positioning Systems (GPS), digital cameras/video recording, microphones, built-in features, and storage.

The primary threats and risks to mobile devices are: (1) lack of physical security controls; (2) use of untrusted mobile devices; (3) use of untrusted networks; (4) use of untrusted applications; and, (5) use of untrusted content. Examples of threats include social engineering attacks such as eavesdropping and shoulder surfing. Other threats are more pervasive: sharing files using Bluetooth, browsing/clicking on the incorrect links, or storing inappropriate content on the mobile device.

Smartphones

The City of Dallas uses mobile devices in various formats, and the characterization of a mobile device can vary across departments, functions, and processes. The list below shows some of the breadth of devices in use:

- Dallas Police Department has e-citation readers.
- Sustainable Development uses iPads for compliance and building specifications.
- Employees and Executives who use cellular devices.
- Dallas Water Utilities has water meter readers.
- Office of Emergency Management has smartphone emergency kits.

Each device provides different services and is designed to meet different activities. To narrow the scope of the audit, the auditor chose cellular devices (smartphones.) Smartphones are ubiquitous in the City of Dallas and can be readily accessed and reviewed.

Design and Structure

The smartphone program is decentralized. Employees can obtain smartphones upon approval and authorization from the City of Dallas and are referred to as *City Owned*. All user activity from *City Owned* smartphones will be billed directly to the City of Dallas. The process of smartphone purchase, activation, and billing is completed solely by the department and its assigned personnel.

Employees can also use their smartphones and receive a reimbursement/allowance through their paycheck. The smartphone allowance process involves the employee's department supervisors, the City Controller's Office, and the Payroll Division. This process is referred to as *City Approved* and works similar to a "Bring Your Own Device" program.

The City of Dallas has eight contracts for cellular devices procurement and relies on the vendor(s) to provide an inventory of smartphones in use. The City of Dallas does not track smartphones in use or available for use. The Department of Information Technology Services estimates that approximately 13,000 devices and related plans are in use.

Operations

The smartphone approval and justification process are dependent upon each department's procedures. As smartphones are provided, each smartphone is equipped with Microsoft Outlook and Workday mobile applications. The employee is asked to acknowledge that the smartphones will not be misused, and internet safety will be followed. There is a recognition that Open Records does apply. The City of Dallas allows employees to use public Wi-Fi and networks and places no Bluetooth technology restrictions. Users can activate and employ basic authentication procedures.

Each department has a phone coordinator responsible for ordering smartphones and delivering them to end-users, activating the smartphones, and disposal of smartphones (e-cycling). Physical security of smartphones on-premises is dependent on the physical location and available physical security measures to the phone coordinator. Financial coordinators of each department complete verification.

Methodology

The audit methodology included: (1) interviewing personnel from the Department of Information and Technology Services and other City departments; (2) reviewing policies and procedures, applicable Administrative Directives, and best practices; and (3) performing various analyses, including benchmarking invoice analysis. All five internal control components of the *Federal Internal Control Standards* were considered in this engagement.

The following documents formed the basis for the audit program's nature and profile, internal controls assessment, and further testing of fieldwork.

- Administrative Directive 4-08, *Mobile Telephone Services*
- ITS Enterprise Standard, Section 21, *General Policy for Mobile Computing Devices*

- Administrative Directive 4-05, *Contracting Standards and Procedures (Interim)*
- Government Accountability Office Report to Congressional Committee 12-757, *Information Security Better Implementation of Controls for Mobile Devices Should be Encouraged*
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-124, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*

The primary testing methodologies for the selected objectives (see above) include confirmation, verification, review of policies and documents. Additionally:

- Analyzing the population of users from different vendors to determine duplicates, generic and multiple users.
- Reviewing a sample of invoices for select employees for accuracy in billing.
- Comparing stipend users with purchases for duplication.
- Reviewing the department procedures for annual reviews.

This performance audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major Contributors to the Report

Bob Smith, CPA, ISA – In-Charge Auditor
Mamatha Sparks, CISA, CRISC, CIA, ISA, – Audit Manager

Appendix B: Management's Response

Memorandum

CITY OF DALLAS

DATE: May 14, 2021

TO: Mark S. Swann, City Auditor

SUBJECT: Response to Audit of Mobile Devices - Smartphones

This letter acknowledges the City Manager's Office received the *Audit of Mobile Devices - Smartphones* and submitted responses to the recommendations in consultation with the Department of Information and Technology Services.

We recognize the importance of maintaining controls over the security and management of smartphones. We concur with the City Auditor's observations that the City provides guidance on smartphone usage and risk, and that smartphones are justified and formally approved prior to issuance.

Additionally, we agree there are opportunities to further align the City's controls over smartphones with industry best practices. To improve the management of smartphones, ITS agrees to:

- Consider centralized governance over the City's smartphone program; and
- Further strengthen City directives and policies related to the procurement and security of smartphones.

However, ITS is unable to agree at this time to four recommendations that require unbudgeted funds to implement. ITS will further research the feasibility of acquiring the tools necessary to successfully implement the recommendations. Additionally, ITS will accept the risk associated with minimizing on-site storage locations for smartphones.

Sincerely,

T.C. Broadnax
City Manager

C: Kimberly Bizor Tolbert, Chief of Staff
M. Elizabeth Reich, Chief Financial Officer
William Zielinski, Director, Information & Technology Services

"Our Product is Service"
Empathy | Ethics | Excellence | Equity

Assessed Risk Rating	Recommendation	Concurrence and Action Plan		Implementation Date	Follow-Up/ Maturity Date
High	We recommend the **Director of the Department of Information and Technology Services:**				
	A.1: Update the smartphone program to consider centralized governance of cost evaluation, work improvement benefits through continued use of smartphones (e.g., improved efficiency, faster response to problems), and justification of smartphone usage at the department or employee level (e.g., role, position, business need).	**Agree:**	The ITS Department shall update and address through AD 4-08 the need and provisioning of smartphones and mobile devices based upon the guidelines, any regulatory compliance need, and security access controls. ITS shall include the centralization of the managed ID to address governance. In addition, ITS shall evaluate the governance of cost evaluation and work improvements, with those document evaluations added to the procedures based upon management approval.	12/31/22	09/30/23
	A.2: Revise Administrative Directive 4-08, *Mobile Telephone Services* to include centralized governance of elements listed in Exhibit 1 and any additional due diligence requirements to demonstrate City of Dallas' accountability of smartphone program.	**Agree:**	The ITS Department shall work with the other appropriate departments, including Budget and Management Services and the Office of Procurement Services to clarify within AD 4-08 the procurement directives for mobile devices. This shall include removal of any security directives from AD 4-08 and place those within the security standards. The revisions to the security standards will address the issues identified within Exhibit 1.	12/31/22	09/30/23

Assessed Risk Rating	Recommendation	Concurrence and Action Plan		Implementation Date	Follow-Up/ Maturity Date
	A.3: Formalize the *City Approved* process as a Bring Your Own Device policy and reinforce management's expectations through Administrative Directive 4-08, *Mobile Telephone Services* and the *ITS Enterprise Security Standard*. If necessary, a separate policy should be created to provide clarity to employees and ensure consistent execution.	**Agree:**	The ITS Department shall add a component within the AD 2-24 to specifically address Bring Your Own Device (BYOD), including drafting BYOD standards that will need to be maintained for the BYOD & City owned devices city data may reside upon.	12/31/22	9/30/23
	A.4: Revise the ITS Enterprise Security Standard to address daily execution and administration of smartphone device management including monitoring for privacy and security breaches.	**Accept Risk:**	The ITS Department agrees in principle to the recommendation, but is unable to agree at this time due to the unbudgeted expenses associated with a Mobile Device Management (MDM) system, necessary for the effective implementation of the recommendation. The ITS Department shall include reference within the Information Security Standard (ISS) to specific standards for the addition of BYOD and the management of data. Additionally, the ITS Department will seek funding for an MDM system and update the ISS to address monitoring activity on BYOD and City-owned devices.	N/A	N/A
	A.5: Establish minimum default configuration requirements for smartphones before issuance for both *City Owned* and *City Approved* devices.	**Agree:**	ITS Security & Compliance Services shall draft MDM Standards to cover City-owned devices and BYOD minimum standards to maintain City data and use on those devices.	09/30/23	6/01/24

Assessed Risk Rating	Recommendation	Concurrence and Action Plan		Implementation Date	Follow-Up/ Maturity Date
	A.6: Implement a centralized mobile device management system that incorporates enterprise ID to validate compliance with smartphone configurations for both *City Owned* and *City Approved* devices.	**Accept Risk:**	The ITS Department agrees in principle to the recommendation, but is unable to agree at this time due to the unbudgeted expenses associated with an MDM system, necessary for the effective implementation of the recommendation. Subject to funding, ITS shall evaluate MDM platforms to address the controls on City owned and BYOD data use within those devices. ITS will work with the Office of Budget and Procurement to evaluate those platforms for budget and necessary procurement.	N/A	N/A
	A.7: Consider additional training needs based on employees' smartphone program roles and responsibilities.	**Agree:**	ITS shall consider additional trainings to assign those users that are allowed BYOD and City owned devices to better address security and compliance with City data existing in on those devices.	09/30/22	09/30/23
High	We recommend the **Director of the Department of Information and Technology Services:**				
	B.1: Consider centralized governance of procurement of smartphones to support cost efficiency, transparency, and consistency.	**Agree:**	ITS shall consider and evaluate the centralization of management of mobile device procurement for cost efficiency, transparency, and consistency.	12/31/22	9/30/23

Assessed Risk Rating	Recommendation	Concurrence and Action Plan		Implementation Date	Follow-Up/ Maturity Date
	B.2: Implement a mobile device management system which would incorporate the use of an enterprise ID to manage inventory, provide continuous monitoring, and enable emergency shut down for device as deemed necessary.	**Accept Risk:**	The ITS Department agrees in principle to the recommendation, but is unable to agree at this time due to the unbudgeted expenses associated with an MDM system, necessary for the effective implementation of the recommendation. Subject to funding, ITS shall create a centralized Enterprise ID to manage the device that will be used within the MDM solution for management and reclamation, including disablement of City-owned devices and the ability to reclaim City data after separation of employment in BYOD data use.	N/A	N/A
	B.3: Minimize on-site storage locations for smartphones to ensure physical security till they are issued, stored for emergencies, or readied for disposal or destruction.	**Accept Risk:**	ITS shall review the current physical storage and attempt to minimize storage locations, including following Recommendation B4 and B5, for all areas.	N/A	N/A
	B.4: Conduct physical security inventories of smartphones at least annually or on a rotating basis.	**Agree:**	ITS shall develop and implement a Standard Operating Procedure for physical inventory evaluation and management.	12/31/22	9/30/23
	B.5: Establish destruction procedures for smartphones.	**Agree:**	ITS shall develop and implement a Standard Operating Procedure for physical inventory evaluation and the destruction of City-owned mobile devices	3/31/23	9/30/23
Moderate	We recommend the **Director of the Department of Information and Technology Services:**				
	C.1: Ensure an appropriate level of management reviews the approval and justification for smartphone requests before issuance.	**Agree:**	As stated above in A.1, ITS shall evaluate the and include the appropriate management approval based upon justification documented in the AD 4-08, with any exceptions identified and documented.	12/31/22	9/30/23

Assessed Risk Rating	Recommendation	Concurrence and Action Plan		Implementation Date	Follow-Up/ Maturity Date
	C.2: Develop easy-to-do monitoring procedures that phone coordinators can complete to provide a minimum level of assurance of user accounts through a combination of user access reviews related to provisioning, re-provisioning, and the deletion of user accounts (e.g., checklists, unscheduled reviews with the help of the Department of Information and Technology Services).	**Accept Risk:**	The ITS Department agrees in principle to the recommendation, but is unable to agree at this time due to the unbudgeted expenses associated with an MDM system, necessary for the efficient implementation of the recommendation. ITS shall develop an easy-to-do monitoring subsequent to implementation of an MDM solution to allow phone coordinators the ability to perform deprovision, deletion of users, and data reclamation, allowing the secure re-provisioning or decommission of a device.	N/A	N/A