



OFFICE OF INSPECTOR GENERAL

JULY 28, 2022

Evaluation of the Information Technology Division's Inventory Accountability and Controls

Evaluation Report 2022-0002-IE-P

MISSION

The OIG promotes efficiency and effectiveness to deter and prevent fraud, waste and mismanagement in AOC operations and programs. Through value added, transparent and independent audits, evaluations and investigations, we strive to positively affect the AOC and benefit the taxpayer while keeping the AOC and Congress fully informed.

VISION

The OIG is a high-performing team, promoting positive change and striving for continuous improvement in AOC management and operations. We foster an environment that inspires AOC workforce trust and confidence in our work.



Results in Brief

Evaluation of the Information Technology Division's Inventory Accountability and Controls

July 28, 2022

Objective

Our objective for this evaluation was to determine if adequate mechanisms and controls are in place to account for agency issued electronic devices (laptops, iPads, cell phones etc.), the extent to which vulnerabilities exist due to lost, stolen or misplaced electronic devices and if adequate procedures are in place to report, track and replace missing property. This evaluation was consistent with our 2021 agency Management Challenges which listed Waste and Accountability as a Management Opportunity and Performance Challenge.

Findings

Based on our evaluation, we found the following:

- The Architect of the Capitol's (AOC) policy for accountable Information Technology (IT) property is outdated, not comprehensive and does not outline the IT property management lifecycle. Additionally, the current policy referenced use of other "related procedures", however, those procedures are not included within the current policy, and are only generally communicated to the AOC organization Accountable Property Officer (APO)s from the IT Program Manager (ITPM) on an ad-hoc basis.
- The Information Technology Division (ITD) uses two separate asset management systems that offer similar inventory management system capabilities to account for agency-issued IT property. In addition, we found instances of each system tracking both types of property, which presents a concern of duplication of effort and

cost waste. The Office of Inspector General (OIG) identified that discontinuing the use of both the inventory management systems and transitioning to Maximo could amount to \$15,385.39 as AOC funds that could be put to better use.

- While the AOC has a Board of Survey process in place to address Lost, Stolen and Damaged IT devices, the process is generally not enforced, not utilized consistently, and lacks a deterrent feature to prevent future occurrences of Lost, Damaged and Stolen IT devices. Furthermore, in cases where a Board of Survey was conducted, paperwork was either not thoroughly completed or signed off on.
- ITD does not frequently perform inventory inspections for IT mobile devices—cellphones, laptops and iPads. Rather, ITD uses its annual telecom memorandum as a self-reported audit feature to track these types of mobile devices, which poses not only an information security vulnerability to the AOC, but also a physical security vulnerability to the agency.

Recommendations

We recommend that:

1. The Chief Information Officer update ITD's current policy for accountable IT property, to include the incorporation of defined program personnel roles, requirements aligned with the property management lifecycle and all current program procedures.
2. The Chief Information Officer continue pursuit of transitioning to a single asset management



Results in Brief

Evaluation of the Information Technology Division's Inventory Accountability and Controls

system that addresses its program needs to track accountable and consumable IT property and establish a detailed implementation plan with target dates to transition to a single asset management system for accountable and consumable IT property as currently captured in Cireson and Jumpstock.

3. The AOC revise the Board of Survey Process with codified punitive actions to act as a deterrent against future instances of employee negligence and misconduct regarding the loss of AOC property, including both IT mobile devices and personal property.
4. The Chief Information Officer, establish internal controls in addition to the current Annual Telecom Memorandum requirement, to identify indications of a mobile device being lost, damaged or stolen and have processes in place to act accordingly.

Management Comments

The AOC provided comments on July 19, 2022, see Appendix B. In its Management Comments, the AOC concurred with three recommendations, and non-concurred with the fourth recommendation. Please see the recommendations table on the next page for the status of each recommendation.



Results in Brief

Evaluation of the Information Technology Division's Inventory Accountability and Controls

Recommendations Table

Responsible Entity	Recommendation Resolved	Recommendation Unresolved	Recommendations Closed
CIO	R1, R2, R3	R4	

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** - Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** - Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – The OIG verified that the agreed upon corrective actions were implemented.



INSPECTOR GENERAL

DATE: July 28, 2022

TO: J. Brett Blanton
Architect of the Capitol

FROM: Christopher P. Failla, CIG
Inspector General 

SUBJECT: Evaluation of the Information Technology Division's (ITD's)
Inventory Accountability and Controls (Project No. 2022-0002-IE-P)

Please see the attached final report for our evaluation of the ITD's Inventory Accountability and Controls, which was announced on November 08, 2021. We found that the ITD's policy for accountable Information Technology (IT) property was outdated, inventory management systems were redundant, enforcement efforts for lost, damaged or stolen mobile devices were underused and lack a deterrent feature, and that ITD lacks frequent inspections of IT mobile devices.

In your response to our official draft report (Appendix B), you concurred with three recommendations and non-concurred with one recommendation. Based on your response to Recommendations 1, 2 and 3, we feel the proposed corrective actions address our recommendations. However, your non-concurrence with Recommendation 4 does not adequately address our concern over ITD's sole reliance on its Annual Telecom Memorandum as an inventory management tool to account for mobile devices and its lack of other internal controls to inventory mobile devices in order mitigate future security incidents as discussed in our report. The status of the recommendations will remain open until final corrective action is taken. We will contact you within 90 days to follow-up on the progress of your proposed management decision.

I appreciate the assistance you and your staff provided throughout the evaluation. Please direct questions to Senior Evaluator Josh Rowell at 202.579.7458, or Joshua.Rowell@aoc.gov or Assistant Inspector General for Inspections and Evaluations Chico Bennett at 202.394.2391, or Chico.Bennett@aoc.gov.

Distribution List:

William O'Donnell, Chief Administrative Officer
Jon Migas, Chief Information Officer
Peter Bahm, Chief of Staff
Jason Baltimore, General Counsel
Mary Jean Pajak, Deputy Chief of Staff

Contents

INTRODUCTION	4
OBJECTIVE	4
BACKGROUND.....	4
REVIEW OF INTERNAL CONTROLS	6
CRITERIA	6
FINDING 1.....	7
ACCOUNTABLE IT PROPERTY POLICY IS OUTDATED AND NOT COMPREHENSIVE	7
CONCLUSION.....	9
RECOMMENDATION	9
FINDING 2.....	10
DUAL-ASSET MANAGEMENT SYSTEMS WITH SIMILAR SYSTEM CAPABILITIES USED TO TRACK IT PROPERTY	10
CONCLUSION.....	12
RECOMMENDATION	12
FINDING 3.....	13
BOARD OF SURVEY PROCESS UNDERUSED FOR LOST, DAMAGED OR STOLEN IT MOBILE DEVICES AND LACKS A DETERRENT FEATURE.....	13
CONCLUSION.....	16
RECOMMENDATION	16
FINDING 4.....	17
ITD LACKS FREQUENT INSPECTIONS OF IT MOBILE DEVICE PROPERTY	17
CONCLUSION.....	19
RECOMMENDATION	20
DATA SNAPSHOT	22
ITD’S TOTAL MOBILE DEVICE INVENTORY AND LOST DAMAGED AND STOLEN MOBILE DEVICES FOR YEARS 2019 THROUGH 2021	22
APPENDIX A.....	26
SCOPE AND METHODOLOGY	26
USE OF COMPUTER-PROCESSED DATA.....	26
PRIOR COVERAGE	26
APPENDIX B.....	27
MANAGEMENT COMMENTS	27
NOTIFICATION LETTER.....	30
ACRONYMS AND ABBREVIATIONS.....	31

Introduction

Objective

The objective of this evaluation was to determine if adequate mechanisms and controls were in place to account for agency issued electronic devices (laptops, iPads, cell phones etc.), the extent to which vulnerabilities exist due to lost, stolen or misplaced electronic devices and if adequate procedures are in place to report, track and replace missing property.

Background

This evaluation was initiated based on an AOC OIG Investigation Division referral submitted to the Inspections and Evaluations Division in August 2021. The investigation raised concerns over the AOC ITD having inadequate inventory accountability procedures in place for issuance and tracking of mobile devices, and other AOC ITD equipment. Prior to the 2021 referral and since 2018, the OIG's Investigations Division conducted ten investigations dealing with ITD accountable property matters.¹

The Federal Property and Administrative Services Act of 1949, 40 USC § 101, et seq. requires Executive Branch federal agencies to manage personal property and maintain accountability for acquired property valued at more than an established monetary or sensitivity threshold as determined by the respective federal agency. The AOC is not subject to the Federal Property and Administrative Services Act of 1949. However, the AOC has acknowledged through its personal property management policy that the agency is not precluded from adopting the law's principles and intended purpose.

AOC ITD

The Accountable IT Property Management Program is administered and overseen by the AOC'S ITD Chief Information Officer (CIO), who delegates authority to the IT Property Manager (ITPM) who is ultimately responsible for the management and oversight of the program. AOC Order 8-4, Accountable Information Technology (IT) Property, April 24, 2015, is the principal AOC policy that describes the process and requirements for the use of accountable IT property by all AOC staff (employees, contractors, and others) and includes an overview of oversight responsibilities for those charged with overseeing the program. The policy defines Accountable IT Property as IT property that has an acquisition value of \$500 or greater, but less than \$25,000. IT equipment valued at \$25,000 or more is considered a capital asset.

¹ Six of the OIG's investigations dealt with AOC De Minimis Use policy violations and the other four investigations concerned inventory management issues where mobile devices either went lost, damaged or stolen. As a result of one of those investigations, the OIG issued a Management Advisory to the AOC in May 2020, detailing concern over Capitol Visitor Center (CVC) IT property not being stored in the AOC's inventory management system for AOC personal property—Maximo.

Mobile telecommunication devices are also considered accountable IT property regardless of value.

Each AOC organizational leader, through the ITPM, has designated and appointed in writing an IT Accountable Property Officer (APO), and those individuals are charged with local oversight duties for their respective organizations as they align with ITD's accountable property IT program and requirements, with specific regard to the acquisition, receipt, accountability, utilization and disposition of accountable IT property. In addition to APO's, each organizational leader also designates and appoints IT Property Custodians (PC) who report to APOs for their respective organization, and those individuals are responsible for day-to-day property management functions within their custodial workshop areas. The APO and PC duties are collateral assignments to employees' primary job duties and requirements.

AOC Capitol Visitor Center

The Capitol Visitor Center Act of 2008 established the position of the Chief Executive Officer for Visitor Services, that operates independently, but in consultation with the Architect of the Capitol. As such, the law provided a separate budget authority from the AOC to support CVC services and operations. While annual budget requests for the CVC are submitted by the Architect of the Capitol annually, they are done so at the recommendation of the Chief Executive Officer, granting the Architect limited purview over CVC operations and matters.

As such, there are certain CVC functions that are independent of the AOC. Due to the objective and scope of this evaluation, it is worthwhile to highlight that the CVC maintains its own IT Specialist, acting in a CIO capacity to manage and oversee unique IT services and systems required at the CVC.² Specifically, the CVC IT Specialist is responsible for the operation and management of three different systems to support the CVC's mission, and which are unique to the AOC in general: 1) The Point of Sales system used for ticketing, food and gift shop sales, 2) the CVC tour scheduler, and 3) the Wi-Fi network. Neither of these systems interfaces with AOC's General Support System (GSS) network, which is overseen and managed by ITD. Given the uniqueness of these systems and the fact that they are only required at the CVC, the CVC IT Specialist has the authority to purchase certain IT mobile devices that the AOC would not (e.g., iPad Pros for scheduling or graphics design purposes) to support the CVC's mission. In such cases, the CVC is responsible for purchasing, supporting and inventorying those mobile devices. Because these devices only interface with CVC networks, there is no cause for security concern that those devices would be able to access the AOC's GSS network. However, because some

² There is no requirement for this person to coordinate CVC activities, or direct report back to the AOC's CIO. Rather the CVC Executive Officer is subject to oversight by the Senate Committee on Rules and Administration and the Committee on House Administration of the House of U.S. Representatives.

CVC employees also require access to the AOC GSS network to carry out work activities at the CVC in support of the AOC's mission, the AOC's ITD will purchase, support, and maintain inventory of cellphones, laptops and iPads, as necessary for those employees.

Review of Internal Controls

We evaluated the AOC's internal controls for its property management program for IT Mobile devices, specifically cellphones, laptops and iPads. Although the AOC had a principal policy for management of accountable IT property, the policy is outdated, not comprehensive and does not outline the IT property management lifecycle. As a result, the potential for process gaps and security vulnerabilities exists in cases where mobile devices are lost, stolen or misplaced.

Criteria

The following criteria were used during this evaluation:

- AOC Order 8-4, Accountable Information Technology Property, April 24, 2015
- AOC Order 34-45, Personal Property Manual, October 15, 2020
- AOC Order 7-4 Information Technology Security, October 10, 2017
- AOC Order 8-5 AOC IT Resources and De Minimis Use, February 20, 2018

Finding 1

Accountable IT Property Policy is Outdated and Not Comprehensive

We found that AOC Order 8-4 served as ITD’s principal policy for accountable IT property; however, the policy is outdated, not comprehensive and does not outline the IT property management lifecycle. Furthermore, the current policy referenced use of other “related procedures;” however, those procedures are not included within the current policy and the ITPM only generally communicates them to AOC organization APOs on an ad-hoc basis.

This occurred because:

- AOC Order 8-4 has not been updated since its initial development in 2015;
- The policy was hurriedly developed after ITD officials realized unique differences in managing IT accountable property, which previously fell under the policy requirements governed by AOC Order 34-45, Personal Property Manual. And, although the draft policy underwent the AOC policy correspondence management record oversight process, a contractor charged with ITD support services developed the policy, as opposed to the ITPM, who would have had greater purview and expertise in defining and developing program requirements; and
- While the policy defined user-roles, it did not outline the property management life cycle for organizational use, nor did it include program procedures for those personnel charged with carrying out program requirements. Rather these procedures were generally communicated by the ITPM on an ad-hoc basis.

As a result, the lack of an updated and comprehensive policy increased the risk and probability of process gaps in the inventory management program for IT equipment across the AOC. Furthermore, because procedures are generally directed on an ad-hoc basis and managed by the ITPM, and not a part of the policy, the program is vulnerable to inconsistent management practices at the local organizational level across the AOC.

Discussion

AOC Order 8-4, Accountable IT Property, dated April 24, 2015, is the principal AOC policy that describes the process and requirements for the use of accountable IT property by all AOC staff (employees, contractors and others) and includes an overview of oversight responsibilities for those charged with overseeing the program.³ However, while AOC Order 8-4 serves as ITD’s principal policy for accountable IT property, we found that the policy is outdated, not comprehensive and does not outline the IT property management lifecycle.

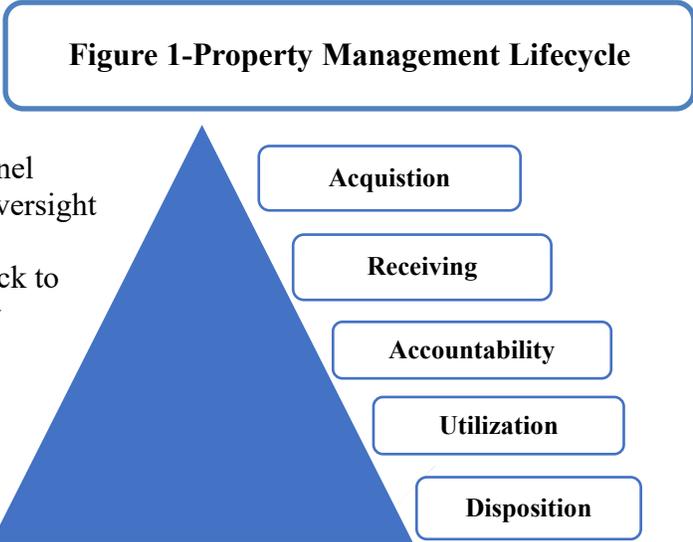
Through interviews with program staff and officials, we learned that the outdated and uncomprehensive policy was likely a result of previous AOC CIO leadership, which was directed by the Office of the Architect at the time. IT officials told the OIG that prior to the current AOC CIO, from approximately 2013 to 2020, the attitude projected onto the ITD staff while managing and distributing IT mobile devices was that “government IT equipment was to be used at the convenience of AOC staff in order for them to complete their job activities,” without credence to proactively managing the potential misuse of IT mobile devices.

IT officials noted that the previous CIO directed ITD personnel to develop its own policy for the accountability and disbursement of IT accountable property approximately during the latter part of 2014. The initiative began because of unique differences in managing IT accountable property (e.g., cellphones, laptops and iPads), which previously fell under the program and policy requirements governed by AOC Order 34-45 for AOC personal accountable property (e.g., tools, utility vehicles and building material). ITD program officials stated that the initial policy, AOC Order 8-4, was hurriedly put together. Although the draft policy underwent the AOC policy correspondence management record oversight process, an AOC contractor charged with support services over ITD equipment developed the policy, as opposed to the AOC ITPM, who would have had greater purview and expertise in defining and developing program requirements.

Furthermore, in our review of AOC Order 8-4, we found that the policy defined program user-roles. The policy was not comprehensive in explaining process requirements and did not follow the general property management lifecycle

³ The policy defines accountable IT property as IT property that has an acquisition value of \$500 or greater, but less than \$25,000. IT equipment valued at \$25,000 or more is considered a capital asset. Mobile telecommunication devices are also considered accountable IT property regardless of value.

principles—Acquisition, Receiving, Accountability, Utilization and Disposition. The policy also did not include program procedures for those personnel charged with carrying out program oversight requirements. Rather, those specific procedures were either referenced back to AOC Order 34-45, Personal Property Manual, or stored separate from the policy on the AOC’s SharePoint intranet and the ITPM only generally communicated to APO’s and other program staff on an ad-hoc basis. ITD officials acknowledged that the current policy was not comprehensive in defining process requirements and noted that the result was likely due to rapid policy development without consideration given to it being a standalone program policy. Instead, it was more likely drafted as a supplement to AOC Order 34-45, Personal Property Manual.



It is noteworthy to point out that during fieldwork for this evaluation, the current AOC CIO and ITPM have acknowledged the inherent weaknesses with the current policy for accountable IT property. The CIO and ITPM have identified the need to update the policy in the near future to ensure the policy is comprehensive.

Impact

Because the policy is outdated and not comprehensive, the AOC is exposed to the potential increased risk and probability of process gaps in the inventory management program for IT mobile devices and equipment. And, because procedures are generally directed on an ad-hoc basis and managed by the ITPM, and not a part of the policy, the program is vulnerable to inconsistent management practices at the local organizational levels across the AOC.

Conclusion

A more robust and inclusive policy would bolster the program’s intended effects, providing for better accountability and management of IT property, while also mitigating IT security risk due to misuse of devices, including when IT mobile devices go lost, damaged or stolen.

Recommendation

Recommendation 1

We recommend that the Chief Information Officer update Information Technology Division’s current policy for accountable Information Technology property, to

include the incorporation of defined program personnel roles, requirements aligned with the property management lifecycle, and all current program procedures.

AOC Comment

The AOC concurs. The Information Technology Division will update AOC Order 8-4, Accountable Information Technology Property to incorporate defined program personnel roles and align requirements with the property management life cycle and all current program procedures.

The estimated completion date for Recommendation 1 is June 30, 2023.

OIG Response

We reviewed the management comment and determined it addresses the finding and recommendation.

Finding 2

Dual-Asset Management Systems with Similar System Capabilities Used to Track IT Property

We found that ITD uses two separate asset management systems to account for agency-issued IT property, which offer similar inventory management system capabilities. In addition, we found instances of each system tracking both types of property, which presents a concern of duplication of effort and cost waste.

This occurred because prior to the acquisition of the inventory asset management system Maximo, which is used to track AOC personal property, the ITD used and continues to use Cireson and Jumpstock to account for IT property. Cireson is currently used to track inventory of IT accountable property and Jumpstock is used to track inventory of IT consumable property. The use of these systems is a result of historical redundance in program practice.

As a result, the two asset management systems both tracking accountable and consumable IT property, increases the potential for inaccurate inventory management records to exist by way of reporting duplication. Furthermore, neither system presents unique features based on program need that a single system of record could provide, thus presenting the appearance of wasted cost by the AOC.

Discussion

During our review, we found that the AOC uses two separate asset management systems to account for its IT inventory and agency-issued mobile devices—Cireson and Jumpstock. Cireson is used to account for IT property and mobile devices, including cellphones, laptops, and iPads and Jumpstock accounts for IT consumable property—items less than \$500. Neither system offers unique features from one another when it comes to the inventory management of IT property, which presents the OIG’s concern of duplication of inventory management efforts and cost waste.

Prior to the acquisition of the inventory asset management system Maximo, which is used to track AOC personal property, the ITD used and continues to use Cireson and Jumpstock to account for IT property. Cireson is currently used to track inventory of IT accountable property and Jumpstock is used to track inventory of IT consumable property. The use of these systems is a result of historical redundancy in program practice. According to ITD officials, the Cireson platform solely tracks inventory of accountable IT property equipment—items between \$500 and \$25,000. They also noted that they are evaluating other information technology service management platforms to better meet their needs but have yet to bring a new system online. Cireson has an annual attributed cost of \$14,282.89. Jumpstock has an annual attributed cost of \$1,102.50. While the OIG did not perform a cost-benefit or mission-critical analysis between the two systems, there is a potential actualized annual cost-savings of \$13,180.39 if the AOC was able to use Jumpstock in place of Cireson. During our interviews with IT officials and IT personnel, we found that there were no unique positive or negative functions presented between the two current systems. It is also worth noting, although for a much lower volume of IT items, ITD also uses a third asset management system, Maximo,⁴ to account for capital assets valued at more than \$25,000. If both Cireson and Jumpstock could be eliminated by virtue of mission need being achieved through the service of the Maximo asset management system, ITD could recoup an annual amount of \$15,385.39 currently spent on its present asset management platforms. As such, the OIG considers the amount of \$15,385.39 as AOC funds that could be put to better use.

Also, while reviewing inventory management records for IT mobile devices from 2019 through 2021, and although both systems appeared to track complete inventory information on their own, we noted several instances of duplicative records being tracked in the data provided. We also found instances where non-mobile devices, like desktop computers and conference telephones, were included in the mobile device count. Having a single system of record that meets the ITD’s program needs and consolidates all IT property into one system would increase the likelihood for accurate inventory record tracking and reporting, and likely also increase work

⁴ The Cireson and Jumpstock systems were already in use by the AOC for IT property prior to the AOC’s acquisition of the Maximo asset management system, which is currently used primarily to track AOC personal property inventory.

activity efficiencies while gathering data and creating inventory reports.

It is noteworthy to point out that during fieldwork for this evaluation, the current AOC CIO and ITPM acknowledged the potential benefit and efficiencies that could be gained through use of a single system and are currently exploring use of an IT service management platform that not only meets the ITD's servicing needs of equipment and software, but also strengthens its IT asset management capabilities over mobile device inventory.

Impact

The ITD's current use of two asset management systems to track IT property, increases the potential for inaccurate inventory management records due to duplication. Neither system presents unique features based on program need that a single system of record could not provide, thus presenting the appearance of wasted cost by the AOC. Leveraging a more robust IT service management platform that appropriately addresses both ITD's servicing and asset management needs could provide a significant improvement in oversight efforts over the inventory lifecycle and accountability of mobile devices and other IT equipment, while also better aligning the program with IT Infrastructure Library best practices.

Conclusion

Consolidating the two asset management systems for accountable and consumable IT property by moving to a single system would better streamline inventory management practices and reduce the potential of duplicative records between two systems while also lessening redundancies in tracking and reporting out inventory numbers. There is also a representative cost savings that the AOC could recoup if ITD determined that the use of Maximo could meet their inventory management needs to account for all IT property.

Recommendation

Recommendation 2

We recommend that the Chief Information Officer continue pursuit of transitioning to a single asset management system that addresses its program needs to track accountable and consumable Information Technology (IT) property and establish a detailed implementation plan with target dates to transition to a single asset management system for accountable and consumable IT property as currently captured in Cireson and Jumpstock.

AOC Comment

The AOC concurs. Leveraging a robust IT service management (ITSM) platform with incorporated IT asset management, when properly implemented, provides significant

accountability and life cycle of IT assets in alignment with industry and Information Technology Infrastructure Library best practices. ITD is currently assessing more robust ITSM tools for future implementation.

The estimated completion date for Recommendation 2 is September 30, 2024. This is an unfunded requirement requiring adherence to the AOC budget and procurement processes.

OIG Response

We reviewed the management comment and determined it addresses the finding and recommendation.

Finding 3

Board of Survey Process Underused for Lost, Damaged or Stolen IT Mobile Devices and Lacks a Deterrent Feature

We found that while the AOC has a Board of Survey process⁵ in place to address Lost, Stolen and Damaged IT devices, the process is generally not enforced, not utilized consistently, and lacks a deterrent feature to prevent future occurrences of Lost, Damaged and Stolen IT devices. And in cases where a Board of Survey was conducted, paperwork was either not thoroughly completed or signed off on.

This occurred because:

- The previous CIO leadership, from approximately 2013-2020, lacked consistent enforcement of the Board of Survey Process;
- In previous cases where IT mobile devices were lost, damaged or stolen, a no-questions-asked-attitude was adopted by those AOC personnel charged with overseeing agency issued mobile devices and the Board of Survey Process was not initiated due to non-endorsement by the previous CIO; and
- The current overall agency attitude towards the Board of Survey Process is that “it has no teeth” to hold employees accountable for lost, stolen or damaged IT mobile devices because the current Board of Survey process is not uniform or automatically initiated in cases of lost, damaged or stolen IT mobile devices. Rather, the process is only initiated on a case-

⁵ The Board of Survey process is a critical tool used for effective property management and is intended to be an investigative tool to provide a value-assessment of AOC property that is lost, damaged or stolen; and also serves as a mechanism for property management officials to authorize retirement and disposition of property that is lost, damaged or stolen.

by-case basis, and much of that initiation is based on agency leadership's desire to pursue the process.

As a result, ITD created a separate Lost, Damaged and Stolen (LDS) procedure which bypasses the Board of Survey Process to better deter future occurrences of lost, damaged, or stolen mobile devices. However, without a standardized process that is consistently enforced at all organizational levels, the AOC is vulnerable to employee waste, misconduct and other levels of criminality.

Discussion

For AOC personal property, the AOC uses a Board of Survey process, outlined in AOC Order 34-45, Personal Property Manual, which uses a standing committee of three to five senior AOC members, appointed by the Chief Operating Officer, who serve a rotating term and are responsible for investigating incidents of lost, damaged or destroyed AOC property. The purpose of the Board of Survey process is to provide a thorough examination of the circumstances surrounding reported lost, damaged or stolen AOC property. Specifically, the process provides a value assessment of the reported lost, damaged or stolen property, whether or not the employee is culpable for repayment or compensation to the agency for lost, damaged or stolen property, and authorizes property management officials the ability to retire and dispose of the property tracked in its management systems. During our review, we found that while the AOC has a Board of Survey process in place to address lost, damaged and stolen IT devices, the process is generally not enforced, not utilized consistently, and lacks a deterrent feature to prevent future occurrences of lost, damaged and stolen IT devices. And in cases where a Board of Survey was conducted, paperwork was either not thoroughly completed or signed off on. While the specific rules and requirements outlining the Board of Survey process is not as detailed in AOC Order 8-4, ITD's policy for accountable IT property does refer to the process as outlined in AOC Order 34-45. It also requires inventory management officials to follow the same process when evaluating incidents of lost, damaged, or destroyed accountable IT property and to promptly initiate the Board of Survey process, when warranted.

Board of Survey Records Between 2019 and 2021

During our review, the OIG requested all Board of Survey records with a mobile device nexus that were conducted between 2019 and 2021. ITD returned only one Board of Survey case with accompanying supporting documentation for an employee who reported losing their cellphone on three separate occasions within a one-year period. During that same period, 144 IT mobile devices were either lost, damaged or stolen. The fact that one record exists represents a disproportionate use of the Board of Survey process.

For the single Board of Survey record provided to the OIG during this evaluation, the record contained an AOC Report of Survey form, a signed U.S. Capitol Police Event Report and email records between AOC staff documenting the third incident of loss. However, the record documentation did not contain AOC Reports of Survey, police reports or emails documenting the previous cellphone losses for that employee earlier in the year. Furthermore, for the completed AOC Report of Survey, several data fields were left incomplete, the recommended Board of Survey action was not detailed, and signatures of the employee and board authorities were not present.

In speaking with ITD officials, we found that the Board of Survey Process requirement was not generally enforced and was underutilized in cases of lost, damaged or destroyed IT accountable property due to a few reasons:

- From approximately 2013-2020, ITD lacked consistent enforcement of the Board of Survey Process because previous CIO leadership projected a no-questions-asked-attitude onto ITD program oversight staff in cases where mobile devices were lost, damaged or stolen and did not endorse the process.
- The current overall agency attitude towards the Board of Survey Process is that “it has no teeth” to hold employees accountable for lost, stolen or damaged IT mobile devices because the current Board of Survey process is not uniform and is not automatically initiated in cases of lost, damaged or stolen IT mobile devices. Rather, the process is only initiated on a case-by-case basis, and that determination is based on agency leadership’s desire to pursue the process.
- The Board of Survey Process is not timely, and several weeks may pass from the time that the incident is reported until the board is formed and reaches a resolution.

As such, ITD created its own procedure⁶, which bypasses the Board of Survey Process to strengthen employee accountability and better deter future occurrences of lost, damaged, or stolen mobile devices. The procedure still offers the ITPM latitude to initiate a Board of Survey, but at a minimum requires that an incident report be filled out documenting the nature of and circumstances surrounding the missing item to give just cause or denial regarding replacement of mobile devices. The incident report feature mimics an in-house investigation into the missing device. For devices that are reported as stolen, the ITPM requires that a police report be submitted in addition to the incident report.

As an accountability tool and to complement ITD’s LDS procedure, the ITPM has created an “elevation of incident” notification threshold to address instances of

⁶ QW011-Lost, Damaged, Stolen Process, effective February 10, 2021.

recurring requests by AOC employees, whom within a two-year period, claim multiple instances of LDS mobile devices. For first- and second-time incidents of LDS mobile devices, the ITPM will, at a minimum, ensure the employee's supervisor is notified of the LDS equipment. For third-time incidents, the ITPM will notify the employee's supervisor and AOC organizational leader. And lastly, if an LDS incident occurs for a fourth time within a two-year period, the ITPM will directly report the incidents to the OIG.

While we acknowledge the notification threshold as a positive mechanism to better hold AOC employees accountable, it does not provide a deterrent effect for future misuse of IT mobile devices by AOC employees since there is no punitive action requirement (e.g., verbal warning, letter of reprimand, employee repayment of mobile device value) working in concert with the notification process. Establishing punitive actions in the handling of egregious cases, such as the one noted above where three cellphones went missing in one-year period, not only holds employees accountable, but also offers a deterrent effect, with the potential long-term outcome of less devices going lost, damaged or stolen.

Impact

As a result, ITD created a separate LDS procedure, which bypasses the Board of Survey Process to deter future occurrences of lost, damaged or stolen mobile devices. However, without a standardized process that is consistently enforced at all organizational levels, the AOC is vulnerable to instances of cost waste, employee misconduct, other levels of criminality and information security concerns in cases where mobile devices are lost or stolen.

Conclusion

While ITD has been proactive in creating its own procedure to deal with LDS mobile devices more effectively, and with hopes of holding AOC employees more accountable, its LDS procedure, along with the Board of Survey Process lacks any sort of deterrent feature to prevent future occurrences of employee neglect or misuse with assigned IT mobile devices. An updated Board of Survey Process, with consideration to punitive action requirements in cases where mobile devices are lost, damaged or stolen would not only create a deterrent effect and encourage employee self-accountability in the handling of assigned AOC property. Such an effect also has the propensity over time to decrease the number of mobile devices or equipment that goes missing, thus lessening cost waste.

Recommendation

Recommendation 3

We recommend that the Architect of the Capitol (AOC) revise the Board of Survey Process with codified punitive actions to act as a deterrent against future instances of

egregious employee negligence and misconduct regarding the loss of AOC property, including both Information Technology mobile devices and personal property.

AOC Comment

The AOC concurs. The Board of Survey process, in accordance with AOC Order 34-45, Personal Property Manual, is conducted by the Supplies, Services and Material Management Division (SSMMD) on lost, damaged or destroyed (LDD) personal property that has been logged into and accounted for in the Maximo inventory control system (ICS). Restitution of LDD personal property logged into and accounted for in Maximo are identified in AOC Order 34-45 under Section 8.13.5 and Appendix D. Additionally Policy Memorandum 752-1, Discipline, lists specific penalties in its Table of Penalties for loss or damage of government property.

Mobile devices and other ITD personal property are not logged into or accounted for within the Maximo ICS system; therefore, a Board of Survey is not conducted by SSMMD. Thus, ITD will incorporate a process to address the auditor's recommendation within the Order 8-4 update.

OIG Response

We reviewed the management comment and determined it addresses the finding and recommendation.

Finding 4

ITD Lacks Frequent Inspections of IT Mobile Device Property

We found that ITD does not frequently perform inventory inspections for IT mobile devices—cellphones, laptops and iPads. Rather, ITD uses its Annual Telecom Memorandum as a self-reported audit feature to track these types of mobile devices, which poses not only an information security vulnerability to the AOC, but also a physical security vulnerability to the agency.

This occurred because AOC organizations are only required to conduct inventory inspections of fixed IT accountable equipment (e.g., desktop computers, printers, digital senders and Apple televisions) located in AOC offices and facilities twice-annually, and ITD does not perform inventory inspections of IT mobile devices. Rather, ITD uses the Annual Telecom Memorandum for issued cellphones, laptops and iPads as an audit feature and inventory mechanism to account for IT mobile devices.

As a result, the lack of frequency of inspections for IT property and solely relying on the Annual Telecom Memorandum to account for issued mobile devices, presents a significant gap in IT property accountability and control across the AOC. Furthermore, there is the potential for a device to be lost, stolen or misused and fall into the hands of a bad actor within days of an AOC employee signing the annual memorandum. Without proper notification, the agency would be unaware of the incident until renewal of the next year's Annual Telecom Memorandum. This represents a potential security vulnerability to the AOC, even if only a single isolated incident occurs, since an unauthorized user could access agency information, movements and systems unbeknownst to AOC.

Discussion

AOC Order 8-4 highlights that physical inventory inspections help to validate the existence and location of accountable IT property, and that they help to also uncover idle or lost, damaged or destroyed property. Historically, ITD would conduct at least one physical inventory inspection of office-fixed assigned accountable IT property (e.g., desktop computers, printers, TVs, digital senders, etc.) for each AOC organization at least annually. Organizational APOs would certify and submit their inventory reports to the ITPM at the time of inspection, and both parties would work to reconcile any noted discrepancies. However, since the onset of the COVID-19 pandemic in 2020, ITD has not conducted these annual inventory inspections due to resource shifts and the need to address the transition to a more virtual workplace.

During our review, we found that ITD does not perform frequent inventory inspections for IT mobile devices—cellphones, laptops, and iPads. Rather, ITD uses its Annual Telecom Memorandum as an audit feature to track these types of mobile devices. The telecom memorandum identifies the device being issued, the manufacturer, make/model, serial number and AOC inventory barcode tracking number. The memorandum also contains a Terms of Use clause stipulating restrictions on use, a privacy statement and user responsibilities that the employee must acknowledge and agree to either at the time of initial issue or re-issue of a device.

Relying solely on the self-reported Annual Telecom Memorandum to account for IT mobile devices presents a potential gap in IT mobile device accountability and control across the AOC and places the AOC in a potentially vulnerable information and physical security state should individuals, other than employees, be able to access AOC systems and information. More specifically, examples depicting the AOC's vulnerability include unauthorized users having the ability to potentially access agency specific personally identifiable information (e.g., email addresses, telephone numbers and employee workplace locations) and sensitive emails, including U.S.

Capitol Police Alerts.⁷ This poses not only an information security vulnerability to the AOC, but also a physical security vulnerability to the agency.

The OIG's concern is further expressed from the result of a substantiated 2021 OIG investigation,⁸ where an AOC employee (who had a history of requesting replacement iPhones) claimed they lost another iPhone and needed a replacement. The iPhone reported as lost was the same phone the employee told their supervisor they lost approximately four months earlier. The OIG investigation revealed that in that four-month period that phone was supposedly lost, more than 1,200 incoming and outgoing voice calls were made and nearly 9,000 text, picture and video messages were either sent or received.

Although, the AOC could immediately deactivate AOC mobile devices, the effectiveness of that countermeasure to safeguard sensitive agency information is reliant on how promptly the device is reported lost, stolen or missing by an AOC employee, which in some cases could take days, weeks or months as evidenced by the OIG investigation noted above.

Impact

As a result, there is the potential for a mobile a device to be lost, stolen, or misused and fall into the hands of a bad actor within days of an AOC employee signing the annual telecom memorandum. If the incident is appropriately reported in a timely manner, then ITD could immediately deactivate the mobile device so it cannot be accessed. However, without proper and timely notification, the agency would be unaware of the incident until renewal of the next year's annual telecom memorandum, posing an inherent risk to internal security controls and spillage/pilferage with no accountability. The OIG believes consideration should be given to scenarios such as this, especially given the AOC's more recent shift and transition to a more remote work environment.

Conclusion

While the COVID-19 pandemic has created challenges for ITD to conduct their annual physical inventory inspections for fixed-office IT equipment across AOC organizations, ITD should resume those inspections to validate the existence and location of assigned IT accountable property. Furthermore, the lack of frequency of inspections for IT mobile devices and solely relying on the Annual Telecom

⁷ U.S. Capitol Police Alerts inform AOC employees and Congressional members and staff across the Capitol campus about potential threats, emergency preparedness drills, events, planned demonstrations and road closures. Although not in all cases, these Alerts often contain information that would not be expressly communicated with the public.

⁸ <https://www.oversight.gov/sites/default/files/oig-reports/aoc/2021-0004-invi-sup-updated-oversight-post-final.pdf>

Memorandum to account for issued mobile devices, presents a potential gap in IT property accountability and control across the AOC, especially as the agency continues to move to a remote work environment.

Recommendation

Recommendation 4

We recommend that the Chief Information Officer, establish internal controls in addition to the current Annual Telecom Memorandum requirement, to identify indications of a mobile device being lost, damaged or stolen and have processes in place to act accordingly.

AOC Comment

The AOC does not concur. The Annual Telecom Memorandum has proven to be an effective point-in-time inventory process, just as any other method used within the AOC. Additional inventory activities, be they visual or self-reporting, will create an unnecessary administrative burden on the AOC staff yielding little value in return.

Additionally, the implementation of the following mitigation controls significantly reduces the risk presented by lost, damaged or stolen devices:

- 1.) User accounts are disabled after 90 days of inactivity.
- 2.) Laptops are removed from the AOC's domain after 90 days of not being logged in, thus preventing access to network resources even with proper login credentials.
- 3.) All mobile devices require two-factor authentication before being accessed.
- 4.) All mobile devices are protected with FIPS 140-2-compliant data at rest encryption
- 5.) iPhones/iPads will wipe automatically after seven failed logins but will remain supervised in the management console.
- 6.) Zero usage exceeding 90 days on a cell phone (iPhone, Android)/iPad (with LTE service) triggers ITD to work with the responsible accountable property officer to determine if the device is still required (this will be included in the policy update).
- 7.) All AOC-issued mobile devices are remotely managed through enterprise security platforms.
- 8.) All AOC-issued mobile devices can be remotely wiped at any time, which is standard practice when a device is reported lost or stolen.

OIG Response

We recognize that the AOC does not concur with this recommendation. The OIG considers the recommendation unresolved. Although the AOC sees little to no value returned by exploring additional internal controls, outside of its Annual Telecom Memorandum, to identify indications of mobile devices being lost, damaged or stolen, the response does not adequately address the OIG's concern over ITD's sole reliance on its Annual Telecom Memorandum as an inventory management tool to account for mobile devices.

While we feel that the Annual Telecom Memorandum, in addition to the other eight mitigation controls highlighted in the AOC's response, are good inventory management tools, the effectiveness of these controls is contingent on whether a lost, damaged or stolen mobile device is reported as such in a timely manner. The controls do not account for instances where lost, damaged or stolen mobile devices are reported in an untimely manner as discussed in the evaluation report's narrative and AOC OIG investigations that served as the impetus for this evaluation. Without proper and timely notification of lost or stolen mobile devices, the agency would be unaware of the incident until renewal of follow-on annual telecom memorandum, thus posing an inherent risk to internal security controls and spillage/pilferage with no accountability.

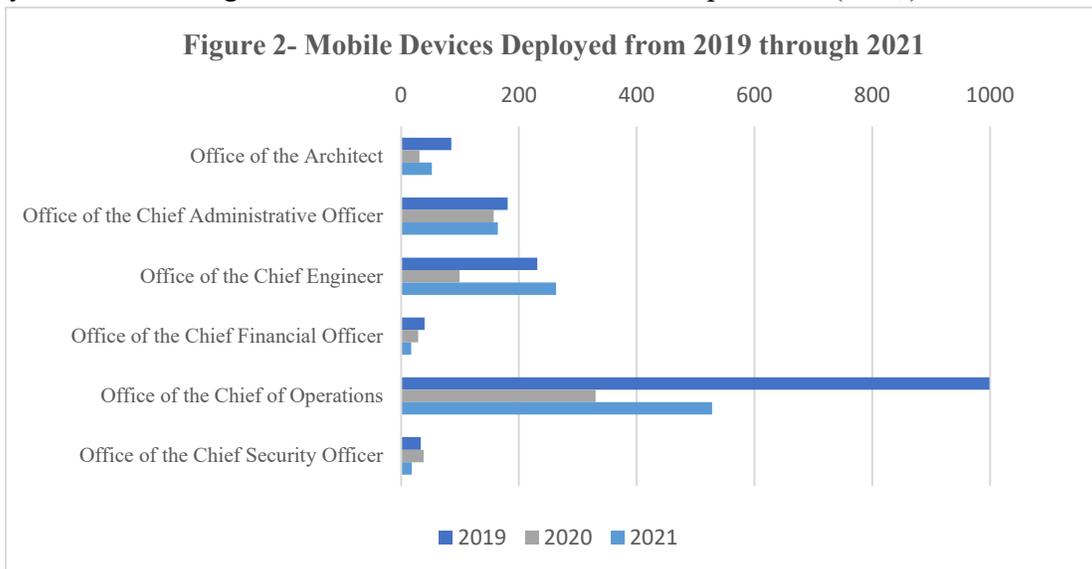
The OIG continues to recommend that the CIO establish internal controls in addition to the current Annual Telecom Memorandum requirement, to identify indications of a mobile device being lost, damaged or stolen, and have processes in place to act accordingly. The OIG will monitor the program progress and follow up on the development of any action items and implementation of program improvements.

Data Snapshot

ITD's Total Mobile Device Inventory and Lost Damaged and Stolen Mobile Devices for Years 2019 through 2021

ITD Mobile Device Inventory

From calendar years 2019 through 2021, the AOC's ITD had a total of 9,264 mobile devices in its inventory, this included a stock of cellphones, laptops and iPads. Respectively, ITD deployed 3,295 of those mobile devices to employees across the agency, representing a 35.6 percent deployment rate. Figure 2 represents ITD's disbursement of mobile device property by AOC business component for calendar years 2019 through 2021. The Office of the Chief of Operations (OCO)⁹ leads in all

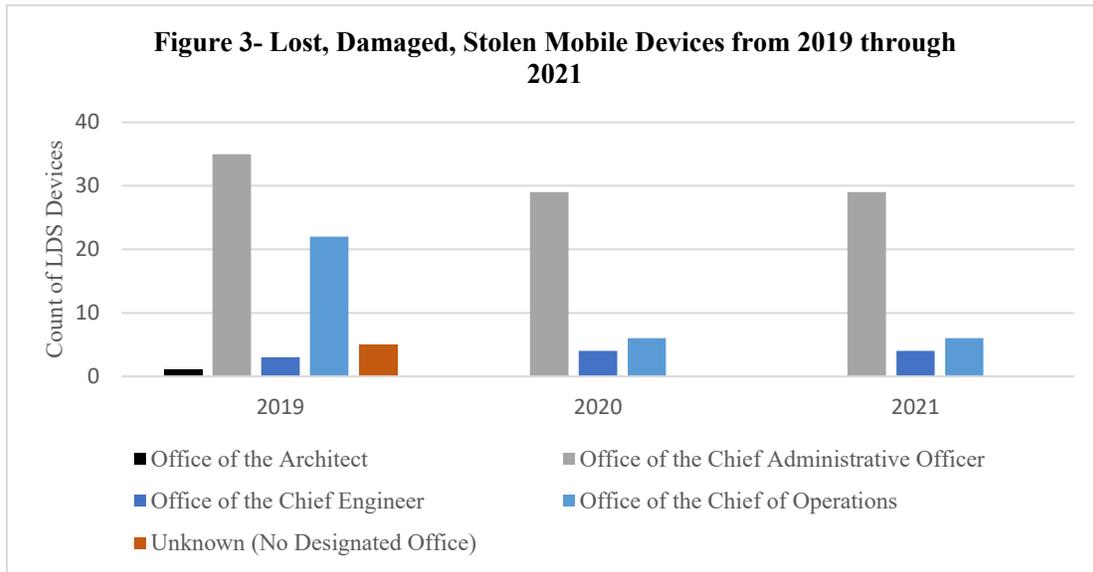


years of mobile device disbursement due to sheer volume of employees the business component holds over other AOC offices. IT officials noted that the COVID-19 pandemic also led to increased spikes in the disbursement of IT mobile devices across all other AOC offices during 2019 and 2021 as the agency transitioned from an onsite work environment to a more remote work environment. This transition prompted employees that may have had a desktop computer prior to the pandemic to request a laptop computer to work remotely.

Lost, Damaged or Stolen Mobile Devices

⁹ OCO is made up of the following ten organizations: Capitol Building, Capitol Grounds and Arboretum, Capitol Visitor Center, House Office Buildings, Library Buildings and Grounds, Office of the Chief of Operations, Senate Office Buildings, U.S. Supreme Court, U.S. Botanic Garden, and Utility Plant Operations and Services.

Figure 3 represents the total number of mobile devices designated by ITD as lost, damaged or stolen in 2019 through 2021. The Office of the Chief Administrative Officer (OCAO) consistently experienced the highest level of lost, damaged or stolen mobile devices.



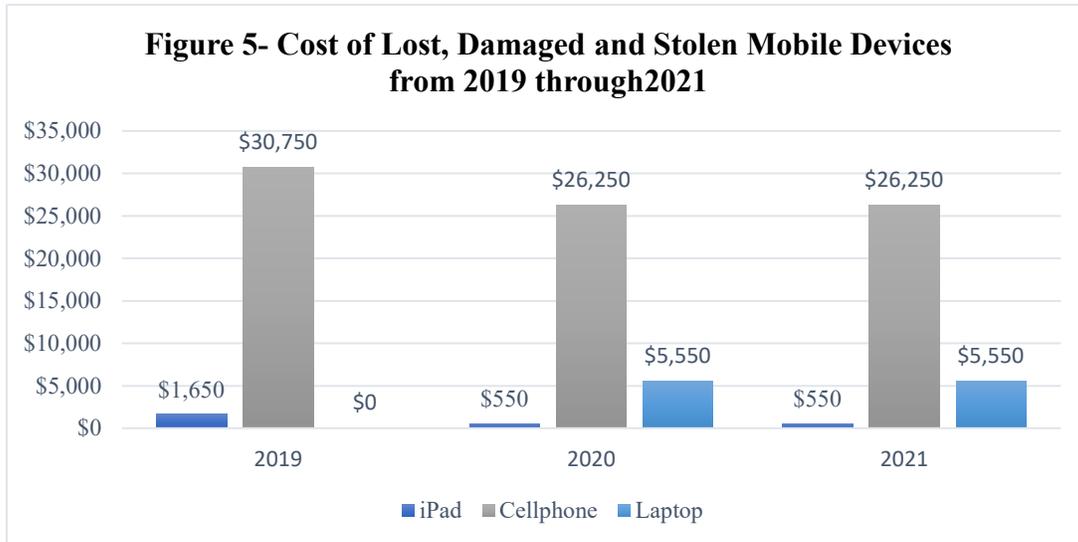
We further compared device deployment data (see Figure 4) and found that ITD deployed 50 percent of its OCAO designated mobile device inventory in 2019. Of that, 19 percent of OCAO's devices were designated as lost, damaged or stolen. This is in direct contrast with FY 2019 data reported by other AOC organizations like the Office of the Chief Engineer (OCE), Office of the Chief Financial Officer and OCO, that each had approximately a 60 percent mobile device deployment rate, with two percent or less falling in the Lost, Damaged or Stolen category.

Figure 4- Rate of Deployment Compared to Rate of Lost, Damaged and Stolen Mobile Devices						
Jurisdiction	2019		2020		2021	
	Deployment Rate	LDS of Deployed	Deployment Rate	LDS of Deployed	Deployment Rate	LDS of Deployed
Office of the Architect	44%	1%	15%	0%	24%	0%
Office of the Chief Administrative Officer	50%	19%	34%	18%	33%	18%
Office of the Chief Engineer	62%	1%	24%	4%	44%	2%
Office of the Chief Financial Officer	63%	0%	38%	0%	22%	0%
Office of the Chief of Operations	61%	2%	18%	2%	26%	1%
Office of the Chief Security Officer	42%	0%	38%	0%	17%	0%

Moreover, in 2020 ITD deployed 34 percent of its OCAO designated mobile devices and of that number of devices 18 percent were designated as lost, damaged or stolen. The same number of OCAO LDS mobile devices were reported in 2021 because ITD carried over 2020's LDS inventory due to no newly reported LDS mobile device inventory. ITD attributed this occurrence due to a max telework environment and the fact that no mobile devices were requested to be decommissioned in 2021. Taken altogether, OCAO's LDS rate was consistently higher than other AOC organizations from 2019 through 2021, even though other AOC offices like OCO had higher mobile device deployment numbers across the agency. Most other AOC business components had an LDS rate of less than two percent annually, with one exception—the OCE had a four percent LDS rate in 2020.

The propensity of IT mobile devices going lost damaged or stolen not only presents a security concern for the AOC, where a bad actor could gain access to AOC systems and information, but it also presents a financial cost to the agency.

Figure 5 represents the amount lost to the AOC due to incidents of lost, damaged or stolen IT mobile devices from 2019 through 2021.¹⁰ As depicted, lost, damaged or stolen cellphones are the most likely device leading to cost-waste over the three years. In the three-year span, the AOC absorbed an approximate cost waste total of \$97,100.



While this number represents the approximate valued cost of the mobile device equipment that went the lost, damaged or stolen, it does not consider the added cost to replace those items. Hypothetically, the total dollar loss to the AOC after replacing the lost, damaged or stolen devices from 2019 through 2021 could be doubled, resulting in an actualized cost to the AOC of approximately \$194,200.

¹⁰ ITD provided the OIG with mobile device cost data and that cost data was used to conduct our analysis. More specifically, ITD stated that the unit cost per cellphone/ iPhone ranged from \$500-\$1000, we used the averaged amount of \$750 for analysis. The unit cost per laptop reported by ITD ranged from \$1700-\$2,000, we used the averaged amount of \$1,850 for analysis. For iPads, ITD provided an actual unit cost of \$561.22 per device, we used the amount of \$550 when running our analysis.

Appendix A

Scope and Methodology

This evaluation was announced on November 8, 2021 and was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency’s “*Quality Standards for Inspection and Evaluation (2020)*.” These standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

This evaluation was self-initiated by the AOC OIG as was consistent with our 2021 agency Management Challenges, which listed Waste and Accountability as a Management Opportunity and Performance Challenge. Our objective was to determine if adequate mechanisms and controls were in place to account for agency issued electronic devices (cellphones, laptops and iPads), the extent to which vulnerabilities exist due to lost, stolen or misplaced electronic devices and if adequate procedures are in place to report, track and replace missing property.

During our evaluation we reviewed relevant AOC policies and procedures related to the accountability and control of AOC ITD equipment from fiscal years 2019 to 2021. We also reviewed AOC ITD equipment logs and records for the noted period to establish if appropriate oversight measures were in place to report, track and replace missing equipment. Lastly, we conducted interviews with the appropriate AOC officials and staff and issued an agency-wide questionnaire to APO’s to determine how ITD inventory accountability and control processes and procedures were carried out in a day-to-day manner.

Use of Computer-Processed Data

We used computer-processed data in the performance of our work and determined that the data provided was sufficiently reliable to support any conclusions made from its use.

Prior Coverage

Since 2018, we have completed one evaluation examining the AOC’s inventory accountability and controls program for AOC personal property. Given unique program processes and requirements, this evaluation did not include a review of IT equipment or mobile devices. The OIG’s Investigations Division also conducted 11 investigations for the same time period, looking into matters of misuse and lost, damaged or stolen ITD property and equipment.

Appendix B

Management Comments



Architect of the Capitol
 U.S. Capitol, Room SB-16
 Washington, DC 20515
 202.228.1793
 www.aoc.gov

United States Government

MEMORANDUM

DATE: July 19, 2022

TO: Christopher P. Failla
 Inspector General

FROM: J. Brett Blanton 
 Architect of the Capitol

SUBJECT: Response to Evaluation of the Architect of the Capitol's Information Technology Division's Inventory Accountability and Controls (Project No. 2022-0002-IE-P)

Thank you for the recommendations identified in the attached draft evaluation report. Provided below are our responses regarding findings and recommendations contained within the report and an estimated completion date for each finding.

Before addressing the recommendations, the Architect of the Capitol (AOC) would like to point out one item of consideration for the Office of Inspector General (OIG). On page 5 of the OIG Report, it states "Because the AOC is a legislative branch agency, it is not subject to the Federal Property and Administrative Services Act of 1949." This statement was reviewed by the AOC, and we determine it to be inaccurate. The AOC was singularly excepted from the act provisions by subsequent legislation (Public Law 81-754), but there is no blanket exception for legislative branch agencies in the act (see 40 United States Code §102(5)). For that reason, it would be more appropriate for the OIG Report to simply state: "The AOC is not subject to the Federal Property and Administrative Services Act of 1949."

OIG Recommendation 1 We recommend that the Chief Information Officer update Information Technology Division's current policy for accountable Information Technology property, to include the incorporation of defined program personnel roles, requirements aligned with the property management lifecycle, and all current program procedures.

AOC Response:

The AOC concurs with the auditor's recommendation. The Information Technology Division (ITD) will update AOC Order 8-4, Accountable IT Property to incorporate defined program personnel roles and align requirements with the property management life cycle and all current program procedures.

The estimated completion date for Recommendation 1 is June 30, 2023.

OIG Recommendation 2 We recommend that the Chief Information Officer continue pursuit of transitioning to a single asset management system that addresses its program needs to track

accountable and consumable Information Technology (IT) property and establish a detailed implementation plan with target dates to transition to a single asset management system for accountable and consumable IT property as currently captured in Cireson and Jumpstock.

AOC Response:

The AOC concurs with the auditor's recommendation. Leveraging a robust IT service management (ITSM) platform with incorporated IT asset management, when properly implemented, provides significant accountability and life cycle of IT assets in alignment with industry and Information Technology Infrastructure Library (ITIL) best practices. ITD is currently assessing more robust ITSM tools for future implementation.

The estimated completion date for Recommendation 2 is September 30, 2024. This is an unfunded requirement requiring adherence to the AOC budget and procurement processes.

OIG Recommendation 3 We recommend that the Architect of the Capitol (AOC) revise the Board of Survey Process with codified punitive actions to act as a deterrent against future instances of egregious employee negligence and misconduct regarding the loss of AOC property, including both Information Technology mobile devices and personal property.

AOC Response:

The AOC concurs with comment regarding the auditor's recommendation. The Board of Survey process, in accordance with AOC Order 34-45, Personal Property Manual, is conducted by the Supplies, Services and Material Management Division (SSMMD) on lost, damaged or destroyed (LDD) personal property that has been logged into and accounted for in the Maximo inventory control system (ICS). Restitution of LDD personal property logged into and accounted for in Maximo are identified in AOC Order 34-45 under Section 8.13.5 and Appendix D. Additionally, Policy Memorandum 752-1, Discipline, lists specific penalties in its Table of Penalties for loss or damage of government property.

Mobile devices and other ITD personal property are not logged into or accounted for within the Maximo ICS system; therefore, a Board of Survey is not conducted by SSMMD. Thus, ITD will incorporate a process to address the auditor's recommendation within the Order 8-4 update.

OIG Recommendation 4 We recommend that the Chief Information Officer, establish internal controls in addition to the current Annual Telecom Memorandum requirement, to identify indications of a mobile device being lost, damaged or stolen and have processes in place to act accordingly.

AOC Response:

The AOC does not concur with the auditor's recommendation. The Annual Telecom Memorandum has proven to be an effective point-in-time inventory process, just as any other method used within the AOC. Additional inventory activities, be they visual or self-reporting, will create an unnecessary administrative burden on the AOC staff yielding little value in return.

Additionally, the implementation of the following mitigation controls significantly reduces the risks presented by lost, damaged or stolen devices:

- 1.) User accounts are disabled after 90 days of inactivity.
- 2.) Laptops are removed from the AOC's domain after 90 days of not being logged in, thus preventing access to network resources even with proper login credentials.
- 3.) All mobile devices require two-factor authentication before being accessed.
- 4.) All mobile devices are protected with FIPS 140-2-compliant data at rest encryption.
- 5.) iPhones/iPads will wipe automatically after seven failed logins but will remain supervised in the management console.
- 6.) Zero usage exceeding 90 days on a cell phone (iPhone, Android)/iPad (with LTE service) triggers ITD to work with the responsible accountable property officer to determine if the device is still required (this will be included in the policy update).
- 7.) All AOC-issued mobile devices are remotely managed through enterprise security platforms.
- 8.) All AOC-issued mobile devices can be remotely wiped at any time, which is standard practice when a device is reported lost or stolen.

Distribution List:

J. Brett Blanton, Architect of the Capitol
Peter Bahm, Chief of Staff
Mary Jean Pajak, Deputy Chief of Staff
William O'Donnell, Chief Administrative Officer
Jon Migas, Chief Information Officer
Harold Honegger, Chief, Supplies, Services and Material Management Division

Doc. No. 220630-02-01

Notification Letter



Office of Inspector General
Fairchild Bldg.
499 S. Capitol St., SW, Suite 518
Washington, D.C. 20515
202.593.1948
www.aoc.gov

United States Government
MEMORANDUM

DATE: November 08, 2021

TO: J. Brett Blanton
Architect of the Capitol

FROM: Christopher P. Failla, CIG 
Inspector General

SUBJECT: Announcement for Evaluation of the Architect of the Capitol's (AOC's)
Information Technology Division (ITD) Inventory Accountability and Controls
(2022-0002-IE-P)

This is to notify you that the Office of Inspector General is initiating an evaluation of the AOC's ITD Inventory Accountability and Controls. Our objective for this evaluation is to determine if adequate mechanisms and controls are in place to account for issued laptops and cell phones and to what extent procedures are in place to report, track and replace missing property.

We will contact the appropriate AOC offices to schedule an entrance conference in the upcoming weeks. If you have any questions, please contact Josh Rowell at Joshua.Rowell@aoc.gov or 410.443.5015 or Chico Bennett at Chico.Bennett@aoc.gov or 202.394.2391.

Distribution List:

William O'Donnell, Chief Administrative Officer
Peter Bahm, Chief of Staff
Mary Jean Pajak, Deputy Chief of Staff
Jason Baltimore, General Counsel
Jon Migas, Chief Information Officer

Acronyms and Abbreviations

AOC	Architect of the Capitol
APO	Accountable Property Officer
CIO	Chief Information Officer
CVC	Capitol Visitor's Center
GSS	General Support System
ICS	Inventory Control System
IT	Information Technology
ITPM	Information Technology Program Manager
ITD	Information Technology Division
LDD	Lost, Damaged or Destroyed
LDS	Lost, Damaged or Stolen
OCAO	Office of the Chief Administrative Officer
OCE	Office of the Chief Engineer
OCO	Office of the Chief of Operations
OIG	Office of Inspector General
PC	Property Custodian
SSMMD	Supplies, Services and Material Management Division



OFFICE OF THE INSPECTOR GENERAL

Fairchild Building, Suite 518

499 South Capitol Street, SW

Washington, DC 20515

(202) 593-1948

hotline@aoc-oig.org