Security and Management of Mobile Devices

August 2021 **AUD-21-004**

Audit Report

Audits, Evaluations, and Cyber

☆☆☆☆☆☆☆☆

Integrity☆Independence☆Accuracy☆Objectivity☆Accountability

Executive Summary

Security and Management of Mobile Devices

The Federal Deposit Insurance Corporation (FDIC) deploys nearly 4,600 smartphones and more than 150 tablets to its employees and contractor personnel to support its business operations and communications. Although these mobile devices offer opportunities to improve business productivity, they also introduce the risk of cyber threats that could compromise sensitive FDIC data. The FDIC must implement proper controls to ensure that it effectively manages its inventory of mobile devices and the associated expenditures.

The FDIC uses a cloud-based mobile device management (MDM) solution to secure and manage its smartphones and tablets. The MDM solution performs a number of important functions, such as connecting mobile devices to the FDIC's network, monitoring the security and configuration settings on the devices, and erasing sensitive FDIC data on the devices when users report them as lost or stolen.

The FDIC Office of Inspector General engaged the professional services firm of Cotton & Company LLP (Cotton & Company) to conduct the audit. The audit objective was to determine whether the FDIC had established and implemented effective controls to secure and manage its mobile devices. The audit identified nine areas to review: Policies, Procedures, and Guidance; Awareness Training; Control Assessments; Logging and Monitoring; Billing Analysis; Configuration Management; Asset Management; Incident Response; and Data Protection.

Results

The audit found that the FDIC had not established or implemented effective controls and practices to secure and manage its mobile devices in three of the nine areas assessed because the controls and practices did not comply with relevant Federal or FDIC requirements and guidance. Specifically, the audit determined that:

- FDIC policies, procedures, and guidance were outdated and did not reflect current business practices pertaining to mobile devices, and they did not address key elements recommended by the National Institute of Standards and Technology (NIST). For example, FDIC policies did not address the Bring Your Own Device (BYOD) program nor the risks associated with personal use of FDIC-furnished mobile devices, such as downloading and using non-work related applications, and texting, messaging, and video.

- The FDIC did not conduct Control Assessments of the MDM solution annually in order to ensure that controls were effective and operating as intended.

- FDIC Logging and Monitoring practices were not guided by written procedures and did not provide for adequate separation of duties.

Controls and practices in the areas of Awareness Training, Billing Analysis, and Configuration Management were partially effective because they complied with some, but not all, relevant security requirements and guidelines. For example, the FDIC did not develop written procedures for testing software updates to its mobile devices or complete testing of software updates before allowing users to download and install them.

The FDIC implemented effective controls and practices in the areas of Asset Management, Incident Response, and Data Protection.

Recommendations

The report contains nine recommendations. The report recommends that the FDIC fully assess the risks associated with its mobile devices; establish mobile device policies and guidance consistent with NIST guidance; and require BYOD users to sign service agreements. The report also recommends that the FDIC strengthen awareness training pertaining to the use of mobile devices and define roles, responsibilities, and procedures for reviewing logs generated by the MDM solution. In addition, the report recommends that the FDIC routinely report mobile device usage information to FDIC business units and require them to suspend or terminate service for devices that are no longer needed. By implementing this recommendation, we estimate that the FDIC can achieve cost savings. Finally, the report recommends that the FDIC develop and implement written roles, responsibilities, and procedures for testing software updates for mobile devices. The FDIC concurred with all nine of the report's recommendations and plans to complete corrective actions by May 30, 2022.

Contents

Part I

☆☆☆☆☆☆☆☆

Report by Cotton & Company LLP

SECURITY AND MANAGEMENT OF MOBILE DEVICES

AUDIT REPORT

July 29, 2021

Cotton & Company LLP
333 John Carlyle Street
Suite 500
Alexandria, Virginia 22314
703.836.6701 | 703.836.0941, fax
lschwartz@cottoncpa.com | www.cottoncpa.com

Table of Contents

Cotton & Company
Answers Questioned

333 John Carlyle Street, Suite 500 | Alexandria, VA 22314
P: 703.836.6701 | F: 703.836.0941 | www.cottoncpa.com

Terry L. Gibson
Assistant Inspector General for Audits, Evaluations, and Cyber
Office of Inspector General
Federal Deposit Insurance Corporation

Subject: Audit of the Federal Deposit Insurance Corporation's Security and Management of Mobile Devices

Cotton & Company LLP (Cotton & Company) is pleased to submit the attached report detailing the results of our performance audit of the Federal Deposit Insurance Corporation's (FDIC) security and management of mobile devices. The FDIC Office of Inspector General engaged Cotton & Company to conduct this performance audit pursuant to Contract Number CORHQ-18-G-0479. We performed the work from July 2019 through April 2021.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (2018 Revision) promulgated by the Comptroller General of the United States. The 2018 Revision to the standards became effective for performance audits beginning on or after July 1, 2019. The standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Sincerely,

Loren Schwartz, CPA, CISSP, CISA
Partner

Introduction

The Federal Deposit Insurance Corporation (FDIC) deploys nearly 4,600 smartphones and more than 150 tablets to its employees and contractor personnel, and it relies heavily on mobile devices (smartphones and tablets) to support its business operations and communications. For example, FDIC executives, managers, and staff use mobile devices to access sensitive information, including personally identifiable information (PII),[1] stored on the FDIC's internal network. FDIC personnel also use mobile devices to exchange emails on bank examinations, bank closings, human resources issues, and other sensitive business activities. In addition, FDIC personnel have the ability to use their smartphones as a personal hotspot to access the FDIC's internal network via their laptop computers. The ability of FDIC personnel to reliably and securely communicate sensitive information and access the internal network through mobile devices is critically important, particularly during a pandemic or other emergency situation in which FDIC personnel are working remotely and do not have access to FDIC facilities.

Although mobile devices can improve business productivity, they also introduce the risk of cyber threats. Such threats include malicious software known as "malware" that can allow a malicious actor to exploit vulnerabilities on the devices; eavesdropping of wireless communications over public Wi-Fi networks; and mobile applications installed by users that can collect and monitor data, such as the user's location, contacts, and browsing history. If not mitigated, such cyber threats have the potential to compromise sensitive FDIC data that may exist outside the FDIC implemented secure container.[2] Further, the FDIC must implement proper controls to ensure that it effectively manages its inventory of mobile devices and associated expenditures.

Background

The FDIC's Chief Information Officer Organization (CIOO) uses a cloud-based mobile device management (MDM) solution to perform a number of information technology (IT) functions, such as connecting mobile devices to the internal network, monitoring the security and configuration settings on mobile devices,[3] and wiping the devices when users report them as lost or stolen. The MDM solution also

[1] FDIC Circular 1360.9, *Protecting Sensitive Information* (April 2007), defines sensitive information as "[a]ny information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of FDIC in carrying out its programs or the privacy to which individuals are entitled." Office of Management and Budget (OMB) Circular Number A-130, *Managing Information as a Strategic Resource* (OMB Circular A-130) (July 2016), defines PII as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."

[2] NIST IT Laboratory, *Computer Security Resource Center Glossary,* https://csrc.nist.gov/glossary, defines a container as "a method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container."

[3] The MDM solution monitors each mobile device connected to the FDIC's internal network for compliance with pre-defined rules that define minimum security and configuration requirements for the devices. For example, the MDM solution monitors the version of the manufacturer's operating system installed on each mobile device. If the MDM solution identifies a mobile device running an outdated operating system, the CIOO can use the MDM solution to prevent the device from operating on the network.

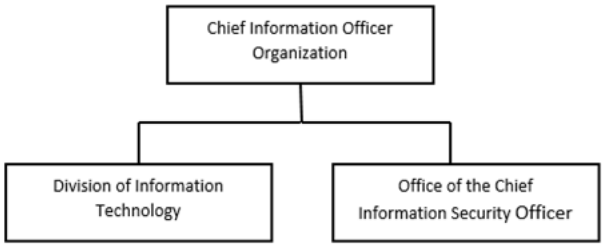
secures certain FDIC applications, such as Email, Calendar, Contacts, and Tasks, in an encrypted container on the mobile devices.

As of May 29, 2020, the FDIC had deployed 4,588 smartphones and 159 tablets to its employees and contractor personnel. More than 99 percent of these mobile devices were equipment furnished by the FDIC, known as Corporate Owned Personally Enabled (COPE) devices. The FDIC purchases both the hardware and the voice and data services for COPE devices from commercial telecommunications carriers. The remaining 37 mobile devices (less than 1 percent) were non-FDIC issued equipment referred to as Bring Your Own Device (BYOD). Employees own BYOD and pay for their own voice and data services. Before employees can use BYOD at the FDIC, the CIOO must install the MDM solution on the device to secure the FDIC's systems and data.

Roles and Responsibilities

Within the FDIC, the CIOO has overall responsibility for IT governance, investments, program management, and information security. As reflected in Figure 1, the CIOO consists of two component organizations: the Division of Information Technology (DIT) and the Office of the Chief Information Security Officer (OCISO). DIT has primary responsibility for the day-to-day operational support and management of the FDIC's information systems and IT infrastructure. The OCISO has primary responsibility for the planning, development, and implementation of an agency-wide information security program, thus fulfilling the FDIC's responsibilities under the Federal Information Security Modernization Act of 2014 (FISMA).[4]

Figure 1: CIOO Organizational Structure



Source: Cotton & Company's analysis of the CIOO's Website.

DIT's End User Computing Section (EUCS) and the OCISO oversee the security and management of FDIC's mobile devices.

> **EUCS** has responsibility for managing mobile devices. This includes overseeing the provisioning, monitoring, testing, de-provisioning, and disposal of mobile devices; implementing the MDM solution; managing the configuration of mobile devices; supporting the DIT helpdesk in resolving service calls for mobile devices; and reviewing vendor billings submitted by telecommunications service carriers.

[4] Pub. L. No. 113-283 (December 2014), codified at 44 U.S.C. § 3554 et seq. The FDIC has determined that FISMA is legally binding on the FDIC.

OCISO provides security oversight of mobile devices. This includes performing security and privacy control assessments to determine the security posture of the MDM solution, including its compliance with government-wide security requirements and guidance. The OCISO uses the results of these security control assessments to identify and address security weaknesses and to inform key risk management decisions, such as authorizing the MDM solution to operate in the FDIC's IT environment.[5]

Federal Security Standards and Guidelines

The FISMA statute requires the National Institute of Standards and Technology (NIST) to develop risk-based standards and guidelines to assist Federal agencies in defining security requirements for their information and information systems. NIST issues standards in the form of Federal Information Processing Standards (FIPS) publications and guidance in the form of Special Publications (SP). NIST FIPS and SPs provide Federal agencies with a framework for developing appropriate controls over the confidentiality, integrity, and availability of their information and information systems.[6]

NIST SP 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (June 2013), identifies security concerns associated with mobile devices and provides recommendations to help organizations secure their mobile devices. The recommendations in NIST SP 800-124, Rev. 1, complement the guidance in NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013).[7] NIST SP-800-53, Rev. 4, contains a comprehensive catalog of recommended security and privacy controls for Federal information systems and organizations. Organizations can customize and implement the security controls in NIST SP 800-53, Rev. 4, as part of an organization-wide process for managing information security and privacy risk.

Audit Objective

The objective of this performance audit was to determine whether the FDIC had established and implemented effective controls to secure and manage its mobile devices. The audit focused on two types of mobile devices in the FDIC's IT environment: smartphones and tablets.

---

[5] OMB Circular A-130 requires Federal agencies to authorize their information systems to operate. A senior management official (the Authorizing Official) reviews security-related information describing the security posture of an information system, and using that information, determines whether the risk to mission/business operations is acceptable. If the Authorizing Official determines that the risk is acceptable, then the official explicitly accepts the risk. At the FDIC, the Chief Information Officer (CIO) functions as the Authorizing Official. The FDIC has determined that OMB Circular A-130 is "generally applicable" to the FDIC, to the extent that the Circular aligns with OMB's statutory authorities, does not impose obligations on the FDIC based on statutes that are legally inapplicable to the FDIC, and does not conflict with the FDIC's independence, statutory obligations, or regulatory authority.

[6] The FDIC has determined that NIST SPs contain statements of best practices or guidance and are not binding on the FDIC.

[7] We used Revision 4 of NIST SP 800-53 as criteria because Revision 4 was in effect at the time of our audit. In September 2020, NIST issued a fifth revision to NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations.* According to OMB Circular A-130, Federal agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines within 1 year of their respective publication dates unless otherwise directed by the OMB.

Mobile Device Controls Assessed During the Audit

We assessed the effectiveness of the FDIC's controls for securing and managing mobile devices in nine areas. We identified these nine areas based on our analysis of FISMA, NIST security standards and guidance, FDIC policy and guidance, and government-wide security policy requirements.[8] Table 1 describes the security control areas we assessed.

Table 1: Security Control Areas Assessed

Control Area	Definition
1. **Policies, Procedures, and Guidance**	FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006),[9] states that policies and procedures play an important role in the effective implementation of enterprise-wide information security programs within the Federal government. Up-to-date policies, procedures, and guidance help to ensure that employees and contractor personnel implement security controls and practices in a proper, consistent, and disciplined manner.
2. **Control Assessments**	FISMA and NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, require Federal agencies to assess their information system security controls. Such assessments evaluate the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the systems.
3. **Logging and Monitoring**	NIST SP 800-92, *Guide to Computer Security Log Management* (September 2006), recommends that organizations review and analyze audit records (logs) for indications of inappropriate or unusual activity. An audit log is a record of events occurring within an information system or network.
4. **Awareness Training**	FISMA requires Federal agencies to provide security awareness training to their personnel, contractors, and other system users. Awareness training helps to ensure that personnel have a proper understanding of their responsibilities for protecting the confidentiality, integrity, and availability of agency data and information systems.
5. **Billing Analysis**	Presidential Executive Order 13589, *Promoting Efficient Spending* (November 2011), states that agencies should assess their IT device inventories and usage and establish controls to ensure agencies do not pay for unused or underutilized IT equipment, installed software, or services. By analyzing billings submitted by vendors, agencies can mitigate the risk of paying for unnecessary devices and services.[10]

[8] See FISMA; FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006); NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013); NIST SP 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (June 2013); NIST SP 800-92, *Guide to Computer Security Log Management* (September 2006); NIST SP 1800-5B*, IT Asset Management* (September 2018); NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide* (August 2012); NIST SP 800-175B, Rev. 1, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms* (March 2020); FDIC Circular 1360.9, *Protecting Sensitive Information* (April 2007); *The FDIC Security and Privacy Control Assessment (SCA) Methodology,* Version 1.0 (April 2020); FDIC CIO's *Policy on IT Asset Management* (May 2017); OMB Circular A-130 (July 2016); and Presidential Executive Order 13589, *Promoting Efficient Spending* (November 2011).

[9] NIST FIPS Publication 200 is a mandatory standard under FISMA. However, it is the FDIC's position that FIPS Publication 200 is not binding on the FDIC because the Secretary of Commerce, who approved the publication, does not have the authority to impose mandatory requirements on the FDIC. The FDIC views FIPS Publication 200 as guidance for "best practices" in implementing security measures for information systems.

[10] It is the FDIC's position that Executive Order 13589 is not binding on the Corporation, but the FDIC may voluntarily comply with any or all provisions it deems appropriate.

Control Area	Definition
6. **Configuration Management**	FISMA requires Federal agencies to ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. Configuration management refers to the collection of activities focused on establishing and maintaining the integrity of IT products and systems. Organizations foster integrity by controlling its processes for initializing, changing, and monitoring the configurations of IT products and systems.
7. **Asset Management**	According to the FDIC CIO's *Policy on IT Asset Management* (May 2017), asset management consists of processes associated with managing and tracking hardware, software, subscription services, and maintenance contracts from inception to disposal.
8. **Incident Response**	FISMA requires Federal agencies to develop, document, and implement policies and procedures for incident response. Incident response involves detecting, responding to, and limiting the consequences of violations of security policies and recommended practices, including malicious cyber-attacks against systems.
9. **Data Protection**	According to FDIC Circular 1360.9, *Protecting Sensitive Information* (April 2007), data protection involves safeguarding sensitive information from loss, misuse, or unauthorized access or modification.

Source: Cotton & Company's analysis of FISMA, NIST standards and guidance, FDIC policy and guidance, and the Government Accountability Office/Counsel of the Inspectors General on Integrity and Efficiency (CIGIE) *Financial Audit Manual* (GAO-18-601G, updated April 2020).

Audit Results

We determined that FDIC's controls were not effective to secure and manage mobile devices in three areas assessed, because their implementation did not comply with or was not consistent with relevant Federal or FDIC guidance. We further determined that FDIC's controls were only partially effective in three additional areas, because the agency did not fully comply with Federal or FDIC guidance. The agency had established and implemented effective controls in three areas. Table 2 identifies the security control areas we assessed and our determinations regarding their effectiveness. A description of our results for each security control area follows the table.

Table 2: Effectiveness by Control Area

Control Area	Audit Result
Policies, Procedures, and Guidance	Not Effective
Control Assessments	Not Effective
Logging and Monitoring	Not Effective
Awareness Training	Partially Effective
Billing Analysis	Partially Effective
Configuration Management	Partially Effective
Asset Management	Effective
Incident Response	Effective
Data Protection	Effective

Source: Cotton & Company's review and analysis of selected security control areas for the FDIC's mobile devices.

Note: Determinations of Effective indicate compliance with relevant Federal and FDIC policy requirements and guidelines. Determinations of Partially Effective indicate compliance with some, but not all, Federal and FDIC

policy requirements and guidelines. Determinations of Not Effective indicate non-compliance with Federal and FDIC policy requirements and guidelines. Appendix 1, Objective, Scope, and Methodology, describes the audit procedures we performed to assess effectiveness.

Outdated Policies, Procedures, and Guidance

NIST SP 800-124, Rev. 1, recommends that organizations establish a mobile device security policy. According to this NIST publication, the policy should define such elements as the types of mobile devices permitted to access the organization's IT resources (including COPE or BYOD) and the IT resources mobile devices can access. Further, NIST SP 800-124, Rev. 1, recommends that organizations identify threats and vulnerabilities related to their mobile devices and periodically assess their policies to address needed changes. In addition, GAO identified the establishment of a mobile device security policy as a recognized practice.[11] According to the GAO, such policies define the rules, principles, and practices that determine how an organization treats its COPE and BYOD mobile devices.

The FDIC established a number of policies governing the management, use, and security of its IT resources and equipment, including its mobile devices. For example, FDIC Directive 1300.04, *Acceptable Use Policy for FDIC Information Technology* (issued in April 2017, and updated in November 2020) defines limitations and prohibitions on the personal use of FDIC-furnished IT equipment.[12] In addition, FDIC Circular 3100.4, *Wireless Telephone and Pager Assignments, Usage, Safeguards, and Asset Management (Wireless Telephone)* (April 2003)[13], defines policy, responsibilities, and procedures for managing mobile wireless devices.

However, the FDIC's IT policies did not reflect the FDIC's current business practices pertaining to mobile devices. For example, the FDIC issued Circular 3100.4 more than 18 years ago—prior to the introduction of smartphones and tablets into the FDIC's IT environment. As a result, FDIC Circular 3100.4 focuses on obsolete mobile technologies, such as pagers, that are no longer in use at the FDIC. In addition, FDIC Circular 3100.4 references other FDIC policies that are outdated, such as FDIC Circular 3100.2, *Guidelines for the Use of Voice Telecommunications Services* (January 2003).

Further, our review of FDIC's IT policies and guidance found that they were not comprehensive, because they did not address several key elements of a mobile device policy as recommended in NIST SP 800-124, Rev. 1, and by GAO.

[11] See GAO Report, *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged* (GAO-12-757) (September 2012).
[12] For example, FDIC Directive 1300.04 establishes restrictions on connecting personally owned peripherals to FDIC-furnished IT equipment, taking FDIC IT equipment outside of the United States, and connecting IT devices to public hotspots, Wi-Fi, and cellular networks.
[13] FDIC Circular 3100.4 was updated in September 2009 with pedestrian changes to include a customer service number and vendor user guides.

Use of BYOD

In May 2019, the FDIC began allowing its bank examiners in the field the option of using BYOD in lieu of receiving a COPE smartphone. The FDIC developed a set of Frequently Asked Questions (FAQs) that described the security requirements that users of BYOD must adhere to and provided these FAQs to examiners that chose to use BYOD. The FAQs addressed such things as:

- The smartphone models that the FDIC has approved for BYOD;
- The requirement for users to install the FDIC's MDM solution on their personally-owned device;
- Required security configurations that users must maintain, such as a current version of the manufacturer's operating system, a passcode, and a screen auto-lock;
- A description of the information the FDIC collects from BYOD devices, such as the device type and operating system version, and personal data the MDM solution does not capture or monitor, such as personal applications, emails and texts;
- The user's obligations for notifying the FDIC when their personal device is lost or stolen;
- The FDIC's processes for remotely wiping devices; and
- Steps users must take to protect their device before traveling internationally.

The FDIC, however, did not incorporate the information in the FAQs into its written policies or guidance. Doing so would help to ensure that owners of BYOD understand their rights and responsibilities. In addition, we noted that FDIC's policies and guidance did not specifically address other matters relevant to BYOD, such as:

- The FDIC's potential liability for problems stemming from work-related use of the device. For example, if the FDIC did not properly remove the secure container from a BYOD device after it was reported lost or stolen, personal data stored on the device outside of the secure container could be inadvertently deleted. Without a clear articulation of liability for the FDIC and the owner of the device, employees may enroll in BYOD without an informed understanding of the risks they are assuming.
- The responsibility of employees to report unusual activity, such as potential malware infections, on their personal devices. If the FDIC does not establish clear expectations for reporting unusual activity, incidents may not be addressed in a timely manner. This, in turn, could place FDIC data at risk of compromise.

Although certain compliance controls are automated, mobile device agreements serve as a key control for holding individuals accountable for non-compliance with FDIC security requirements. Such agreements require users to acknowledge their responsibility for using the device in a manner that does

not compromise the security of FDIC data, such as storing sensitive data outside of the secure container. While the FDIC required users of COPE smartphones to sign a *SmartPhone Service Agreement* wherein they consent to certain rules of behavior,[14] the FDIC did not require users of BYOD to sign a similar agreement. NIST SP 800-124, Rev. 1, states that organizations should define user responsibilities for implementing security measures in mobile device agreements. Absent a mobile device agreement, BYOD users may not fully understand the FDIC's expectations regarding the use of mobile devices in the IT environment, including the user's responsibility to comply with the minimum standards in FDIC Directive 1300.04, *Acceptable Use Policy for FDIC Information.*

Personal Use of COPE Devices

The FDIC's *SmartPhone Service Agreement*, FDIC Directive 1300.04, *Acceptable Use Policy for FDIC Information*, and FDIC Circular 3100.4, *Wireless Telephone and Pager Assignments, Usage, Safeguards, and Asset Management (Wireless Telephone)*, require users of COPE devices to adhere to certain rules of behavior. However, the *SmartPhone Service Agreement*, directive, and circular do not address certain risks associated with personal use of mobile devices outside of the secure container.

Mobile Applications

FDIC Directive 1300.04, *Acceptable Use Policy for FDIC Information Technology*, prohibits employees and contractor personnel from using IT resources for certain activities, such as installing software or services designed to share data or files with other internal or external users or viewing inappropriate images or files. However, the FDIC has not specifically addressed in its IT policies or guidance minimum expectations regarding the downloading and acceptable use of mobile applications. The FDIC allows its employees and contractor personnel to download applications from the manufacturer of its mobile devices and install the applications outside of the secure container. As a result, these personnel can download a wide range of applications onto government-furnished equipment, including applications that do not serve a business purpose. We reviewed a listing of applications installed on COPE devices generated by the FDIC's MDM solution as of March 5, 2021. We found that employees and contractor personnel had downloaded non-work related applications related to such things as social media, dating services, shopping, sports entertainment, and movie streaming services.[15]

The use of such applications presents security and reputational risk. From a security perspective, some mobile applications have the ability to track a user's location and movements through enabled services on the device; access the contacts, microphone, and camera on the device with the user's consent; and record Internet browsing habits. Application developers may collect this data and share it with third

[14] The *SmartPhone Service Agreement* is attached to FDIC Form 1380-08, *Request for Wireless Services* (September 2020).

[15] The FDIC's MDM solution was not designed to generate reports regarding employee or contractor use of mobile applications stored outside of the secure container. Therefore, we could not determine the extent to which employees and contractor personnel used non-work related applications. The CIOO had also not implemented technical controls to prevent employees or contractor personnel from downloading non-work related applications available from the mobile device manufacturer.

parties for marketing and other purposes. If a user inadvertently or inappropriately stores sensitive FDIC information outside of the secure container, there is an increased risk that a mobile application could access and share the information outside of the FDIC. From a reputational risk perspective, the use of non-business related mobile applications could create a perception that FDIC employees and contractor personnel use government-furnished equipment for personal entertainment while working.[16]

In September 2020, the U.S. Securities and Exchange Commission's (SEC) Office of Inspector General (OIG) issued an audit report that identified similar issues regarding mobile device applications.[17] In its report, the SEC OIG identified applications that did not appear to relate to the business of the SEC and that were not part of the SEC's catalog of approved applications. Such applications included video streaming applications, children's applications and/or social media applications, and shopping, dating, and other entertainment applications. According to the SEC OIG's report, without adequate safeguards, the use of untrusted applications increases the risk of unauthorized access to SEC data.

Text Messaging, Audio, and Video

Before employees and contractor personnel can receive a COPE mobile device, they must sign the *SmartPhone Service Agreement*. The rules of behavior defined in this agreement prohibit individuals from storing mission critical and other sensitive FDIC information outside of the secure container on the device. However, neither the *SmartPhone Service Agreement* nor FDIC policy address the risks associated with texting sensitive FDIC information or taking photographs and videos of sensitive FDIC materials outside of the secure container.

Further, COPE devices have the ability to sync text messages, photographs, and audio recordings stored outside of the secure container with a third-party cloud provider. This syncing process generates a duplicate copy of the data and stores it at a third-party cloud provider so that individuals can access the data from any device using a user identification and password. The cloud provider is not subject to security assessments by the FDIC. If a user inadvertently or inappropriately stored sensitive FDIC information outside of the secure container, the information could be accessed by the third-party cloud provider.

The FDIC does not have a centralized way of monitoring activity outside of the secure container. Some mobile applications have the ability to access the microphone on mobile devices, which could provide a third-party access to audio recordings that contain sensitive FDIC information. In addition, the FDIC cannot monitor data that employees and contractor personnel may inappropriately store outside of the secure container for compliance with the FDIC's Record Retention Schedule.[18] If the FDIC wanted to see the content of an employee's text message, or what photographs or recordings the employee has stored

[16] The FDIC's Risk Appetite Statement states that reputational risk can diminish the stature, credibility, or effectiveness of the FDIC.
[17] SEC OIG Report, *Opportunities Exist To Improve the SEC's Management of Mobile Devices and Services*, (Report No. 562) (September 30, 2020).
[18] The Records Retention Schedule defines the required retention and disposal periods for FDIC business records. As previously noted, employees are prohibited from storing sensitive FDIC information outside of the secure container on a mobile device.

on the mobile device, the FDIC would need to obtain the physical device and review the underlying data (text messages, photographs, or videos).

FDIC policy and guidance also does not address the risks associated with using the microphone on mobile devices to make audio recordings stored outside of the secure container that may contain sensitive information. Ensuring that employees and contractors are aware of these risks is important because the MDM solution does not have the ability to monitor whether individuals have placed sensitive FDIC information intentionally or inadvertently in texts, photographs, and audio recordings outside of the secure container.

NIST SP 800-124, Rev. 1, identifies the elements that organizations should include in their mobile device security policies and the factors that organizations should consider when formulating policy decisions underlying each element. Without current and comprehensive policies and guidance covering mobile devices, FDIC personnel may not be aware of relevant risks associated with their mobile devices or the steps they should take to mitigate those risks. Current and comprehensive mobile device policies and guidance serve as an important control for helping to inform employees and contractor personnel of their responsibilities regarding the proper use of mobile devices, and for holding accountable those personnel who fail to meet those responsibilities. Further, up-to-date mobile device policies and guidance help to ensure that both IT personnel and users implement their responsibilities in a proper, consistent, and disciplined manner.

We recommend that the CIO:

1. Perform a documented assessment of risks associated with BYOD and the personal use of COPE devices, including the installation and use of mobile applications, text messaging, and audio and video capabilities.

2. Establish mobile device policies and guidance that align with NIST and GAO recommended practices. The policies and guidance should (a) reflect the FDIC's current business practices for mobile devices and (b) be based on the documented assessment of risks in Recommendation 1.

3. Require users of BYOD to consent to rules of behavior in a mobile device security agreement.

Control Assessments Not Conducted

FISMA requires Federal agencies to test and evaluate at least annually the effectiveness of their information system security controls. FISMA also extends this requirement to systems that "support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." The *FDIC Security and Privacy Control Assessment (SCA) Methodology* (Version 1.0, April 2020), defines the FDIC's processes for assessing the effectiveness of controls in all

FDIC information systems, including cloud-based systems such as the MDM solution. According to the *FDIC Security and Privacy Control Assessment (SCA) Methodology*, the OCISO must assess all security and privacy controls for cloud-based systems on a 3-year cycle, with at least some controls tested every year.

We found that the OCISO did not conduct annual SCAs of the MDM solution. The OCISO had completed only one SCA of the MDM solution prior to the CIO's initial authorization of the system on August 25, 2016. The OCISO did not include any of the FDIC's cloud-based systems on the CIOO's schedule for conducting SCAs, and therefore, it did not conduct the required annual SCAs of the MDM solution.

In September 2019, the FDIC created a Plan of Action and Milestone (POA&M)[19] to remediate the weakness it identified that it was not subjecting cloud-based systems to annual security and privacy control assessments. The POA&M recommended that the FDIC add all of its cloud-based information systems to the CIOO's schedule for conducting SCAs. In March 2020, the CIOO scheduled the MDM solution for an SCA with an estimated start date between April and June 2020.

According to NIST SP 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* (December 2014), SCAs are the principal vehicle used by agencies to verify that controls meet their stated goals and objectives. The FDIC uses the results of SCAs to support a number of important risk management activities. Such activities include identifying security and privacy weaknesses in information systems and the IT environment; prioritizing risk mitigation activities; confirming the resolution of known security and privacy weaknesses; informing system authorization decisions; and supporting resource allocation decisions. Without annual testing of controls for the MDM solution, the FDIC cannot be sure that it can identify and remediate security and privacy weaknesses in a timely manner. Such weaknesses could threaten the confidentiality, integrity, and availability of sensitive FDIC information.

We initially reported that the FDIC had not conducted annual SCAs of its cloud-based information systems in our FISMA audit report issued in October 2020.[20] We recommended in our FISMA audit report that the CIO subject all of the FDIC's cloud-based information systems, including the MDM solution, to annual SCAs. The FDIC completed the SCA of the MDM solution in February 2021.

[19] A POA&M is a management tool used by agency CIOs, security personnel, program officials, and others to track the progress of corrective actions pertaining to security vulnerabilities identified through security control assessments and other sources. POA&Ms assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective actions pertaining to information security vulnerabilities.
[20] See FDIC Office of Inspector General, *The FDIC's Information Security Program–2020* (AUD-21-001, October 2020).

Logging and Monitoring Processes Not Documented

NIST SP 800-92, *Guide to Computer Security Log Management* (September 2006), states that routine analysis of information system audit logs[21] can identify security incidents, policy violations, fraudulent activity, and operational problems that organizations need to address. NIST SP 800-92 provides organizations with guidance for developing, implementing, and maintaining effective log management practices. According to NIST SP 800-92, organizations should establish policies and procedures for log management that "clearly define mandatory requirements and suggested recommendations for log management activities, including log generation, transmission, storage, analysis, and disposal." Such policies and procedures should include defined roles and responsibilities for key personnel involved in log management.

We found that an MDM system administrator periodically reviewed the audit logs generated by the MDM solution for unusual and suspicious activity. However, the process for reviewing these logs was informal and not guided by written procedures. Specifically, DIT had not developed written procedures that defined roles and responsibilities for:

- Extracting audit logs from the MDM solution for review;
- Reviewing audit logs generated by the MDM solution, including the scope and required frequency of the reviews and the associated documentation requirements;
- Investigating suspicious activity identified during log reviews; and
- Maintaining and securing audit logs and associated review materials.

The FDIC did not develop procedures for reviewing audit logs generated by the MDM solution, because DIT did not consider it to be a priority matter. Up-to-date procedures that describe processes helps to ensure that FDIC personnel understand management's expectations as well as their roles and responsibilities for implementing processes in a proper, consistent, and disciplined manner. The absence of written procedures for reviewing audit logs increased the operational risk associated with staff turnover because DIT was dependent on the knowledge and experience of a key administrator to perform this function.

[21] NIST SP 800-92 defines the term "log" as a record of events occurring within an organization's information systems and networks. Events can include successful and failed login attempts, security configuration changes, account changes (e.g., account creations and deletions), the use of administrative credentials, and system activity such as processing errors and application failures.

Separation of Duties

NIST SP 800-92 states that organizations should consider the principle of separation of duties when deciding how to assign audit log management duties among staff. According to NIST, separation of duties involves dividing critical functions among different staff in an attempt to ensure that no one individual has enough information or access privilege to misuse the system on their own, or to perpetrate damaging fraud.[22] For example, NIST SP 800-92 states that "having someone other than a system administrator review the logs for a particular system helps to provide accountability for the system administrator's actions, including confirming that logging is enabled."

We found that the FDIC had designated the same individual as responsible for both (i) reviewing the audit logs generated by the MDM solution; and (ii) serving as an MDM administrator. Having one individual perform both of these responsibilities did not provide for appropriate separation of duties. As an MDM administrator, the individual has elevated access privileges that could be used to create accounts in the MDM solution, change configuration settings on mobile devices, and bypass system controls to perform troubleshooting activities. By tasking the MDM administrator with reviewing audit logs, this individual was effectively responsible for reviewing the appropriateness of his own actions. Such responsibility could allow this individual to perform unauthorized activities, such as implementing unapproved security configuration changes to mobile devices or altering or deleting audit logs, without detection.

In July 2020, after we brought this issue to the CIOO's attention, the CIOO created a POA&M to address the separation of duties weakness we identified. The POA&M acknowledges the need to better separate responsibilities for system administration from audit logging and monitoring for the MDM solution.

We recommend that the CIO:

4. Define and document roles, responsibilities, and procedures for reviewing audit logs generated by the MDM solution.

5. Separate responsibilities for performing systems administration from conducting reviews of audit logs generated by the MDM solution.

[22] See NIST IT Computer Security Resource Center Glossary, https://csrc.nist.gov/glossary/term/Separation_of_Duty/.

Insufficient Awareness Training

FISMA requires Federal agencies to provide security awareness training to their personnel, contractors, and other system users. According to FISMA, the purpose of such training is to inform personnel of the information security risks associated with their activities and their responsibility to comply with agency policies and procedures designed to reduce these risks. In addition, NIST SP 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, recommends that organizations provide training and awareness to users of mobile devices on relevant threats and security practices. According to GAO,[23] training employees on an organization's mobile security policies can help to ensure that employees use mobile devices in a secure and appropriate manner.

FDIC policy[24] requires all employees and contractor personnel with access to the FDIC's internal network to complete annual Information Security and Privacy Awareness (ISPA) Training. The FDIC requires its employees and contractors to take this training to raise their awareness of computer security and privacy laws, regulations, and policies; rules of behavior and effective security practices; and compliance requirements governing the FDIC's collection, use, sharing, and protection of sensitive data, including PII.

However, we found that the ISPA Training contained limited information on threats to mobile devices and security practices for mitigating those threats. This occurred because the FDIC based its ISPA Training on FDIC Circulars 1300.4, *Acceptable Use Policy for IT Resources* (October 2018), and 1360.9, *Protecting Sensitive Information* (October 2015), which contain limited content on mobile device threats and security practices. NIST's National Cybersecurity Center for Excellence has published a Mobile Threat Catalogue that describes, identifies, and structures threats posed to mobile systems.[25] The Mobile Threat Catalogue contains information that could assist the FDIC in developing awareness training for its mobile device users. The ISPA Training did not address the following areas (several of which are covered in FDIC's IT policies):

- Risks associated with using unsecured public Wi-Fi hotspots, and guidance on how to identify and connect to secure wireless networks when users must access public hotspots.
- Guidance for identifying suspicious activity on mobile devices, such as blocked attempts to access the secure container and text messages from unknown parties that include links to potentially malicious websites.

[23] See GAO Report, *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged* (Report No. GAO-12-757, September 2012).
[24] FDIC Circulars 1360.16, *Mandatory Information Security Awareness Training* (March 2012), and 1360.9, *Protecting Sensitive Information* (April 2007).
[25] See NIST Mobile Threat Catalogue, https://pages.nist.gov/mobile-threat-catalogue/.

- Risks associated with downloading mobile applications, such as privacy concerns associated with applications that can track user activities.

- Security considerations regarding the use of Bluetooth[26] to connect mobile devices with peripheral devices.

- Risks associated with texting sensitive FDIC information to other individuals.

- Security precautions users should take to prior to, during, and immediately following, foreign travel.

Awareness training on mobile device threats and security practices is an important control for helping to ensure that FDIC employees and contractor personnel have a proper understanding of their responsibilities for safeguarding mobile devices and the data they contain. Individuals who do not receive periodic awareness training are less likely to be familiar with FDIC policies, guidance, and sound practices for protecting mobile devices. Effective awareness training, together with up-to-date policies, procedures, and guidance, can help to mitigate mobile device threats and reduce the risk of security incidents.

We recommend that the CIO:

6. Develop and implement awareness training to address risks and security practices related to the use of mobile devices.

Unreported Billing Analysis

As noted earlier, Presidential Executive Order 13589, *Promoting Efficient Spending* (November 2011), states that Federal executive departments and agencies should establish controls to ensure agencies do not pay for unused or underutilized equipment and services (including smartphones and tablets).[27] In addition, OMB Memorandum M-16-20, *Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services* (August 2016), encourages Federal agencies to analyze over and under usage of their mobile devices and services and identify and terminate unused mobile devices and services.[28] By analyzing usage and billing information submitted by telecommunications service carriers, agencies can mitigate the risk of paying for unnecessary devices and services.

[26] According to NIST SP 800-121, Rev. 2, *Guide to Bluetooth Security* (May 2017), Bluetooth is a wireless technology used primarily to establish wireless personal area networks. Bluetooth has been integrated into many types of business and consumer devices including, but not limited to, cell phones, laptops, printers, keyboards, mice, and headsets. Bluetooth allows users to form ad hoc networks between a wide variety of devices to transfer voice and data.

[27] The FDIC has determined that Executive Order 13589 is not legally binding on the FDIC, but has stated that it may choose to voluntarily comply with any or all provisions of the Executive Order.

[28] The FDIC has determined that OMB Memorandum M-16-20 is not legally binding on the FDIC, but has stated that it may choose to voluntarily comply with any or all provisions of the memorandum.

The FDIC engaged a contractor to analyze the accuracy of monthly billings submitted by the two telecommunications service carriers that support the FDIC's mobile devices. The contractor uses written procedures (Work Instructions) to analyze the carriers' monthly billings. The contractor's analysis includes an assessment of mobile device usage (including voice and data) reported by the carriers.

According to billing and usage data provided by EUCS, the FDIC paid a total of $136,305 during calendar year 2020 for its mobile devices and wireless hotspot devices called MiFi's with "zero usage" [29] (an average of $11,359 per month). Such inactivity is an indicator that there may no longer be a business need for the device. A representative of EUCS stated that the FDIC experienced an increase in the number of zero usage MiFi devices in 2020 due to the COVID-19 pandemic. The EUCS representative explained that many FDIC employees began using their home Wi-Fi during the pandemic instead of the MiFi devices used at onsite examinations to access the FDIC's network.

We found that the FDIC did not establish a process to routinely report usage information for mobile devices and MiFi devices, including zero usage information, to business units in the FDIC's Divisions and Offices or require the business units to provide EUCS documentation supporting the continued need for zero usage devices. Such reporting and documentation is important, because the business units are in the best position to make informed decisions regarding the continued business need for their devices. Further, the FDIC can achieve cost savings[30] if the business units in the Divisions and Offices routinely receive usage information for mobile devices and MiFi devices and suspend or terminate services that are no longer needed.

The FDIC's EUCS did not routinely report usage information for mobile devices or MiFi devices to FDIC's Divisions and Offices, because it had not identified an automated tool that could extract and generate usage information in a suitable format. Unless EUCS routinely reports usage information to the business units, decision makers will not have the information they need to make timely determinations regarding the continued need for zero usage devices. Routine reporting of usage information could also facilitate timely identification of unused devices that may be lost or stolen, but not reported as such. In addition, EUCS stated that they monitor zero usage monthly against an internally established tolerance level and informally follow-up with Divisions and Offices if that tolerance level is met. However, CIOO stated its zero usage cost have consistently been under the tolerance level. Further, the tolerance level is not documented in formal FDIC policy and we have not assessed the appropriateness of the tolerance level.

We recommend that the CIO:

[29] The FDIC defines zero usage as a lack of activity (including voice, data and texting) on a device for a period of 3 or more months. The $136,305 total for zero usage devices was comprised of $37,605 for smartphones and tablets and $98,700 for MiFi devices.
[30] The dollar amount of yearly cost savings will depend on the results of the Division and Office analyses of usage information and the CIOO's business continuity requirements.

7. Implement a process to routinely report usage information for mobile devices and MiFi devices to business units in the FDIC's Divisions and Offices.

8. Require the FDIC's Divisions and Offices to provide EUCS with documentation to support the continued business need for zero usage devices and take action to suspend or terminate unnecessary devices and services.

Configuration Management Procedures Needed Improvement

FISMA requires Federal agencies to ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. Organizations establish configuration requirements for their information systems in a document or repository called a "baseline configuration." A baseline configuration defines the required specifications for a system, such as its required security settings, software version, patch levels, and documentation. Organizations use baseline configurations to assess their systems for compliance with configuration requirements and to help manage future builds, releases, and changes. NIST SPs 800-53, Rev. 4, and 800-128, *Guide for Security-Focused Configuration Management of Information Systems* (August 2011), recommend that organizations test and document, system changes before implementing them. Such changes include installing software patches and updates to operating systems that address security vulnerabilities and improve system performance and functionality. Without effective processes for testing changes, information systems may not operate properly or may stop operating altogether.

We found that the CIOO developed and approved baseline configurations for its COPE and BYOD mobile devices. In addition, the CIOO prepared Acceptances of Risk[31] for deviations from its approved baseline configurations. However, the FDIC did not test software updates for its mobile devices before users downloaded and installed them.

The manufacturer of the FDIC's mobile devices periodically releases operating system updates to address security weaknesses and improve functionality. DIT's EUCS tests these software updates to ensure they function properly in the FDIC's IT environment. However, EUCS had not developed written procedures that described the tests it performs or how EUCS records, maintains, and reports testing results. Without procedures to guide the testing of software updates, FDIC personnel may not evaluate the updates in a consistent or repeatable manner. In addition, the FDIC is dependent on the knowledge and experience of a few key personnel, which exposes the FDIC to operational risk should these key personnel depart the FDIC.

[31] An Acceptance of Risk is a memorandum signed by the FDIC's CIO, CISO, and other IT professionals that describes a known security weakness or vulnerability for which the FDIC has reviewed mitigation controls, decided not to pursue further remediation, and accepted the residual risk.

Further, we found that EUCS performs functional testing of operating system software updates for mobile devices when the manufacturer releases the updates to the public. However, EUCS had not configured the MDM solution to prevent users from downloading and installing these updates until EUCS completed its testing and confirmed that the updates did not cause issues in the FDIC's IT environment. This approach presents an operational risk that users will install a software update that causes a widespread IT interoperability issue.

Such an issue occurred in September 2019, when the manufacturer of the FDIC's smartphones released an operating system software update. After installing the update, some users were no longer able to use the hotspot functionality on their mobile devices to connect their laptops to the FDIC's internal network. This issue occurred because the software update for the smartphone was not fully compatible with the software on the FDIC's laptops. The ability to connect to the FDIC's network via the hotspot on the smartphone is especially important for employees who work remotely, such as bank examiners. Without connectivity to the network, employees and contractor personnel working remotely may not be able to perform their duties. Had EUCS completed its functional testing before allowing users to download the software update, EUCS could have identified and remediated the hotspot connectivity issue before users started calling the Helpdesk to report the problem.

EUCS representatives stated that the manufacturer of the FDIC's mobile devices coordinates with the manufacturer of the MDM solution before releasing software updates to mitigate the risk of functional or interoperability issues. In addition, EUCS cannot begin testing software updates until the manufacturer releases them to the public. Further, the CIO issued guidance to FDIC Divisions and Offices in December 2018[32] stating that users should download and install software updates to their mobile devices "as soon as possible, but no later than 30 days" after the manufacturer releases them. The CIO's guidance states that many software updates address security issues that could put mobile devices or the data they contain at risk. Therefore, users should install software updates as promptly as possible.

Although EUCS cannot begin testing software updates until the manufacturer releases them, EUCS could configure the MDM solution to prevent users from downloading and installing updates until EUCS completes its testing. According to a representative of EUCS, it typically takes only a few days to complete functional testing of software updates. Testing these updates before users install them would mitigate the risk of introducing interoperability issues into the FDIC's IT environment that require the expenditure of unnecessary resources to respond to help desk tickets from affected users.

After we brought this issue to the attention of the CIOO, EUCS configured the MDM solution to prevent users from downloading and installing software updates on mobile devices until 3 days after the

[32] Memorandum from the FDIC CIO to Division and Office Directors, entitled *Mobile Phone and Tablet Software Updates Must Be Installed Within 30 Days* (December 2018).

manufacturer releases the updates. This change was intended to provide EUCS time to complete its testing of software updates before users install them in the FDIC's IT environment. Although EUCS implemented this change during our audit, it had not yet updated its mobile device policy to reflect the change.

We recommend that the CIO:

9. Develop and implement written policies and/or procedures that define roles, responsibilities, and requirements for testing mobile device software updates and documenting the associated results before users are permitted to download and install them.

Asset Management

NIST SP 1800-5B, *IT Asset Management* (September 2018), recommends that organizations implement an IT asset management approach that provides management with a complete picture of what, where, and how assets are being used throughout their lifecycle. According to NIST SP 1800-5B, a typical asset lifecycle includes an enrollment, operation, and end-of-life phase. In addition, NIST SP 800-124, Rev. 1, emphasizes the importance of organizations maintaining a current mobile device inventory. A current inventory allows an organization to effectively manage and secure its mobile devices, including determining if devices have been lost or stolen.

Our work in the asset management area focused on reviewing key asset management processes for managing mobile devices in the enrollment, operations, and end-of-life phases described below. We also determined whether the FDIC had a process in place to conduct periodic inventories of its mobile devices.

We found that the FDIC issued Policy 05-006, *Policy on IT Asset Management* (May 2017), which outlines the CIOO's responsibilities for managing IT assets throughout the acquisition, deployment, management and disposal processes. In addition, the FDIC issued Directive 1380.2, *Information Technology Asset Management Program* (June 2017), which requires the CIOO to conduct periodic inventories of its IT assets. We also found the following conditions with respect to the enrollment, operations, and end-of-life phases of mobile devices.

Enrollment. During the enrollment phase, an FDIC user submits a completed FDIC Form 1380-08, *Request for Wireless Services*, to the CIOO to request an FDIC-issued mobile device. Upon receipt of a completed FDIC Form 1380-08, the CIOO performs several steps before providing the user a mobile device. Specifically, FDIC policy requires the CIOO places a label on the device containing its serial number and barcode for tracking and inventorying purposes, enrolls the device in the MDM solution to

apply configuration settings, and records the owner of the asset and serial number in ServiceNow.[33] We tested a sample of 45 of 4,503 mobile devices as of March 2020, to determine whether the FDIC completed these enrollment activities for newly issued mobile devices. We confirmed that all 45 users submitted a completed Form 1380-8 to request a mobile device. In addition, the CIOO enrolled the devices in the MDM solution, applied the appropriate configuration settings, and recorded the device owner's name and serial number in ServiceNow.

Operations. During the operations phase, the CIOO tracks and monitors changes to mobile devices, such as updates to the devices' operating system, and ensures such changes adhere to established requirements. For example, we confirmed that the CIOO used its MDM solution to determine if users operated FDIC-issued mobile devices outside the United States without proper approval. The CIOO has the ability to disable devices operating outside of the United States. In addition, the CIOO tracked whether users downloaded required mobile device operating system updates within the CIOO's required 30 day timeframe and disabled devices that did not comply with this requirement.

End-of-Life. When mobile devices reach their end-of-life, users must return the device to CIOO so that it can remove sensitive FDIC data and update information in ServiceNow. The CIOO also prepares the device for physical removal from the FDIC's IT environment and records the reason for disposal and the date it retired the device in ServiceNow. We compared a sample of 44 out of 1,915 employees and contractor personnel who separated from the FDIC between January 1, 2019, and January 31, 2020, to a list of active BYOD and COPE users generated by the MDM solution as of March 6, 2020 and May 29, 2020, respectively, and confirmed that the FDIC had removed all 44 users from the MDM solution.

We also confirmed that the CIOO had a process in place to conduct annual inventories of its mobile devices as part of its overall corporate IT Asset Inventory and update inventory information within its Enterprise Asset Management System (EAMS)[34] and ServiceNow. We did not test the reliability of the mobile device inventory data.

We determined that the CIOO's asset management processes for managing and inventorying its mobile devices were effective.

Incident Response

FISMA requires Federal agencies to develop, document, and implement an agency-wide information security program that includes policies and procedures for Incident Response. In addition, NIST SP 800-

[33] ServiceNow contains information on helpdesk tickets and details on the FDIC's mobile device inventory, such as serial numbers, manufacturers, models, locations, and status information.
[34] EAMS is the FDIC system used for cataloging and managing IT assets throughout their life cycle (including the request, procurement, and receipt of assets), and serves as the system of records for assets. EAMS records 'key' information on the IT asset including asset name, quantity, date received and serial number.

61, Rev. 2, *Computer Security Incident Handling Guide* (August 2012), provides guidance to assist agencies in establishing incident response teams; acquiring necessary tools and resources; detecting, analyzing, and reporting incidents; and containing, eradicating, investigating, and recovering from incidents. NIST SP 800-61, Rev, 2, recommends that organizations develop policies and procedures for detecting, reporting, analyzing, and closing security incidents. Such procedures apply to security incidents involving mobile devices.

The FDIC established policies and procedures for responding to computer security incidents, including incidents involving mobile devices. For example, FDIC Directive 1360.12, *Reporting Information Security Incidents* (April 2017), establishes policies, procedures, and guidelines for the management and reporting of information security incidents involving FDIC data. Our review of FDIC Directive 1360.12 found that it addressed procedures for handling security incidents involving mobile devices and required all users of FDIC information systems or possessors of FDIC information to report all information security incidents to the FDIC's Computer Security Incident Response Team (CSIRT). CSIRT has responsibility for investigating and tracking all reported information security incidents and reporting those incidents to the OCISO. In addition, OCISO operated a centralized system to track and manage incidents, including incidents involving mobile devices. Further, the CIOO developed a severity classification framework to prioritize and escalate computer security incidents.

We reviewed a sample of 33 of 397 incidents involving mobile devices reported as lost or stolen to determine whether the FDIC documented and handled the incidents consistent with FDIC policy.[35] We found that the FDIC documented and reported the incidents, remotely locked and wiped the mobile devices, and recorded appropriate disposition information in ServiceNow. Therefore, we concluded that the CIOO's processes that we reviewed for detecting and handling security incidents involving mobile devices were effective.

Data Protection

FDIC Circular 1360.9, *Protecting Sensitive Information* (April 2007), establishes policy for protecting sensitive information collected and maintained by the FDIC, which would apply to information collected and maintained within the secure container on mobile devices. In addition, FDIC Circular 1360.9 states that it is the policy of the FDIC to encrypt[36] sensitive information stored on end-user IT equipment and transmitted through email or other transmission systems. Our work related to Data Protection focused on the security of information inside the secure container on the mobile devices.

[35] We identified 397 incidents by searching ServiceNow—the FDIC's centralized ticketing system—for tickets with the phrase "CSIRT Lost." This search identified a population of 33 incidents opened between January and May 2020.

[36] Encryption is a process intended to safeguard sensitive information from unauthorized disclosure or modification. Encryption involves converting information and data into an unreadable form or code so that unauthorized users cannot understand the underlying information or data. Decryption involves converting encrypted information back to its original form so it can be understood.

We determined that the FDIC's MDM solution encrypted sensitive FDIC information stored within the secure container on the mobile devices. In addition, the MDM solution encrypted communications between the mobile devices and the FDIC's internal network. We found that the MDM solution encrypted information using a NIST-recommended encryption protocol. Further, we confirmed that users could not access FDIC information or applications stored in the secure container without first authenticating through the MDM solution using a personal identification number or biometric identification.[37] Further, the CIOO configured the MDM solution to prevent users from:

- Accessing FDIC information or applications stored in the secure container using non-FDIC applications downloaded from the Internet;
- Employing common IT tools to extract FDIC information from the secure container; and
- Making backup copies of FDIC information stored in the secure container to external devices or Internet sites.

In addition, the CIOO offered several technical solutions that users could employ to encrypt sensitive FDIC information emailed to internal and external (non-FDIC) recipients via mobile devices.[38] The CIOO also used a Data Loss Prevention (DLP) tool to monitor email messages sent and received via mobile devices to mitigate the risk of unauthorized exfiltration of sensitive FDIC information.[39] Further, users received a system-generated warning message when they attempted to send an email to external email addresses via mobile devices. These system-generated warnings were intended to mitigate the risk of users inadvertently sending sensitive information to external recipients. Moreover, EUCS can use the MDM solution to remotely wipe devices when users report them as lost or stolen, or when the MDM solution detects that the device has been "jailbroken."[40] Remote wiping of mobile devices helps to reduce the risk of unauthorized disclosure of sensitive FDIC information. Therefore, we concluded that the CIOO's processes for protecting sensitive FDIC data within the secure container on mobile devices was effective.

[37] NIST SP 800-12, Rev.1, *An Introduction to Information Security* (June 2017), defines the term biometric identification as a measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Examples of biometrics include facial images, fingerprints, and iris scans. Users of FDIC's mobile devices can authenticate to the MDM solution using facial recognition technology.

[38] Such solutions include Microsoft's Azure Information Protection, Zix Mail, and PK Zip.

[39] The DLP tool is a software program that can monitor, detect, and block sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage). With respect to email, the DLP tool searches for keywords that match business rules intended to protect sensitive information. Information Security Managers (ISMs) with the FDIC's divisions and offices create these business rules. For example, an ISM may create a rule for the DLP to flag for review any document with the acronym "SIFI," for Systemically Important Financial Institution, which a user attempts to email to an external recipient. ISMs provide a security focus and role within FDIC's Divisions and Offices and promote compliance with security policies and procedures, among other security tasks.

[40] The term jailbreaking refers to bypassing restrictions imposed by the manufacturer in order to access to the device's operating system and change configuration settings. For example, a user may jailbreak a device to install unauthorized software. FDIC Directive 1300.04 strictly prohibits the jailbreaking FDIC-furnished IT devices.

Conclusion

We determined that the FDIC's controls were not effective to secure and manage mobile devices in three areas: Policies, Procedures and Guidance; Control Assessments; and Logging and Monitoring. In addition, we determined that the FDIC's controls were only partially effective in three additional areas: Awareness Training, Billing Analysis, and Configuration Management. The FDIC had implemented effective controls and practices in the areas of Asset Management, Incident Response, and Data Protection. Our report contains nine recommendations intended to strengthen the effectiveness of the FDIC's security controls and practices over its mobile devices.

Appendix 1: Objective, Scope and Methodology

The objective of this performance audit was to determine whether the FDIC had established and implemented effective controls to secure and manage its mobile devices. Cotton & Company conducted the audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) (2018 revision).[41] These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We assessed the effectiveness of internal controls that we deemed significant to the audit objective. Specifically, we assessed 7 of the 17 internal control principles defined in GAO's *Standards for Internal Control in the Federal Government* (the Green Book) (September 2014).[42] Table 3 below summarizes the principles we assessed.

Table 3: Internal Control Principles Assessed

Control Environment
Principle 4 – Demonstrate Commitment to Competence
Risk Assessment
Principle 7 – Identify, Analyze, and Respond to Risks
Principle 9 – Identify, Analyze, and Respond to Change
Control Activities
Principle 10 – Design Control Activities
Principle 11 – Design of Activities for the Information System
Principle 12 – Implement Control Activities
Monitoring
Principle 16 – Perform Monitoring

Source: Cotton & Company analysis of the Green Book and work performed on this audit.

The report presents the internal control deficiencies we identified within the findings. Because our audit was limited to the seven principles presented above, it may not have disclosed all internal control deficiencies that may have existed at the time of the audit.

The audit focused on the effectiveness of controls for securing and managing two types of mobile devices in the FDIC's IT environment: smartphones and tablets. We determined effectiveness by assessing compliance with relevant Federal and FDIC requirements and consistency with relevant Federal guidelines. Controls were effective if they complied with and/or were consistent with relevant

[41] Cotton & Company began this performance audit in July 2019. The 2018 revision of GAGAS became effective for performance audits beginning on or after July 1, 2019.

[42] The Green Book organizes internal control through a hierarchical structure of five components and 17 principles. The five components, which represent the highest level of the hierarchy, consist of the Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. The 17 principles support the effective design, implementation, and operation of the components, and represent the requirements for establishing an effective internal control system.

Federal and FDIC requirements and guidelines; partially effective if they complied with and/or were consistent with some, but not all, requirements and guidelines; and not effective if they did not comply with or were inconsistent with requirements and guidelines.

Our audit covered nine security control areas that we identified based on our analysis of FISMA, relevant NIST security standards and guidance, FDIC policy and guidance, and government-wide security policy requirements.[43] Table 1 in the Background section of the report describes the nine security control areas we assessed. We chose these nine areas because a control failure in these areas could impair the FDIC's ability to ensure the confidentiality, integrity, and availability of its mobile devices and the sensitive FDIC data they store and transmit. Such a failure could also impair the FDIC's ability to support its business operations and communications.

We assessed the design, implementation, and operating effectiveness of selected controls within each of the nine security control areas by:

- Assessing the extent to which FDIC policies, procedures, and guidance related to mobile devices aligned with NIST and government-wide security policy and guidance.

- Performing inquiries of CIOO personnel regarding the implementation of their responsibilities for administering the MDM solution; managing the provisioning, maintenance, monitoring, and de-provisioning of mobile devices; controlling and testing changes to mobile devices; conducting security control assessments of the MDM solution; and identifying and addressing risks pertaining to mobile devices.

- Selecting a sample of mobile devices to assess the consistency of FDIC's practices for provisioning the devices and obtaining required approvals.

- Testing the effectiveness of selected controls, including encryption and user settings (e.g., screen locks), intended to protect data in the secure container.

- Evaluating the effectiveness of controls, including controls intended to ensure appropriate separation of duties, over audit logging, monitoring, and reporting.

- Evaluating the adequacy of user awareness and training for mobile devices.

[43] See FISMA; FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006); NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013); NIST SP 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* June 2013); NIST SP 800-92, *Guide to Computer Security Log Management* (September 2006); NIST SP 1800-5B*, IT Asset Management* (September 2018); NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide* (August 2012), NIST SP 800-175B Rev. 1, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms* (March 2020); *The FDIC Security and Privacy Control Assessment (SCA) Methodology* Version 1.0 (April 2020); OMB Circular A-130 (July 2016); and Executive Order 13589, *Promoting Efficient Spending* (November 2011).

- Selecting a sample of reported incidents involving mobile devices to determine if the FDIC processed the incidents consistent with its policy and guidance.

- Assessing DIT's processes for reviewing billings submitted by wireless carriers to ensure that charges paid by the FDIC were accurate and credits and refunds due to the FDIC were obtained.

- Selecting a sample of terminated employees and contractors to determine if the FDIC removed the users from the MDM solution.

We utilized FISMA, NIST SPs 800-124, Rev. 1, and 800-53, Rev. 4, as the primary criteria for determining whether the FDIC had established and implemented effective controls to secure and manage its mobile devices. We discussed our preliminary exceptions and conclusions with representatives of FDIC management throughout the audit. We performed our work at the FDIC's Virginia Square offices in Arlington, Virginia and remotely as a result of the Coronavirus Disease 2019 (COVID-19) pandemic.

Appendix 2: List of Acronyms

Acronym	Description
BYOD	Bring Your Own Device
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
COPE	Corporate Owned Personally Enabled
CSIRT	Computer Security Incident Response Team
DIT	Division of Information Technology
DLP	Data Loss Prevention
EAMS	Enterprise Asset Management System
EUCS	End User Computing Section
FAQ	Frequently Asked Questions
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
ISPA	Information Security and Privacy Awareness
IT	Information Technology
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
OCISO	Office of Chief Information Security Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
SCA	Security Control Assessment
SEC	Securities and Exchange Commission
SP	Special Publication

Part II

☆☆☆☆☆☆☆☆

FDIC Comments and OIG Evaluation

FDIC Comments and OIG Evaluation

The FDIC's Chief Information Officer (CIO) and Chief Information Security Officer (CISO) provided a written response, dated July 26, 2021, to a draft of the report. The response is presented in its entirety beginning on page II-2. In the response, the CIO and CISO concurred with all nine of the report's recommendations. The recommendations will remain open until we confirm that corrective actions have been completed and are responsive. A summary of the FDIC's corrective actions begins on page II-8.

CONTROLLED//FDIC INTERNAL ONLY

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500
Office of the Chief Information Officer

July 26, 2021

TO: Terry L. Gibson
Assistant Inspector General for Audits, Evaluations, and Cyber

FROM: Sylvia W. Burns
Chief Information Officer and Chief Privacy Officer
Director, Division of Information Technology

SYLVIA BURNS Digitally signed by SYLVIA BURNS Date: 2021.07.26 15:02:17 -04'00'

Zachary N. Brown
Chief Information Security Officer

ZACHARY BROWN Digitally signed by ZACHARY BROWN Date: 2021.07.26 17:44:21 -04'00'

SUBJECT: Management Response to the Draft Audit Report Titled *Audit of the FDIC's Security and Management of Mobile Devices* (Assignment No. 2019-010)

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, titled *The Audit of the FDIC's Security and Management of Mobile Devices*, issued on July 7, 2021. The FDIC recognizes the objective of the audit to determine the effectiveness of implemented controls to secure and manage the FDIC's mobile devices through the Corporation's Mobile Device program. We appreciate the OIG's assessment and findings including the OIG's recognition that the FDIC had effective controls in three key areas, including the critical area of Data Protection. The CIO Organization's (CIOO) core objective for the mobile device program is to maintain a platform to allow users to perform business functions while providing a safe and secure platform to ensure data availability, integrity and confidentiality.

In its report, the OIG/Cotton & Company Inc. (C&C) audit team made nine recommendations to the Chief Information Officer (CIO). As a result of the audit and subsequent discussions, the CIOO concurs with each of the nine recommendations. The issues identified in the report represent opportunities for the FDIC to improve the Mobile Device Management (MDM) program and better ensure policies and procedures are applied consistent with OMB policy, NIST guidance, and internal security policies.

The OIG assessed the MDM program in nine control areas. OIG found controls related to Asset Management, Incident Response, and Data Protection to be Effective. OIG found controls related to Awareness Training, Billing Analysis, and Configuration Management to be Partially Effective. OIG found controls related to Policies, Procedures and Guidance; Control Assessments; and Logging and Monitoring to be Not Effective. The FDIC will address the recommendations issued by the OIG associated with those control areas that the OIG found to be less than effective.

The CIOO continuously strives to improve the MDM program and enhance our information security risk posture through various activities. These activities have allowed us to identify control gaps and take appropriate actions to remediate risk. We believe actions we have

completed or are currently pursuing, along with actions we will take in response to the audit recommendations, will further improve and strengthen the FDIC's MDM program.

CONTROLLED//FDIC INTERNAL ONLY

MANAGEMENT RESPONSE

Recommendation 1 –

We recommend that the CIO:

1. Perform a documented assessment of risks associated with BYOD and the personal use of COPE devices, including the installation and use of mobile applications, text messaging, and audio and video capabilities.

   Management Decision: Concur

   Corrective Action: The CIOO will perform and document a risk assessment of the personal use of COPE devices, including the installation and use of mobile applications, text messaging, and audio and video capabilities. The CIOO will document its decision to discontinue the BYOD program, including evidence that the program has been terminated.

   Estimated Completion Date: 1/30/2022

Recommendation 2 –

We recommend that the CIO:

2. Establish mobile device policies and guidance that align with NIST and GAO recommended practices. The policies and guidance should (a) reflect the FDIC's current business practices for mobile devices and (b) be based on the documented assessment of risks in Recommendation 1.

   Management Decision: Concur

   Corrective Action: The CIOO will update mobile device policies and relevant guidance that aligns with applicable federal regulatory requirements including NIST controls and will consider implementing recommended practices issued by authorities such as the GAO based on the FDIC's operating environment, current business practices, and the results of the risk assessment we will conduct in response to Recommendation 1.

   Estimated Completion Date: 5/30/2022

Recommendation 3 –

We recommend that the CIO:

3. Require users of BYOD to consent to rules of behavior in a mobile device security agreement.

   Management Decision: Concur

Corrective Action: The CIOO has initiated the process to end the BYOD program and remove the limited number of devices (23) enrolled in the program. Remediation of the recommendation will be fulfilled by completing the activities needed to retire the program.

Estimated Completion Date: 12/30/21

Recommendation 4 –

We recommend that the CIO:

4. Define and document roles, responsibilities, and procedures for reviewing audit logs generated by the MDM solution.

Management Decision: Concur

Corrective Action: The CIOO will establish a standard operating procedure that defines roles, responsibilities and the procedures for reviewing audit logs generated by the MDM solution.

Estimated Completion Date: 12/30/21

Recommendation 5 –

We recommend that the CIO:

5. Separate responsibilities for performing systems administration from conducting reviews of audit logs generated by the MDM solution.

Management Decision: Concur

Corrective Action: The CIOO will separate responsibilities for performing systems administration from conducting reviews of audit logs generated by the MDM solution based on actions taken and documented to address Recommendation 4

Estimated Completion Date: 12/30/21

Recommendation 6 –

We recommend that the CIO:

6. Develop and implement awareness training to address risks and security practices related to the use of mobile devices.

Management Decision: Concur

Corrective Action: OCISO will coordinate with Corporate University to update the Corporation's information security and privacy awareness training, including expanded guidance relating to the use of mobile devices.

Estimated Completion Date: 2/28/2022

Recommendation 7 –

We recommend that the CIO:

7. Implement a process to routinely report usage information for mobile devices and MiFi devices to business units in the FDIC's Divisions and Offices.

Management Decision: Concur

Corrective Action: The CIOO will establish a process to report usage information for mobile device assets to business units in the FDIC's Divisions and Offices.

Estimated Completion Date: 3/31/22

Recommendation 8 –

We recommend that the CIO:

8. Require the FDIC's Divisions and Offices to provide EUCS with documentation to support the continued business need for zero usage devices and take action to suspend or terminate unnecessary devices and services.

Management Decision: Concur

Corrective Action: The CIOO will establish a process to ensure Divisions and Offices provide approvals from managers to support continued business need for zero usage devices and take actions accordingly.

Estimated Completion Date: 3/31/22

Recommendation 9 –

We recommend that the CIO:

9. Develop and implement written policies and/or procedures that define roles, responsibilities, and requirements for testing mobile device software updates and documenting the associated results before users are permitted to download and install them.

Management Decision: Concur

Corrective Action: The CIOO will develop a Standard Operating Procedure (SOP) for testing mobile device software updates and document testing results before users are permitted to download and install such updates.

Estimated Completion Date: 12/30/21

If you have any questions regarding this response, please contact Montrice Yakimov, Chief, IT Risk Governance and Policy, Enterprise Strategy Branch, at monyakimov@FDIC.gov.

cc: E. Marshall Gentry, Director, Office of Risk Management and Internal Controls
Greg S. Kempic, Office of Risk Management and Internal Controls
Jennah Mathieson, Deputy Director, Enterprise Strategies Branch

This table presents management's response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The CIOO will perform and document a risk assessment of the personal use of COPE devices, including the installation and use of mobile applications, text messaging, and audio and video capabilities. The CIOO will document its decision to discontinue the BYOD program, including evidence that the program has been terminated.	January 30, 2022	$0	Yes	Open
2	The CIOO will update mobile device policies and relevant guidance that aligns with applicable federal regulatory requirements including NIST controls and will consider implementing recommended practices issued by authorities such as the GAO based on the FDIC's operating environment, current business practices, and the results of the risk assessment the CIOO will conduct in response to Recommendation 1.	May 30, 2022	$0	Yes	Open
3	The CIOO has initiated the process to end the BYOD program and remove the limited number of devices (23) enrolled in the program. Remediation of the recommendation will be fulfilled by completing the activities needed to retire the program.	December 30, 2021	$0	Yes	Open
4	The CIOO will establish a standard operating procedure that defines roles, responsibilities, and the procedures for reviewing audit logs generated by the MDM solution.	December 30, 2021	$0	Yes	Open
5	The CIOO will separate responsibilities for performing systems administration from conducting reviews of audit logs generated by the MDM solution based on actions taken and documented to address Recommendation 4.	December 30, 2021	$0	Yes	Open
6	OCISO will coordinate with Corporate University to update the Corporation's information security and privacy awareness training,	February 28, 2022	$0	Yes	Open

	including expanded guidance relating to the use of mobile devices.				
7	The CIOO will establish a process to report usage information for mobile device assets to business units in the FDIC's Divisions and Offices.	March 31, 2022	$0	Yes	Open
8	The CIOO will establish a process to ensure Divisions and Offices provide approvals from managers to support the continued business need for zero usage devices and take actions accordingly.	March 31, 2022	$0	Yes	Open
9	The CIOO will develop a Standard Operating Procedure for testing mobile device software updates and document testing results before users are permitted to download and install such updates.	December 30, 2021	$0	Yes	Open

[a] Recommendations are resolved when —

1. Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.
2. Management partially concurs or does not concur with the recommendation, but alternative action meets the intent of the recommendation.
3. Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Recommendations will be closed when the OIG confirms that corrective actions have been completed and are responsive.

Federal Deposit Insurance Corporation
Office of Inspector General

3501 Fairfax Drive
Room VS-E-9068
Arlington, VA 22226

(703) 562-2035

★★★★★★

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding FDIC programs, employees, contractors, or contracts, please contact us via our Hotline or call 1-800-964-FDIC.