OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS

Opportunities Exist To Improve the SEC's Management of Mobile Devices and Services

MEMORANDUM

September 30, 2020

TO: Kenneth Johnson, Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General

SUBJECT: *Opportunities Exist To Improve the SEC's Management of Mobile Devices and Services,* Report No. 562

Attached is the Office of Inspector General (OIG) final report detailing the results of our audit of the U.S. Securities and Exchange Commission's (SEC) management of mobile devices and services. The report contains seven recommendations that should help improve the SEC's management of mobile devices and services.

On September 18, 2020, we provided management with a draft of our report for review and comment. In its September 25, 2020, response, management concurred with our recommendations. We have included management's response as Appendix V in the final report.

Within the next 45 days, please provide the OIG with a written corrective action plan that addresses the recommendations. The corrective action plan should include information such as the responsible official/point of contact, timeframe for completing required actions, and milestones identifying how management will address the recommendations.

We appreciate the courtesies and cooperation extended to us during the audit. If you have questions, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects.

Attachment

cc: Jay Clayton, Chairman
      Sean Memon, Chief of Staff, Office of Chairman Clayton
      Bryan Wood, Deputy Chief of Staff, Office of Chairman Clayton
      Kimberly Hamm, Chief Counsel/Senior Policy Advisor, Office of Chairman Clayton
      John Moses, Managing Executive, Office of Chairman Clayton
   Hester M. Peirce, Commissioner
      Benjamin Vetter, Counsel, Office of Commissioner Peirce
   Elad L. Roisman, Commissioner
      Matthew Estabrook, Counsel, Office of Commissioner Roisman
   Allison Herren Lee, Commissioner
      Andrew Feller, Counsel, Office of Commissioner Lee
   Caroline A. Crenshaw, Commissioner

Armita Cohen, Counsel, Office of Commissioner Crenshaw
Gabriel Benincasa, Chief Risk Officer
Matthew Keeler, Management and Program Analyst, Office of Chief Risk Officer
Holli Heiles Pandol, Director, Office of Legislative and Intergovernmental Affairs
John J. Nester, Director, Office of Public Affairs
Robert B. Stebbins, General Counsel
David Bottom, Director/Chief Information Officer, Office of Information Technology
Andrew Krug, Chief Information Security Officer, Office of Information Technology
Bridget Hilal, Branch Chief, Cyber Risk and Governance Branch, Office of Information Technology
Vance Cathell, Director, Office of Acquisitions
Michael Whisler, Assistant Director, Office of Acquisitions
Nick Chung, Competition Advocate/Small Business Specialist, Office of Acquisitions

EXECUTIVE SUMMARY

Opportunities Exist To Improve the SEC's Management of Mobile Devices and Services

REPORT NO. 562 | SEPTEMBER 30, 2020

WHY WE DID THIS AUDIT

Executive Order 13589 directed Federal agencies to assess information technology (IT) device inventories and usage, and to establish controls to ensure agencies do not pay for unused or underused IT equipment, including smartphones and tablets (collectively referred to as mobile devices). The Office of Management and Budget also published guidance for acquiring and managing mobile devices and services. Although mobile devices offer greater workplace flexibilities, they are susceptible to security compromise; are vulnerable to theft, loss, or damage; and create challenges for ensuring the confidentiality, integrity, and availability of the information they access, store, and process.

We conducted this audit to evaluate the U.S. Securities and Exchange Commission's (SEC or agency) management of mobile devices and services. Specifically, we assessed the agency's (1) controls for managing costs associated with SEC-issued mobile devices in fiscal year (FY) 2019 and in the first quarter of FY 2020 (that is, between October 2018 and December 2019); and (2) efforts to safeguard SEC information accessed, stored, or processed on mobile devices with access to the agency's network in FY 2020.

WHAT WE RECOMMENDED

We made seven recommendations to improve the SEC's management of mobile devices and services. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action. This report contains non-public information about the SEC's information technology program. We redacted the non-public information to create this public version.

WHAT WE FOUND

The SEC's employees and contractors use mobile devices to perform their work and access SEC information. According to agency usage reports, between October 2018 and December 2019, the SEC spent nearly $5 million on about 6,300 mobile devices and associated services. The agency used enterprise-wide contracts and a mobile device management system to implement safeguards. However, the SEC has not effectively managed its mobile devices and associated costs.

Specifically, about half of the devices on the SEC's primary wireless service provider usage reports during the period we reviewed were either unused or appeared to be underused, while other devices appeared to have high data usage, in some cases for potentially unauthorized purposes. In addition, the SEC did not (1) provide evidence to support and justify international charges; (2) consistently maintain documentation to demonstrate the continued business need for devices; and (3) adequately plan for the replacement of mobile devices and services. These conditions occurred because the agency's Office of Information Technology (OIT) did not establish and/or implement controls, including comprehensive processes and procedures, to effectively oversee the SEC's mobile devices and services. As a result, the SEC:

- did not leverage available information to effectively manage mobile devices and services, thereby wasting almost $732,000 on 1,567 devices with zero usage between October 2018 and December 2019;

- spent nearly $160,000 on international charges between July and December 2019 without documented justifications to support that those costs were for valid business needs; and

- spent about $1 million in FY 2019 to replace mobile devices at a higher price instead of procuring mobile device models available at no or lower additional cost without a documented justification.

To safeguard information accessed, stored, and processed on mobile devices, the SEC took steps to improve mobile device security controls during our audit. For example, in FY 2020, OIT assessed the security of mobile devices enrolled in the mobile device management system, made progress to ensure those devices used more recent operating system versions, and incorporated mobile device security into the SEC's annual privacy and information security awareness training program. However, additional safeguards are needed to adequately document security controls applicable to mobile devices and improve policies and procedures addressing mobile device inventory controls, provisioning, applications, sanitization, and operating system updates. Also, OIT should implement controls to effectively mitigate the risk of allowing certain mobile devices to access the SEC's network. Because OIT had not developed comprehensive policies and procedures specific to mobile device security or adequate processes to ensure compliance with recognized major controls affecting enterprise mobile device security, the SEC's processes did not adequately ensure compliance, assess risk, identify issues, or mitigate vulnerabilities specific to mobile device security.

We also identified a matter related to the effectiveness of the SEC's mobile device sanitization process that did not warrant recommendations. We discussed this matter with agency management for their consideration.

Contents

Tables and Figure

Abbreviations

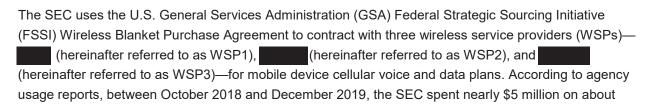|	
App	application
███	██████████████████
FSSI	Federal Strategic Sourcing Initiative
FY	fiscal year
GAO	U.S. Government Accountability Office
██	████
GFE	government furnished equipment
GSA	U.S. General Services Administration
██	████████████
██	████████
IT	information technology
MDM	mobile device management system
NIST	National Institute of Standards and Technology
OA	Office of Acquisitions
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
SEC or agency	U.S. Securities and Exchange Commission
SECR	SEC administrative regulation
SP	Special Publication
SSP	system security plan
WSP	wireless service provider

Background and Objectives

BACKGROUND

The U.S. Securities and Exchange Commission's (SEC or agency) employees and contractors use smartphones and tablets (collectively referred to as mobile devices) to perform their work and to access SEC information resources anywhere and at any time. The SEC spends about $3.6 million each year on mobile devices and services, and manages an inventory of thousands of mobile devices. Executive Order 13589, issued in November 2011, directed Federal agencies to assess device inventories and usage, and to establish controls to ensure agencies do not pay for unused or underused information technology (IT) equipment, including mobile devices.[1] In addition, in May 2012, the Office of Management and Budget (OMB) published a digital government strategy governing, among other things, the purchase and management of mobile devices across the government.[2] As part of the strategy, and to promote fiscal responsibility, OMB required agencies to develop and maintain an enterprise-wide inventory of their mobile devices and wireless service contracts, and to include an evaluation of government-wide contract vehicles in their alternatives analysis for all new mobile-related procurements. In August 2016, OMB published additional guidance for acquiring and managing mobile devices and services, noting that the Federal Government cannot efficiently and effectively buy mobile devices and services if it does not have visibility into what it buys, or if it does not know what it needs to help fulfill agency missions.[3]

Although mobile devices with computing capabilities offer greater workplace flexibility, they (1) are susceptible to security compromise; (2) are vulnerable to theft, loss, and damage; and (3) create challenges for ensuring the confidentiality, integrity, and availability of the information they access, store, and process. According to the National Institute of Standards and Technology (NIST), security controls and control enhancements focus on the fundamental safeguards necessary to protect information during processing, while in storage, and during transmission.[4] Therefore, mobile device programs with an inadequate set of safeguards may result in the compromise and/or unauthorized access of agency data including, but not limited to, non-public or personally identifiable information.

The SEC uses the U.S. General Services Administration (GSA) Federal Strategic Sourcing Initiative (FSSI) Wireless Blanket Purchase Agreement to contract with three wireless service providers (WSPs)— ▮▮▮▮ (hereinafter referred to as WSP1), ▮▮▮▮ (hereinafter referred to as WSP2), and ▮▮▮▮ (hereinafter referred to as WSP3)—for mobile device cellular voice and data plans. According to agency usage reports, between October 2018 and December 2019, the SEC spent nearly $5 million on about

---

[1] Executive Order 13589, *Promoting Efficient Spending*; November 2011.

[2] Office of Management and Budget, *Digital Government: Building a 21st Century Platform to Better Serve the American People*; May 2012.

[3] Office of Management and Budget, M-16-20, *Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services*; August 2016.

[4] NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4; April 2013.

6,300 mobile devices and associated services across the three WSPs, with about 98 percent of the total cost paid to WSP1, the primary WSP.[5] With each WSP, the agency used multiple rate plans, including pooled and unlimited voice and data plans, allowing a large number of users to share and allocate their plan minutes and data. Table 2 in Appendix II summarizes the SEC's mobile device and service costs for the period we reviewed, by WSP and rate plan.

The SEC uses the ██ to manage its inventory of hardware assets, including mobile devices. The agency's Office of Information Technology (OIT) conducts annual capital asset inventories, biennial accountable asset inventories, and periodic spot checks to track and maintain accountability of the SEC's hardware assets. According to ████ inventory reports, as of January 2020, the SEC had an inventory of 5,120 SEC-issued mobile devices. As Table 1 shows, 5,037 of these devices (or about 98 percent) were ████ mobile devices—such as ████████ (hereinafter referred to as smartphones) and ████████ which OIT remotely manages using a mobile device management system (MDM) known as ████████ OIT also uses the MDM to manage contractor-issued mobile devices that access SEC resources (that is, mobile devices that contractor companies issue to their personnel to perform work at the SEC).

TABLE 1. Type and Number of Mobile Devices in ████ Inventory, as of January 2020

Type of Mobile Device	Number of Mobile Devices
████	4,637
██	400
Other Tablet (such as ████████)	48
████████	23
Cell Phone (such as ████████)	11
Wireless Card	1
Total	**5,120**

Source: Office of Inspector General (OIG)-generated based on the January 2020 ████ inventory report.

SEC Roles and Responsibilities

The SEC's Office of Acquisitions (OA) supports all aspects of the agency's procurement and contract administration, including the procurement of mobile devices and services, whereas OIT has overall management responsibility for the SEC's IT program. The following OIT groups are involved in the SEC's management of mobile devices and services:

Network Operations Branch. OIT's Network Operations Branch is responsible for managing and designing the SEC's telecommunication infrastructure, including its mobile device infrastructure. This includes specifying the agency's mobile device infrastructure requirements, coordinating with

---

[5] This includes about $1 million for acquiring mobile devices and nearly $4 million for associated voice and data plans.

OA to acquire mobile devices and services that meet SEC requirements, and monitoring WSPs' deliverables for compliance with contract terms.

Customer Services Branch. OIT's Customer Services Branch provides first-level support for SEC customers for general IT needs, including mobile device needs. This includes issuing SEC mobile devices to authorized agency and contractor personnel, provisioning and enrolling SEC-issued and contractor-issued mobile devices in the MDM,[6] and assisting users with making changes to their device settings.

OIT Information Security Organization. The OIT Information Security Organization is responsible for implementing and maintaining technical controls to protect SEC information systems, networks, and telecommunications. OIT Information Security is also responsible for developing, implementing, and maintaining information security policies, procedures, standards, and guidelines. This includes establishing, documenting, and approving the security configurations of the SEC's mobile device infrastructure, and defining the agency's mobile device security policies.

Infrastructure Engineering Branch. OIT's Infrastructure Engineering Branch is responsible for the MDM infrastructure. This includes implementing mobile device security policies and profiles in coordination with the OIT Information Security Organization, and testing and implementing the MDM and ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ updates.

IT Asset Management Branch. The IT Asset Management Branch provides accountability and oversight of IT assets across the SEC. This includes receiving IT equipment and assets, including mobile devices, and managing and accounting for the agency's IT equipment and asset inventory.

OBJECTIVES

Our overall objective was to evaluate the SEC's management of mobile devices and services. Specifically, we assessed the SEC's:

1. controls for managing costs associated with SEC-issued smartphones and tablets in fiscal year (FY) 2019 and the first quarter of FY 2020 (that is, between October 2018 and December 2019); and

2. efforts to safeguard SEC information accessed, stored, or processed on mobile devices with access to the agency's network in FY 2020.

To address our objectives, we (1) interviewed staff from OA and OIT; (2) reviewed applicable Federal guidance and SEC regulations, policies, and procedures; (3) reviewed OIT and OA risk control matrices and management assurance statements for FY 2019; and (4) identified and assessed internal controls

---

[6] According to NIST SP 1800-4, *Mobile Device Security: Cloud and Hybrid Builds* (February 2019), mobile device provisioning and enrollment includes identifying and associating specific mobile devices with organizational user accounts to ensure that remote access is granted only to authorized users using approved devices.

relevant to our audit. In addition, we used analytical tools to review mobile device data such as mobile device usage reports, MDM reports, electronic invoices, and ▉▉▉▉ inventory reports. We also performed other tests and assessments using nonstatistical, judgmental samples to determine whether the SEC (1) issued mobile devices to users based on need and in accordance with SEC guidance, (2) consistently implemented mobile device security configurations in accordance with agency and Federal security baselines, (3) decommissioned lost or stolen mobile devices in a timely manner, and (4) ensured mobile devices awaiting to be disposed were effectively sanitized.

Appendix I includes additional information about our scope and methodology, including our review of relevant internal controls and prior coverage. Appendix II summarizes the SEC's mobile device and service costs for the period we reviewed, by WSP and rate plan. Appendix III provides examples of ▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉ ▉▉▉▉▉▉▉▉▉▉▉ for the SEC's mobile device program, as further discussed in Finding 2. Appendix IV includes our calculation of monetary impact (that is, unsupported costs) we identified during our audit.[7]

---

[7] As Appendix IV states, we relied on the Inspector General Act of 1978, as amended (Public Law 95- 452; 5 U.S.C. App.), to define unsupported costs.

Results

FINDING 1. THE SEC HAS PROCESSES FOR PROCURING AND ISSUING MOBILE DEVICES, BUT HAS NOT EFFECTIVELY MANAGED MOBILE DEVICES AND ASSOCIATED COSTS

An Executive Order and OMB guidance directed agencies to better manage mobile device spending. To manage its own operations, the SEC established an acceptable use policy, a high-level directive governing mobile devices, and processes for procuring mobile devices and services using enterprise-wide contracts under the GSA FSSI wireless program. However, the agency has not effectively managed its mobile devices and associated costs. This occurred because OIT did not establish and/or implement controls, including comprehensive processes and procedures, to effectively oversee the SEC's mobile devices and services based on business needs and good governance.[8] As a result, the SEC:

- did not leverage available information to effectively manage mobile devices and services, thereby wasting almost $732,000 on 1,567 devices with zero usage between October 2018 and December 2019;[9]

- spent nearly $160,000 on international charges between July and December 2019 without documented justifications to support that those costs were for valid business needs; and

- spent about $1 million in FY 2019 to replace mobile devices at a higher price instead of procuring mobile device models available at no or lower additional cost without a documented justification.

Federal Guidance and SEC Policy for Managing Mobile Devices and Services

As previously discussed, Executive Order 13589 addresses the need for agencies to assess current device inventories (including mobile device inventories) and usage. The Executive Order also states that agencies should take steps to limit the number of IT devices (including mobile devices) issued to employees. Moreover, OMB's 2012 digital government strategy sought to ensure that the government seized opportunities to procure and manage devices in smart, secure, and affordable ways. With the issuance of OMB Memorandum M-16-20 in 2016, OMB encouraged agencies to:

- reduce the number of contracts for mobile devices and services;

- transition to a government-wide solution(s); and

---

[8] According to the Comptroller General of the United States, good governance in the public sector is critical to fulfill the government's responsibility to citizens and taxpayers (GAO-07-78CG; April 2007).

[9] The 2018 revision to the *Government Auditing Standards* (GAO-18-568G, July 2018) states, "Waste is the act of using or expending resources carelessly, extravagantly, or to no purpose. Importantly, waste can include activities that do not include abuse and does not necessarily involve a violation of law. Rather, waste relates primarily to mismanagement, inappropriate actions, and inadequate oversight."

- optimize the level of service acquired by analyzing over and under usage and establishing and enforcing agency-wide policies for identifying and terminating unused devices and services.

OMB Memorandum M-16-20 makes it clear that, "the Federal Government cannot efficiently and effectively buy mobile devices and services if it does not have visibility into what it buys today or if it does not know what it needs to help fulfill agency missions." According to the Memorandum, "too often, agencies buy excessive levels of service, such as unlimited data and minute plans, when a lesser amount of data or number of minutes pooled across many thousands of users would meet the demands of the agency without risk of overage charges."

At the SEC, OIT's high-level directive governing the agency's mobile devices discusses the importance of establishing a business need before management grants eligible employees a device.[10] According to the directive, "the SEC offers mobile devices as another tool for performing assigned duties and to facilitate the appropriate use of this technology for work-related purposes." In addition, according to the SEC's administrative regulation (SECR) on the acceptable use of agency IT resources, government-provided IT resources (including mobile devices) are intended for official and

> *Government-provided IT resources are for official and authorized purposes*

authorized purposes, and employees are permitted to make limited ("de minimis") use of those resources for personal purposes.[11] However, the permission for limited personal use does not create a right to use SEC IT resources for non-governmental purposes, or extend to modifying equipment, including loading personal software or making configuration changes, such as installing video streaming applications (apps).

Despite Federal guidance and agency policy regarding good mobile device governance, the SEC has not effectively managed its mobile devices and associated costs. As further discussed in the sections that follow, we found that:

- about half of the devices on the SEC's WSP1 usage reports from October 2018 through December 2019 were either unused or appeared to be underused, while other devices appeared to have high data usage, in some cases without validating that such usage was for authorized purposes;

- the SEC did not provide evidence to support and justify international charges incurred by users of SEC mobile devices;

---

[10] OIT Directive 24-4.3-PD-01, *Hand Held Communication (Mobile) Devices Operating Procedure*; October 2016.

[11] SECR 24-4.3, *Acceptable Use Of SEC Information Technology Resources,* Revision 5; May 2018. This SECR defines "de minimis" as personal use that involves negligible additional expense to the Government and does not disrupt or interfere with operations.

- the SEC did not consistently maintain documentation to demonstrate the continued business need for mobile devices; and

- the SEC did not adequately plan for the replacement of mobile devices and services.

Devices Were Either Unused or Were Potentially Underused, While Others Had High Data Usage for Potentially Unauthorized Purposes

OIT receives from each of the three WSPs monthly usage reports that include charges for total data, voice, and text messages, as well as international charges. In addition, at least every 6 months, OIT receives from each WSP a rate plan analysis report that includes the SEC's historical spending. As previously stated, about 98 percent of the SEC's mobile device costs were paid to WSP1. Based on the two WSP1 rate plan analysis reports we reviewed (covering September 2018 to August 2019), and consistent with the WSP1 contract, the data available per user was generally ▮▮▮▮▮▮▮ per month under the pooling plans.[12] We reviewed the SEC's WSP1 usage reports from October 2018 through December 2019, detailing usage for 6,339 mobile devices, and determined the following:

- **1,573 devices (or about 25 percent) had zero data usage for the entire period reviewed.** This included 1,567 devices with zero data, no voice, and no text messaging. The remaining 6 devices each had zero data, less than 330 voice minutes, and less than 90 text messages for the entire period reviewed.

- **1,643 devices (or about 26 percent) appeared to be underused based on their data usage.** Although OIT did not establish specific definitions or usage thresholds, for the purposes of this audit and as Appendix I explains, we defined "potential underuse" as average monthly data usage between ▮▮▮▮▮ and ▮▮▮▮▮ (or data usage of less than ▮▮▮ for the entire period reviewed).

- **199 devices (or about 3 percent) appeared to have high data usage.** As previously stated, OIT did not establish specific definitions or usage thresholds. For the purposes of this audit and as Appendix I explains, we defined "potential high usage" as average monthly data usage above ▮▮▮▮▮.

- **The remaining 2,924 devices (or about 46 percent) had an average monthly data usage between ▮▮▮▮ and ▮▮▮▮▮** This included 2,885 devices with average monthly data usage within the ▮▮▮ available per user, and 39 devices with average monthly data usage between ▮▮▮ and ▮▮▮▮.

Figure 1 on the next page depicts the distribution of the devices within each category.

---

[12] A small number of users assigned devices had unlimited data plans. According to WSP1's online calculator, using ▮▮▮ of data in a month corresponds to sending and receiving about 30,000 e-mails.

FIGURE 1. WSP1 Average Monthly Data Usage, October 2018 through December 2019

Source: OIG-generated based on WSP1 usage reports from October 2018 through December 2019 provided by OIT.

Although the 199 devices with the highest average monthly data usage exceeded the potential available data for pooled plans (specified in rate plan analysis reports), the devices had a pooled rate plan.[13] Therefore, the SEC did not incur additional usage charges. Nonetheless, the U.S. Government Accountability Office (GAO) reported that, "while contracts with unlimited or shared usage can help limit the risk of incurring charges from overuse, they can increase the risk that agencies are paying for unused service on infrequently used devices. Thus, reliance on plans providing unlimited or shared usage is not an effective substitute for adequate oversight of device-level usage."[14]

In addition, based on available information, we could not determine how the data was used, for what purpose, or whether users exceeded the standard for limited personal use of government-provided IT resources. We were able to establish the total data used by each device using, primarily, the WSP usage reports. Moreover, we determined that 12 of the 20 devices (or 60 percent) with the highest average monthly data usage during the period we reviewed—and many other SEC mobile devices with less usage—included apps that did not appear to relate to the business of the SEC and that were not part of OIT's catalog of approved apps.[15] This included, but was not limited to, video streaming apps, messaging apps, children's apps, and/or social media apps. One of the 12 devices with the highest data usage had 118 apps installed, including ████████ which is included in OIT's list of prohibited apps, whereas other

---

[13] Only 2 of the 199 devices (or about 1 percent) had an unlimited plan. The remaining 197 devices had a pooled plan.

[14] U.S. Government Accountability Office, *Telecommunications – Agencies Need Better Controls to Achieve Significant Savings on Mobile Devices and Services* (GAO-15-431; May 2015).

[15] The remaining eight devices included seven that did not have any unapproved apps, and one device that was not enrolled in the MDM (and which OIT recommended for disconnection).

devices with less usage contained shopping, dating, and other entertainment apps. We further discuss the risk of third-party apps and the SEC's lack of ███████ processes in Finding 2.

The SEC Did Not Provide Evidence To Support and Justify International Charges

According to the Federal Acquisition Regulation[16] and SEC policy,[17] contracting officer's representatives assist in the technical monitoring or administration of a contract. Their responsibilities include maintaining adequate contract records and reviewing invoices and charges for accuracy before payment. WSPs' monthly invoices detail the charges incurred by the SEC. We reviewed the invoices received from each of the three WSPs between July and December 2019 and inquired about the business need for international charges, which appeared on the SEC's WSP1 invoices for each of the 6 months we reviewed. We determined that the SEC did not provide evidence to support and justify international charges incurred by users of SEC mobile devices. Therefore, as Appendix IV shows, we consider these charges to be unsupported.[18] During our audit, OIT was developing a policy to address the use of SEC IT equipment, including mobile devices, during international travel.

The SEC Did Not Consistently Maintain Documentation To Demonstrate the Continued Business Need for Mobile Devices

OIT guidance establishes criteria for issuing mobile devices to SEC and contractor personnel, and the documentation requirements.[19] In addition, the SEC uses the MDM to provide secure access to SEC resources. We judgmentally selected 25 out of about 4,100 users of SEC-issued mobile devices included in usage reports from October 2018 through December 2019. We found that OIT did not maintain documentation to demonstrate that 13 of those 25 users (or 52 percent) had a continued business need for the devices, or to demonstrate that the users met the agency's eligibility criteria for receiving a device. The 13 users included former SEC and contractor employees, at least 1 of whom left the agency nearly 4 years ago. We also found that about 600 of the nearly 4,800 mobile devices shown in the December 2019 usage reports from all three WSPs (or about 13 percent) were not enrolled in the MDM, and therefore did not have access to SEC resources such as e-mail. OIT could not provide documentation to demonstrate the continued business need for these 600 devices, which also included devices assigned to former SEC employees who separated from the agency years ago. Although the former employees' devices we identified were no longer active, the devices still appeared in WSP usage reports and invoices. During our audit, OIT reconciled the usage reports to the MDM, and suspended the 600 devices we questioned.

---

[16] Title 48 of the Code of Federal Regulations, *Federal Acquisition Regulations System* (Revised); March 2005.

[17] OA Operating Procedure 1, *Acquisition*, (May 2019) prescribes the SEC's acquisition policies, responsibilities, and procedures.

[18] As defined by the Inspector General Act of 1978, as amended (Public Law 95–452; 5 U.S.C. App.), unsupported costs are those costs questioned because, at the time of the audit, the costs were not supported by adequate documentation.

[19] ███

The SEC Did Not Adequately Plan for the Replacement of Mobile Devices and Services

As part of an agency-wide smartphone refresh initiative, the SEC replaced mobile devices and services in FY 2019 without adequate planning. OIT officials told us that they decided to upgrade to mobile devices with a higher price instead of procuring mobile device models available at no or lower additional cost, so that the agency maintains its ability to update ▓▓ versions, and to avoid performing another agency-wide refresh event for a period of time. According to OMB Memorandum M-16-20, the Federal Government should evaluate the cost of replacing mobile devices, and "previous generation devices are typically equally capable of meeting all the requirements and needs of a Government user" at potentially lower prices than the latest models. Agency capital planning processes also address the decision criteria that officials should use when selecting IT investments, stating that investment selection criteria should include establishing whether and how proposed investments have been evaluated to determine their benefits and risks from both business and technical perspectives.[20] Although OIT officials provided e-mail communications indicating they had discussed the pricing and technical feasibility of upgrading to higher priced devices, OIT officials did not perform and document an evaluation to determine (1) the cost, type, and quantities of mobile devices and services that needed to be replaced; and (2) the rationale (including the benefits and risks) for upgrading to higher priced devices.

The conditions we observed occurred because OIT did not establish and/or implement controls, including comprehensive processes and procedures, to effectively oversee the SEC's mobile devices and services based on business needs and good governance. Specifically, OIT did not have processes requiring periodic reviews and reconciliations of mobile device usage reports, rate plan analysis reports, and MDM reports. Without such processes, OIT personnel did not review the SEC's mobile device usage to identify and address key indicators of potential inefficient or unauthorized use including overuse, underuse, or zero use. In addition, OIT did not have processes requiring periodic reviews of WSPs' invoices. Without such processes, the contracting officer's representatives responsible for overseeing the SEC's mobile device and services contracts did not review monthly invoices to ensure unusual or additional charges, such as international charges, were accurate, were for authorized purposes, and were adequately supported. Moreover, existing OIT guidance for issuing mobile devices did not include processes to periodically assess and recertify the continued need for mobile devices, did not specify the criteria for assigning rate plans to mobile device users, and did not include a process for communicating assigned plans. Finally, OIT did not define a mobile device program-level acquisition strategy. Notably, a previous OIG audit recommended that OIT establish a uniform refresh plan or a strategic approach for the replacement of hardware assets.[21] As of the date of this report, the audit recommendation remains open.

---

[20] SECR 24-02, *Information Technology Capital Planning and Investment Control*, Revision 2.2; July 2018.

[21] U.S. Securities and Exchange Commission, Office of Inspector General, *The SEC Has Processes To Manage Information Technology Investments But Improvements Are Needed* (Report No. 555, September 2019).

As a result, the SEC did not leverage available information to effectively manage mobile devices and services, thereby wasting almost $732,000 on 1,567 devices with zero usage between October 2018 and December 2019. As further discussed in Appendix IV, the SEC also spent nearly $160,000 on international charges between July and December 2019 without documented justifications to support that those costs were for valid business needs. In addition, the SEC spent about $1 million[22] to replace mobile devices at a higher price instead of procuring mobile device models available under the GSA FSSI Wireless Blanket Purchase Agreement at no or lower additional cost without a documented justification. This procurement, made under the WSP1 contract, included a bulk acquisition of mobile devices for about $700,000, which the agency did not capitalize even though this bulk acquisition was above the capitalization threshold specified in the Office of Financial Management's Reference Guide[23] and in the SECR on property management.[24] The Office of Financial Management reviewed all mobile device acquisitions over the life of the WSP1 contract during our audit, and determined that the bulk acquisition in question was not material to the agency's financial statements. Moreover, the agency's position is that the cost of mobile devices is an incidental cost which is integral to the service being provided and thus should not be capitalized given that the total cost of mobile devices acquired under the WSP1 contract represented less than 10 percent of the overall contract value. However, to ensure the agency's policy is clear, the Office of Financial Management proposed to update applicable guidance to specifically exclude mobile devices from the SEC's capitalization rules in the future.

During our audit, OIT officials stated that the SEC is continuously evolving and improving its processes for managing mobile devices, and OIT suspended some of the devices we identified with zero usage. OIT also initiated quarterly reviews of mobile device usage. However, the roles, responsibilities, and activities involved in the review process were not documented as of the date of this report, and other corrective actions are needed as recommended below.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

To improve the SEC's management of its mobile devices and associated costs, we recommend that OIT:

Recommendation 1:

Assess the continued business need for the devices we identified as unused and potentially underused; and, as appropriate, take action to suspend services to those devices.

> **Management's Response.** Management concurred with the recommendation. According to the Chief Operating Officer, the Office of Information Technology is continuing to work with the vendors to analyze the lines of service identified as unused or potentially underused, and will discontinue

---

[22] Although the SEC received loyalty credits and credits for turning in old devices (totalling $340,392), the agency would have received these credits regardless of the equipment model selected.

[23] The Office of Financial Management's Reference Guide is the repository for the SEC's financial policies and procedures, business process narratives, issue papers, and reference materials.

[24] SECR 9-2, *Property Management Program*, Revision 4; October 2018.

services to any mobile device deemed to no longer have a business need. The Office of Information Technology will also apply the policies and procedures developed pursuant to recommendation 3 to perform ongoing reviews of the continued business need for devices. Management's complete response is reprinted in Appendix V.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 2:

Establish and implement comprehensive processes and procedures and/or update existing guidance to:

a. Require periodic reviews and reconciliations of mobile device usage reports, rate plan analysis reports, and mobile device management sytem reports to identify and address key indicators of potential inefficient or unauthorized use including overuse, underuse, or zero use.

b. Require periodic reviews of wireless service providers' invoices to ensure unusual or additional charges, such as international charges, are accurate, are for authorized purposes, and are adequately supported.

Management's Response. Management concurred with the recommendation. According to the Chief Operating Officer, the Office of Information Technology will establish and implement processes and procedures for performing the periodic reviews described in this recommendation. Management's complete response is reprinted in Appendix V.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 3:

Update existing guidance to include periodic assessments and recertifications of the continued need for mobile devices, specify criteria for assigning rate plans to mobile device users, and establish a process for communicating the plans' limits to users.

Management's Response. Management concurred with the recommendation. According to the Chief Operating Officer, the Office of Information Technology will update existing guidance to include periodic assessments and recertifications of the continued need for mobile devices, specify criteria for assigning rate plans to mobile device users, and establish a process for communicating the plans' limits to users. Management's complete response is reprinted in Appendix V.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 4:

Define an agency-wide mobile device program-level acquisition strategy, including conditions and criteria for approving the procurement of mobile devices that meet defined SEC requirements.

Management's Response. Management concurred with the recommendation. According to the Chief Operating Officer, the Office of Information Technology will formalize and document its acquisition strategy for mobile devices prior to the next program-level acquisition. The strategy will be linked to the agency's capital planning and investment control guidance for steady state acquisitions, and will define the proposed timeframes, list the documents required, and identify the steps required for this type of investment. Management's complete response is reprinted in Appendix V.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

FINDING 2. THE SEC HAS TAKEN STEPS TO SAFEGUARD INFORMATION ACCESSED, STORED, AND PROCESSED ON MOBILE DEVICES, BUT ADDITIONAL SAFEGUARDS ARE NEEDED

NIST SP 800-53 presents the state-of-the-practice safeguards (that is, security controls) for Federal information systems and organizations necessary to protect information during processing, while in storage, and during transmission. In addition, NIST SP 800-124 identifies controls specific to mobile devices.[25] To ensure information accessed, stored, and processed on mobile devices is safeguarded, the SEC took steps to improve mobile device security controls during our audit. For example, in FY 2020, OIT performed a security assessment of mobile devices enrolled in the MDM. In addition, OIT made progress in ensuring that mobile devices enrolled in the MDM use more recent operating system versions.

Furthermore, OIT incorporated mobile device security into the SEC annual privacy and information security awareness training program. However, additional improvements are needed to adequately safeguard SEC mobile devices. Specifically, OIT needs to adequately document

> *Improvements are needed to adequately safeguard SEC mobile devices*

security controls applicable to mobile devices and improve policies and procedures addressing mobile device inventory controls, provisioning, apps, sanitization, and operating system updates. ▮▮▮▮

▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮

▮▮▮▮▮▮▮▮▮ Because OIT had not developed comprehensive policies and procedures specific to mobile device security or adequate processes to ensure compliance with NIST major controls affecting enterprise mobile device security, the SEC's processes did not adequately ensure compliance, assess risk, identify issues, or mitigate vulnerabilities specific to mobile device security.

Federal Guidance Applicable to Mobile Device Security

According to NIST SP 800-53, a system security plan (SSP) is a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. NIST also states "the protection of a system must be documented in [an SSP]." Mobile device security controls include establishing usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and authorizing the connection of mobile devices to organizational information systems. Furthermore, NIST SP 800-124 identifies 21 "major controls" in the NIST SP 800-53 control catalog that affect enterprise mobile device security.

---

[25] NIST SP 800-124, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, Revision 1; June 2013.

OIT Should Adequately Document Security Controls Applicable to Mobile Devices

The General Support System SSP covers aspects of mobile device security controls. However, OIT did not adequately document or detail the security controls applicable to mobile devices in the SEC's General Support System SSP. In addition, OIT did not ███████████████████████████████████████ ████████████████████████████████████ We reviewed security documents such as the (1) General Support System SSP, (2) ██████████ security assessment reports, and (3) MDM configuration baselines, and identified inadequacies in the control details and OIT's implementation of ████████████ controls that affect mobile device security identified in NIST SP 800-124. For examples ███████████████████████████████ see Appendix III.

OIT Should Ensure That the SEC's Mobile Device Inventory is Accurate and Comprehensive

NIST SP 800-124 states that operational processes that are particularly helpful for maintaining mobile device security include "keeping an active inventory of each mobile device, its user(s), and its applications." In addition, according to GAO, a comprehensive inventory is critical to managing mobile device costs.[27] The SECR on property management establishes the SEC's policy for tracking and managing government provided hardware assets (including mobile devices). Although the SEC has established inventory controls to keep track of mobile devices in █████, the SEC's inventory of mobile devices did not accurately and completely reflect the mobile devices connected to the agency's network via the MDM. Specifically, we reconciled the █████ inventory to the MDM and found that, out of about 4,500 mobile devices in the April 2020 MDM report, about 600 mobile devices were not in █████ (that is, we could not identify these devices in ███ ██████████████████████████████ We also found that, out of almost 5,100 devices included in █████ inventory reports, nearly 1,200 were not in the MDM. The remaining 3,900 devices in █████ were in the MDM.

During our audit, OIT reconciled the █████ inventory to the MDM and provided explanations for the discrepancies noted. Certain devices (1) had an incorrect ██████████ (2) were contractor-issued devices not paid for by the SEC (and not tracked in █████; (3) were not yet assigned to a specific user; or (4) were WIFI-only devices or were used by the SEC's ████████████████ OIT also stated that it had performed a periodic reconciliation between █████ and the MDM in March 2020. The SEC's inventory of mobile devices in █████ did not accurately and completely reflect the mobile devices connected to the agency's network, in part, because OIT incorrectly recorded the █████ of certain devices.[28] In addition, OIT did not define which mobile devices should be in the MDM. Also, although OIT

█ ███

[27] U.S. Government Accountability Office, *Telecommunications – Agencies Need Better Controls to Achieve Significant Savings on Mobile Devices and Services* (GAO-15-431; May 2015).

[28] We found that, for nearly 4,700 out of almost 5,100 devices in █████ OIT entered the devices' ████████████████ For the remaining nearly 400 devices, OIT used a █████████████████

reconciled ▮▮▮▮ to the MDM during our audit, OIT inventory control processes did not include a periodic reconciliation between the ▮▮▮ systems.

Without accurate and complete inventories of mobile devices connected to the agency's network, the SEC may be unable to identify and properly mitigate mobile device vulnerabilities. In addition, the agency may not ensure proper accountability over its mobile devices and risks paying for unused or underused mobile devices, as Finding 1 discusses. ▮▮▮ In a previous audit report, we recommended that OIT define and implement a process to develop and maintain up-to-date inventories that include detailed information necessary for tracking and reporting of hardware assets connected to the agency's network.[29] As of the date of this report, the audit recommendation remains open.

OIT Should Consistently Provision Mobile Devices Enrolled in the MDM

The SEC uses the MDM to secure and remotely manage ▮▮▮▮ mobile devices.[30] The MDM allows OIT to assign device profiles to each mobile device. Device profiles represent the settings used to enforce SEC security and compliance policies. From our judgmental sample of 20 SEC-issued mobile devices out of nearly 4,200 SEC devices enrolled in the MDM, we found that 19 ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ the MDM.[31] However, OIT did not provide any documentation supporting these ▮▮▮▮▮▮▮▮▮▮ ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ ▮▮▮▮▮▮▮▮▮ Similarly, from our judgmental sample of 10 ▮▮▮▮▮▮▮ mobile devices enrolled in the MDM, we found that 5 ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ ▮▮▮▮▮▮▮ supporting ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ ▮▮▮▮▮▮▮▮▮ these devices. During our audit, OIT initiated efforts to identify ▮▮▮▮▮▮ ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ on devices enrolled in the MDM.

▮▮
▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮
▮▮
▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮
▮▮

According to NIST SP 800-124, a mobile device security policy should define how provisioning should be handled. In addition, NIST states, "it is important to determine how both new and existing devices will be provisioned with client software, authenticators, configuration settings, etc."

---

[29] U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017* (Report No. 546, March 2018).

[30] As previously discussed, the SEC has a small number of ▮▮▮▮▮▮ mobile devices, which OIT identified as low risk.

[31] During our audit, OIT performed an analysis and identified at least 64 devices with missing or non-standard profiles.

OIT Should Effectively Mitigate the Risk From Untrusted Mobile Device Apps

Mobile devices are designed to make it easy to find, acquire, install, and use third-party apps from mobile device app stores. However, without adequate safeguards, the use of untrusted apps increases the risk of unauthorized access to SEC data. According to NIST SP 800-124, mobile device security considerations include restricting which app stores may be used and restricting which apps may be installed through app "allow lists" (preferable) or "prohibited lists."[32] In addition, NIST includes app vetting as a major consideration for mobile device security. According to NIST, to reduce the risk from untrusted apps, organizations can (1) prohibit all installation of third-party apps; (2) allow installation of approved apps only; or (3) implement a secure container that isolates the organization's data and apps from all other data and apps on the mobile device.

To mitigate the risk from untrusted apps, ███

██

OIT Should Consistently Un-Enroll Lost, Stolen, and Decommissioned Devices From the MDM in a Timely Manner, and Maintain Sanitization Records

According to NIST SP 800-124, mobile device security considerations include remotely wiping (that is, sanitizing) the device if it is lost or stolen and is at risk of having its data recovered by an untrusted party. Furthermore, NIST SP 800-88[33] states that, following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized. NIST also states that verifying the selected information sanitization and disposal process is an essential step in maintaining confidentiality. In addition, Federal guidance recommends that, upon the end-of-life or retirement of a mobile device, agencies consider removing (or un-enrolling) the device's access to the agency's infrastructure via the mobile device management solution, and removing agency asset data from the device.[34] OIT's ████████████ requires users to immediately report all lost or stolen devices to the OIT Service Desk. In addition, OIT's ███████████████████ states all information system media (including mobile devices) that are to be decommissioned must be properly sanitized before disposal, in accordance with NIST. Lastly, the General Support System SSP states a certified record of the sanitization and/or destruction process is maintained in accordance with applicable Federal and organizational standards and policies. ████████████████████████

██

██████████████████

Between October 1, 2018, and December 31, 2019, 92 SEC-issued mobile devices were reported lost or stolen. We found that 22 of these devices ██████████████ in the MDM at least ██████████ after being reported lost or stolen. ████████████████████████████████

██

██

██

██

██

██

██

---

[33] NIST SP 800-88, *Guidelines for Media Sanitization*, Revision 1; December 2014.

[34] *Mobile Security Reference Architecture* (May 2013), a product of the Federal [Chief Information Officer] Council and Department of Homeland Security National Protection and Program Directorate Office of Cybersecurity and Communications Federal Network Resilience.

████████████████████████

████████████████████████████

████████████████████████

███

███

████████████████████████

OIT Should Consistently Prevent Mobile Devices Without the Latest Operating System Updates From Accessing the SEC Network

According to NIST, agencies should ensure that updates and patches are applied promptly to protect the device from attacks against known vulnerabilities.[38] Furthermore, NIST SP 800-124 states that helpful operational processes for maintaining the security of mobile devices include checking for upgrades and patches, and acquiring, testing, and deploying them. █████████████████

███

███

███

████████████████████████

During our audit, OIT took steps to enforce ████ updates by ███████████████████ ████████████ versions. In doing so, OIT reduced the number of ████████████████ ████████████████████████████ Nevertheless,

███

███

███

████████████████████████

Numerous critical vulnerabilities are attributed to older ████ versions. By allowing mobile devices without the latest operating system updates to access the SEC network, the agency is at greater risk of compromise from known risks.

███

████████████████████████

███

███

███

███

███

███

---

[38] NIST SP 800-46, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, Revision 2; July 2016.

████████████████████████████████

████████████████████████████████████
███
██
███
███
████████████████████████████████████
██
██
██
██

According to NIST SP 800-124, each organization should make its own risk-based decisions about what levels of access should be permitted from which types of mobile devices. NIST also states that organizations may have more restrictive requirements for work involving sensitive information, such as permitting only organization-issued devices to be used. In addition, the *Mobile Security Reference Architecture* states that the use of non-GFE devices (such as contractor-issued mobile devices) for agency work "should be governed by a policy of informed consent with some technical enforcement." This guidance also states that, although there is currently no legal precedent to do so, agencies should work with their respective Office of the General Counsel to determine whether their policies or procedures could support the confiscation or destruction of non-GFE under specific circumstances, such as spillage of controlled unclassified information.

███
██
██
██
███
███
███
██
██
█████████████████

Overall, by taking additional steps to improve security policies and procedures for its mobile devices, the agency will reduce the likelihood of compromise, loss, and/or unauthorized access of agency data including, but not limited to, non-public information or personally identifiable information.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

To improve safeguards on information accessed, stored, and processed on mobile devices to mitigate risks of unauthorized disclosure of SEC non-public information and/or personally identifiable information, we recommend that OIT:

Recommendation 5:

Update applicable system security plans to include security controls applicable to mobile devices identified in Federal guidance, and update documentation ████████████████████████ ████████████████████████████████
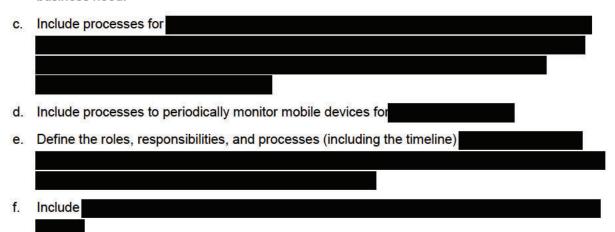
Management's Response. Management concurred with the recommendation. According to the Chief Operating Officer, the agency will review and, if necessary, update the system security plan for the mobile device management system/mobile device environment to be compliant with the most current controls specified in federal guidance, and create or update other documentation necessary ████ ██████████████████ Management's complete response is reprinted in Appendix V.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 6:

Update existing policies and procedures to include additional controls addressing mobile device inventory, provisioning, applications, sanitization, and operating system updates. Specifically, OIT should update existing policies and procedures to:

a. Require a periodic reconciliation between ██████ and the mobile device management system, and clearly define which mobile devices should be enrolled in the mobile device management system.

b. Clearly define the roles, responsibilities, and processes for provisioning devices based on business need.

c. Include processes for ████████████████████████████ ████████████████████████████████ ████████████████████████████████ ████████████████████

d. Include processes to periodically monitor mobile devices for ████████████

e. Define the roles, responsibilities, and processes (including the timeline) ████████████ ████████████████████████████████ ████████████████████████

f. Include ████████████████████████████ ██████

Management's Response. Management concurred with the recommendation. According to the Chief Operating Officer, the Office of Information Technology will review and as necessary, update existing policies and procedures to include additional controls addressing mobile device inventory, provisioning, applications, sanitization, and operating system updates. Management's complete response is reprinted in Appendix V.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 7:

In coordination with the Office of the General Counsel, assess the risk of allowing ███████████ ██████████ ██ ██████ █████████████████████████████ If the agency's determination is to continue ██ ███ ██

Management's Response. Management concurred with the recommendation. According to the Chief Operating Officer, the Office of Information Technology will analyze the risk █████████████████ ████████████████████████████████████ and if this risk is deemed appropriate, the agency will develop policies and processes addressing the use of these devices. Management's complete response is reprinted in Appendix V.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Other Matter of Interest

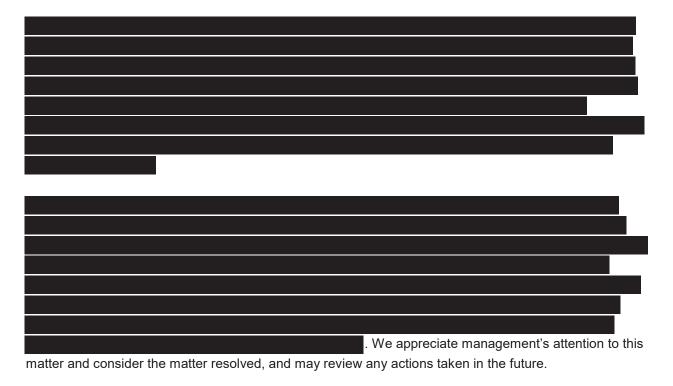During our audit, we identified a matter that did not warrant recommendations. We discussed this matter with agency management for their consideration. The matter, management's response, and our evaluation of management's response are described below.

Effectiveness of the SEC's Mobile Device Sanitization Process

Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other devices, including the unintentional disclosure of sensitive data on decommissioned devices. Sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. According to NIST SP 800-88, parties attempting to obtain sensitive information may seek to focus their efforts on alternative access means such as retrieving residual data on media that has left an organization without sufficient sanitization efforts having been applied. Consequently, applying effective sanitization techniques is a critical aspect of ensuring that sensitive SEC data is effectively protected against unauthorized disclosure.

. We appreciate management's attention to this matter and consider the matter resolved, and may review any actions taken in the future.

Appendix I. Scope and Methodology

We conducted this performance audit from November 2019 through September 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Objective and Scope

Our overall objective was to assess the SEC's management of mobile devices and services. Specifically, we assessed the SEC's (1) controls for managing costs associated with SEC-issued smartphones and tablets in FY 2019 and in the first quarter of FY 2020 (that is, between October 2018 and December 2019); and (2) efforts to safeguard SEC information accessed, stored, or processed on mobile devices with access to the agency's network in FY 2020.

For the purpose of this audit, we limited our review of mobile device and service costs to smartphones and ▮▮▮▮ which represented the vast majority of mobile devices that accessed the SEC's network during the period we reviewed. In addition, we did not assess the security controls of smartphones and tablets that were not enrolled in the MDM because, according to OIT personnel, those devices had limited access to SEC resources. We performed detailed tests of relevant information from the period between October 1, 2018, and December 31, 2019, and remained abreast of developments in the SEC's management of mobile devices and services throughout our audit. We performed fieldwork at the SEC's Headquarters in Washington, DC, although our review included mobile devices issued to SEC employees from across the agency, including its regional offices.

Methodology

To address our objectives, among other work performed, we sent written inquiries to and interviewed officials from OIT and OA to gain an understanding of the SEC's processes for managing mobile devices and services, and safeguarding the information accessed, stored, and processed on mobile devices. In addition, we:

- reviewed applicable Federal guidance;

- reviewed relevant SEC policies, procedures, and administrative regulations, and OIT documents addressing mobile device security risks;

- assessed internal controls relevant to our audit; and

- used analytical tools to review mobile device data (such as inventory reports, MDM reports, and WSPs' invoices and usage reports) from the period we reviewed.

Because OIT did not establish specific definitions or mobile device usage thresholds, for the purposes of this audit, we defined "potential underuse" as average monthly data usage between ▮▮▮▮▮ and ▮▮▮▮▮ (or data usage of less than ▮▮▮ for the entire period reviewed), and "potential high use" as average monthly data usage above ▮▮▮▮ To determine these ranges/categories, we used the frequency distribution to analyze the spread of average monthly data usage reported in WSP1 usage reports between October 2018 and December 2019. We did not analyze the average monthly text usage because WSP1 service plans provide unlimited text per device. In addition, we did not analyze the average monthly voice usage because WSP1 invoices reviewed showed that the SEC received more credit from pooling voice than data.

We also selected and reviewed a number of nonstatistical, judgmental samples. Specifically, to determine whether the SEC issued mobile devices to users based on need and in accordance with SEC guidance, we judgmentally selected and reviewed information relevant to a sample of 25 users with SEC-issued mobile devices out of about 4,100 users included in usage reports during the period we reviewed. To assess whether the SEC consistently implemented mobile device security configurations in accordance with agency and Federal security baselines, we judgmentally selected and reviewed information relevant to 20 SEC-issued mobile devices and 10 ▮▮▮▮▮▮▮▮▮ mobile devices out of about 4,300 devices enrolled in the MDM as of January 17, 2020. In addition, to determine whether the SEC decommissioned lost or stolen mobile devices in a timely manner, we judgmentally selected and reviewed information relevant to 10 of the 92 devices reported lost or stolen during the period we reviewed. Finally, to determine whether mobile devices awaiting disposal were effectively sanitized, we judgmentally selected and performed limited testing of five mobile devices collected from OIT in June 2020. Although these samples were nonstatistical and our results cannot be projected to the total population for each test performed, the evidence we gathered helped support our findings, conclusions, and recommendations.

Internal Controls

We identified and assessed internal controls, applicable internal control components, and underlying principles significant to our objectives, as described below.

Control Environment. We assessed the control environment established by OIT's Network Operations Branch, Customer Services Branch, Information Security Organization, Infrastructure Engineering Branch, and IT Asset Management Branch, as key OIT groups with separate roles and responsibilities for overseeing the SEC's mobile device program.

Risk Assessment. We obtained and reviewed OIT's and OA's FY 2019 management self-assessment statements and risk controls matrices to identify risks and controls related to mobile devices or the SEC's mobile device program. OIT and OA did not identify internal control deficiencies related to mobile devices. We also reviewed OIT security assessment reports, policies, procedures, guidance, and supporting documents to determine whether management identified security risks applicable to mobile devices and clearly defined the objectives of the SEC's mobile device program, including what is to be achieved, who is to achieve it, how it will be achieved, and the timeframes for achievement. In addition, we inquired about OIT's processes for ensuring accurate reporting/accounting treatment of mobile device

acquisitions, and for ensuring the SEC is not paying for unused or underused devices, or for devices used by non-current SEC employees or contractors, or for unauthorized purposes.

Control Activities. We reviewed applicable Federal guidance and SEC policies, procedures, and administrative regulations to identify and test key control activities. We also sent inquiries to responsible personnel to obtain written descriptions of the control activities applicable to mobile devices. Control activities identified and reviewed included the SEC's use of enterprise-wide contract mechanisms; top-level reviews of mobile device usage, including wireless service providers' invoices; security controls over mobile devices; and access restrictions.

Information and Communication. We determined that OIT communicated policies and procedures related to mobile devices to SEC staff through the SEC internal site and the agency's annual privacy and information security awareness training.

Monitoring. We reviewed SEC policies, procedures, and administrative regulations, and discussed with OIT officials their roles and responsibilities for monitoring the cost of SEC mobile devices and services, and in implementing safeguards to secure mobile devices used to access, store, or process SEC information. Monitoring activities reviewed included invoice reviews, inventory control processes, mobile device security baselines and configurations, and security assessment reports.

Based on the work performed, as noted in this report, we identified internal control deficiencies that were significant within the context of our objectives. Our recommendations, if implemented, should correct the weaknesses we identified.

Data Reliability

GAO's *Assessing Data Reliability* (GAO-20-283G, December 2019) states reliability of data means that data are applicable for audit purpose and are sufficiently complete and accurate. Data primarily pertains to information that is entered, processed, or maintained in a data system and is generally organized in, or derived from, structured computer files. Furthermore, GAO-20-283G defines "applicability for audit purpose," "completeness," and "accuracy" as follows:

> "Applicability for audit purpose" refers to whether the data, as collected, are valid measures of the underlying concepts being addressed in the audit's research objectives.

> "Completeness" refers to the extent that relevant data records and fields are present and sufficiently populated.

> "Accuracy" refers to the extent that recorded data reflect the actual underlying information.

To address our objectives, we relied on computer-processed data such as mobile device usage reports, MDM reports, electronic invoices, and ▓▓▓▓ inventory reports. To assess the reliability of usage reports, MDM reports, and electronic invoices, we interviewed OIT officials, performed a walkthrough of the MDM, and reconciled usage reports to invoices. In addition, to assess the reliability of ▓▓▓ inventory reports, we reviewed the SEC OIG report *Audit of the SEC's Compliance With the Federal Information Security*

Modernization Act for Fiscal Year 2017 (Report No. 546, March 2018), which addressed the need for the SEC to define and implement a process to develop and maintain up-to-date inventories that include detailed information necessary for tracking and reporting of hardware assets (including mobile devices) connected to the agency's network. We also analyzed and reconciled ▮▮▮▮ inventory reports to MDM reports. Based on our assessment, we found the data from the usage reports, MDM reports, and electronic invoices sufficiently reliable for the purpose of this audit. We incorporated the discrepancies noted between ▮▮▮▮ inventory reports and MDM reports in Finding 2 of this report.

Prior Coverage

Between 2012 and 2020, the SEC OIG and GAO issued the following reports of particular relevance to this audit.

SEC OIG:

- *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017* (Report No. 546, March 2018).

- *Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 552, December 2018).

- *The SEC Has Processes To Manage Information Technology Investments But Improvements Are Needed* (Report No. 555, September 2019).

- *Fiscal Year 2019 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 558, December 2019).

GAO:

- *Information Security – Better Implementation of Controls for Mobile Devices Should be Encouraged* (GAO-12-757, September 2012).

- *Telecommunications: Agencies Need Better Controls to Achieve Significant Savings on Mobile Devices and Services* (GAO-15-431, May 2015).

- *Federal Personal Property: Opportunities Exist to Improve Identification of Unneeded Property for Disposal* (GAO-18-257, February 2018).

These reports can be accessed at https://www.sec.gov/oig (SEC OIG) and https://www.gao.gov (GAO).

Appendix II. Summary of Mobile Device and Service Costs Reviewed

Table 2 summarizes the SEC's mobile device and service costs for the period we reviewed (October 2018 through December 2019), by wireless service provider and rate plan.

TABLE 2. SEC Mobile Device and Service Costs, October 2018 through December 2019

WSP	Rate Plan Description/Features	Total Cost (October 2018 – December 2019)
WSP1	███████████████████ ██████████████████████ ████████	$940,759
	██████████████████████ ██████████████████████ ████████	$3,391,974
	██████████████████████	$222,705
	Other WSP1 plans	$118,611
WSP1 Subtotal		**$4,674,049**
WSP2	██████████████████████████ ████████████████	$29,421
	████████████████████████ ████████████████████████ ████████████████████ ██████████████	$5,985
	████████████████████████ ████████████████████████ ████████████████████████ ██████████████	$26,035
	Other WSP2 plans	$8,559
WSP2 Subtotal		**$70,000**
WSP3	████████████████████████ ████████████████████	$1,196
WSP3 Subtotal		**$1,196**
Total cost of SEC mobile devices and services[40]		**$4,745,245**

Source: OIG-generated based on wireless service providers usage reports provided by OIT.

---

[40] The total cost includes about $1 million spent to acquire mobile devices, as discussed in Finding 1.

Appendix III. Examples of ████████████████████ ██████████████████████████████

Table 3 provides examples of NIST SP 800-124 "major controls" that affect enterprise mobile device security ████████████████████████████████████ ████████████████

TABLE 3. Examples of ██████████████████████████

NIST Control Family, Control ID, and Control Name	Control Description The organization…
██████████████████ ██████████	████████████████████████████████████ ██████████████████████
████████████ ████	████████████████████████████████ ████████████████████████████████ ████████████████████
██████████████████ ██████████████████ ██████	████████████████████████████████ ████████████████████████████ ██████████████████
██████████████████ ██████████	████████████████████████████████ ██████████████
██████████████████ ██████	████████████████████████████████ ██████████████████████
██████████████████ ██████████████ ████	████████████████████ ████████████████
██████████████████ ██████████	████████████████████ ████████████
██████████████████ ██████████████ ██████	████████████████████████████ ████████████████████████ ████████████████

Source: OIG-generated based on our comparison of NIST SP 800-124 and NIST SP 800-53 to ████████ security controls provided by OIT.

Appendix IV. Monetary Impact

As Finding 1 discusses, between July and December 2019, the SEC spent nearly $160,000 on international charges incurred on agency-issued mobile devices without documented justifications to support that those costs were for valid business needs. Because OIT did not provide evidence to demonstrate that those charges related to official international travel or to international travel approved by management, we consider the costs to be unsupported, as Table 4 shows.[41]

TABLE 4. Unsupported Costs

Item	Cost
Actual cost of international charges billed to and paid by the SEC between July and December 2019	$157,605
Total Unsupported Costs	**$157,605**

Source: OIG-generated based on WSP1 invoices.

---

[41] As defined by the Inspector General Act of 1978, as amended (Public Law 95–452; 5 U.S.C. App.), unsupported costs are those costs questioned because, at the time of the audit, the costs were not supported by adequate documentation.

Appendix V. Management Comments

MEMORANDUM

To: Rebecca Sharek, Deputy Inspector General for Audits, Evaluations, and Special
            Projects, Office of Inspector General

From: Kenneth A. Johnson, Chief Operating Officer   KENNETH   Digitally signed by
                                                               JOHNSON   KENNETH JOHNSON
                                                                          Date: 2020.09.25
                                                                          18:48:23 -04'00'

Date: September 25, 2020

Subject: Management Response to Draft OIG Report, "Opportunities Exist to Improve the
            SEC's Management of Mobile Devices and Services"

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG)
recommendations related to its evaluation of the Securities and Exchange Commission's (SEC)
management of mobile devices and services. The report evaluates the SEC's spending controls
and security with respect to mobile devices, in accordance with Executive Order 13589,
Promoting Efficient Spending, Office of Management and Budget, M-16-20, *Category
Management Policy 16-3: Improving the Acquisition and Management of Common Information
Technology: Mobile Devices and Services*, and National Institute of Standards and Technology
(NIST) Special Publication (SP) 800-124, *Guidelines for Managing the Security of Mobile
Devices in the Enterprise.*

We take these issues very seriously. The Chairman and his fellow Commissioners supported the
review of the SEC's management of its mobile devices and services as part of the OIG Fiscal
Year (FY) 2020 audit work plan, released in October 2019. In addition, as soon as the Chairman
was notified of the initial findings from the OIG, he directed the staff to alert the Government
Accountability Office (GAO) and begin remediation. I supported these efforts as well. We
appreciate the recommendations for further improvement.

I appreciate OIG's extensive work analyzing mobile device management at the SEC, and concur
with the report's seven recommendations for improvement. The Chairman has instructed that
these recommendations be carried out as promptly as practicable as part of our remediation
efforts. In addition, and also at the instruction of the Chairman in consultation with the SEC's
Chief Risk Officer, I will work with our Chief Risk Officer to identify an appropriate
professional outside of the relevant offices to provide an independent view of our policies and
procedures around mobile device acquisition and management, as well as other areas that may be
appropriate.

OIG's report contains important insights on how we can better control our expenses and enhance
our security—two paramount priorities for the agency. To that end, we are committed to
implementing these recommendations swiftly, and already have initiatives underway to do so.
Consistent with OIG's recommendations and as discussed in more detail below, we anticipate

1

taking the following steps to further improve the management of the SEC's mobile devices and services:

(1) analyzing the lines of service that OIG reported as unused or potentially underused and promptly discontinuing services as appropriate;

(2) instituting policies and procedures to monitor and regularly review mobile device and service usage;

(3) improving policies and procedures related to the issuance of mobile device hardware and services to SEC personnel, including periodic reassessments of the need for mobile devices and communication of usage parameters to users;

(4) documenting our strategy and approach for future enterprise mobile device acquisitions;

(5) improving documentation of the mobile device environment to achieve compliance with current NIST security controls;

(6) updating protocols regarding device inventory, provisioning, applications, sanitization, and operating system updates; and

(7) developing and implementing policies, procedures, or guidance addressing the use ▮ ▮▮▮▮▮▮▮▮▮

Before discussing our concurrence with each of OIG's recommendations, I would like to provide some additional context regarding certain sections of the report, as well as some of the proactive steps the agency has already taken in these areas.

Mobile Device Services

We recognize the need to tighten controls so we can discontinue unused mobile device services on a timely basis. The Office of Information Technology (OIT) had identified and discontinued unused devices on an ad hoc and occasional basis multiple times in the past, including since at least March 2016 when nearly 650 devices were discontinued from service, but as the report indicates, we did not adequately adjust our policies and procedures. OIG's review demonstrates that OIT was not as rigorous as it should have been in carrying out policies and managing our mobile device expenses. Clearly, improvements in this process and, in particular, the time to discontinue devices, are needed.

During the course of the audit, OIT began implementing an improved monthly review of mobile carrier invoices, to regularly identify and discontinue unused or underutilized device services. The SEC has discontinued service to a tranche of approximately 600 lines in September 2020, and will continue to review the lines identified by the OIG and take action as necessary. OIT

2

will also continue to refine the new review process and document it in accordance with OIG's recommendations.

International Travel Services

Historically, OIT has endeavored to accommodate SEC staff requests for international service so that they could continue to stay connected on work matters while overseas. While we believe that most or all of these requests were for staff to support mission objectives while on travel, we recognize that our policies can benefit from better formalization. The SEC has worked to develop a new international travel policy for IT devices, which among other objectives would improve the process by which users request international service. On September 17, 2020, the new policy, titled SECR 24-12, *Requirements for Securing SEC Information Technology Resources in Connection With International Travel,* was published and announced to all SEC staff. The SECR defines the types of devices that can be taken when traveling for either official business or personal travel, the types of connections permitted, and best practices for safeguarding devices while traveling. In conjunction with this release, OIT updated the form for initiating international service on an SEC-issued device to require a justification and supervisor approval, so the requests can be tracked and analyzed. The SEC will ensure this new policy is consistently implemented and device and service usage granted in accordance with this policy.

Mobile Device Replacement

With respect to the recent replacement of mobile devices discussed in the report, I would like to provide some additional context. The agency's intent was to replace out-of-service devices with a model that both (1) met agency requirements and (2) was not expected to be imminently discontinued, in order to avoid potentially having to spend additional funds on another replacement program in the near future.

For example, one of the SEC's requirements was a minimum internal storage capacity of at least ████████ In addition, SEC expected, based on previous device retirement cycles from the vendor, that ████████████ would be discontinued in the near term. As described in Table 1, SEC then selected the lowest cost device that met these considerations. This selection was the fifth lowest cost model out of seventeen available models on the vendor selection list, and it was the least expensive model that has not since been discontinued.

Further, the report states the agency spent nearly $1 million in FY 2019 to replace mobile devices. However, I would note the SEC received vendor credits totaling over $240,000, which made the total FY 2019 investment approximately $760,000.

Table 1, *Contractually Available* ███ *Device Models and Costs, At Time of Selection,* illustrates the options for device purchases.

3

Table 1. Contractually Available ▮ Device Models and Costs, At Time of Selection

▮	Storage	Upgrade / New Line Price	Full Retail	Notes
		$0.99	$449.99	Discontinued in ▮
		$99.99	$549.99	Discontinued in ▮
		$119.99	$569.99	Discontinued in ▮
		$149.99	$599.99	Discontinued in ▮
		$201.71[1]	**$749.99**	**SELECTED**
		$219.99	$669.99	Discontinued in ▮
		$249.99	$699.99	Discontinued in ▮
		$299.99	$749.99	Discontinued in ▮
		$349.99	$799.99	Not Selected due to Cost
		$399.99	$849.99	Discontinued in ▮
		$449.99	$899.99	Not Selected due to Cost
		$449.99	$899.99	Not Selected due to Cost
		$549.99	$999.99	Not Selected due to Cost
		$599.99	$1,049.99	Not Selected due to Cost
		$649.99	$1,099.99	Not Selected due to Cost
		$699.99	$1,149.99	Not Selected due to Cost
		$799.99	$1,249.99	Not Selected due to Cost

However, OIG rightfully pointed out the agency did not adequately document the requirements and strategy for this procurement. While in looking back we believe that the correct procurement decisions were made, our documentation was not what it should have been. Accordingly, we intend to develop policies and procedures to document our strategy and approach for future purchases.

Mobile Device Security and Configuration

The SEC is taking additional action in the area of mobile device security to safeguard information accessed, stored, and processed on mobile devices. For example, OIT has taken steps to improve mobile device security controls, including by undertaking an evaluation of the security of mobile devices enrolled in ▮ OIT also acted to ▮

---

[1] The price of $201.71 reflects the final cost of the device after the credits for returned devices were applied.

4

[REDACTED] and incorporated mobile device security into the SEC's annual privacy and information security awareness training program. In addition, SEC staff have been engaged with the vendors for both the mobile device management (MDM) software[2] and the devices to address configuration limitations in areas such as [REDACTED] Finally, I would note the SEC prohibited specific applications from mobile devices before government-wide instructions to do so. Going forward, we will work to develop comprehensive policies and procedures for application vetting and associated controls on our devices.

Thank you once again for the professionalism and courtesies you and all of the OIG personnel demonstrated throughout this audit. Appendix A presents our formal responses to each recommendation. We intend to pursue these remaining corrective actions as a top priority, and look forward to working with your office to confirm our actions fully address the issues identified in your report.

cc: David Bottom, Chief Information Officer, Office of Information Technology

       Vance Cathell, Director, Office of Acquisitions

Appendix A: Management's Responses to OIG's Recommendations

The following are management's responses to each of the recommendations provided in the OIG report.

Recommendation 1: Assess the continued business need for the devices we identified as unused and potentially underused; and, as appropriate, take action to suspend services to those devices.

Response: We concur. As discussed above, we are continuing to work closely with the vendors to analyze the lines of service that OIG reported as unused or potentially underused. Based on this assessment with the vendors, OIT will discontinue services to any mobile devices deemed to no longer have a business need. OIT also will apply the policies and procedures developed pursuant to Recommendation 3 to perform ongoing reviews of the continued business need for devices.

Recommendation 2: Establish and implement comprehensive processes and procedures and/or update existing guidance to:

   a) Require periodic reviews and reconciliations of mobile device usage reports, rate plan analysis reports, and ▮▮▮▮▮ reports to identify and address key indicators of potential inefficient or unauthorized use including overuse, underuse, or zero use.

   b) Require periodic reviews of wireless service providers' invoices to ensure unusual or additional charges, such as international charges, are accurate, are for authorized purposes, and are adequately supported.

Response: We concur. OIT will establish and implement processes and procedures for performing the periodic reviews described in this recommendation.

Recommendation 3: Update existing guidance to include periodic assessments and recertifications of the continued need for mobile devices, specify criteria for assigning rate plans to mobile device users, and establish a process for communicating the plans' limits to users.

Response: We concur. OIT will update guidance to include periodic assessments and recertifications of the continued need for mobile devices. Pursuant to Recommendation 2, OIT will define the criteria for assigning rate plans to users, and will prepare a communications approach to inform mobile users of the appropriate business uses and limits of the acceptable limited personal use policy.

Recommendation 4: Define an agency-wide mobile device program-level acquisition strategy, including conditions and criteria for approving the procurement of mobile devices that meet defined SEC requirements.

6

Response: We concur. OIT will formalize and document its acquisition strategy for mobile devices prior to the next program-level acquisition. The strategy will be linked to the SEC's capital planning and investment control (CPIC) guidance for steady state acquisitions. The acquisition strategy will define the proposed timeframes, list the documents that will be required once the acquisition is underway (e.g., requirements documents, cost-benefit analysis), and identify which steps of the CPIC process are required for this type of investment.

Recommendation 5: Update applicable system security plans to include security controls applicable to mobile devices identified in Federal guidance, and update documentation of the ██

Response: We concur. The SEC will review and, if necessary, update the system security plan for the ████████ mobile device environment to be compliant with the most current controls specified by NIST, and create or update other documentation necessary ████████ ████████████████████

Recommendation 6: Update existing policies and procedures to include additional controls addressing mobile device inventory, provisioning, applications, sanitization, and operating system updates. Specifically, OIT should update existing policies and procedures to:

a) Require a periodic reconciliation between ████████████████ and clearly define which mobile devices should be enrolled in ████████

b) Clearly define the roles, responsibilities, and processes for provisioning devices based on business need.

c) Include processes for ██ ██

d) Include processes to periodically monitor mobile devices for ████████████

e) Define the roles, responsibilities, and processes (including the timeline) for ████████ ████████████████████████████████████

f) Include ████████████████████████████████████

Response: We concur. OIT will review, and as necessary, update existing policies and procedures to include additional controls addressing mobile device inventory, provisioning, applications, sanitization, and operating system updates. OIT has recently issued a new mobile device policy focusing on Recommendation 6(b), and will work to address the other listed items in this recommendation. Regarding Recommendation 6(f), ████████████████████ ██ OIT will continue to work

7

with both the device and MDM vendors to ███████████████████████████████
██
██

Recommendation 7: In coordination with the Office of the General Counsel, assess the risk of allowing ██ If the agency's determination is to continue ██
██

Response: We concur. ██
██
██
███████████████████████ OIT will analyze the risk of
██ and per the OIG's recommendation, if this risk is deemed appropriate SEC staff will develop policies and processes addressing the ██████████████████

8

Major Contributors to the Report

Kelli Brown-Barnes, Audit Manager
Sara Tete Nkongo, Lead Auditor
Michael Burger, Auditor
Douglas Carney, Auditor
Sharice Cole, Auditor
David B. Witherspoon, Senior Attorney

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, evaluations, or reviews, please send an e-mail to OIG Audit Planning at AUDplanning@sec.gov. Comments and requests can also be mailed to the attention of the Deputy Inspector General for Audits, Evaluations, and Special Projects at the address listed above.

TO REPORT

fraud, waste, and abuse

Involving SEC programs, operations, employees, or contractors

FILE A COMPLAINT ONLINE AT

www.sec.gov/oig

CALL THE 24/7 TOLL-FREE OIG HOTLINE

833-SEC-OIG1

CONTACT US BY MAIL AT
U.S. Securities and Exchange Commission
Office of Inspector General
100 F Street, N.E.
Washington, DC 20549