Montgomery County, Maryland
Office of the County Executive
Office of Internal Audit

Information Technology Audit
IT Asset Management

January 21, 2022

MCIA-22-2

Highlights

Why MCIA Did this Review

The Montgomery County Office of Internal Audit (MCIA) conducted an Information Technology (IT) audit of certain asset management functions within the Montgomery County Department of Technology and Enterprise Business Solutions (TEBS). The audit included a review of policies and procedures surrounding the County's asset management processes and assessed effectiveness of the County's IT asset management function within TEBS, specifically the Device Client Management (DCM) program. Within TEBS, DCM is responsible for full lifecycle management of all approved endpoint devices, such as laptops, desktops, tablets, workstations, and hardware, authorized for use by County employees, contractors, and business associates. This report includes results specific to IT assets managed by DCM and TEBS. Findings with respect to mobile devices are discussed in a separate MCIA report.

This audit was conducted as a result of MCIA's 2019 IT risk assessment. The focus was to evaluate the current internal control environment of the County's IT asset management function. The audit was conducted by the accounting firm SC&H Group, Inc., under contract with MCIA.

MCIA is making eight recommendations to DCM to strengthen the existing control environment within the County's IT asset management processes.

January 2022

IT Audit of the County's IT Asset Management Processes

What MCIA Found

The audit of the County's asset management determined that established IT asset management processes and controls optimize IT asset lifecycles and support achievement of secure IT asset disposition. The audit identified several opportunities to mitigate risks. The risks can be addressed by enhancing or implementing internal controls within the asset management processes.

We identified eight recommendations to strengthen controls and mitigate risks within the County's asset management processes:

1. Develop policy and procedure documentation that defines the roles and responsibilities of the Telaforce Deskside team and physical security requirements at the DCM Warehouse and Replacement Depot.
2. Update and enforce formal policy requirements, including retaining equipment order forms, transferring of assets to the end user, and evidence of tagging and/or assignment of appropriate means of asset identification.
3. Develop and enforce completion of standardized IT purchase request forms.
4. Reinforce the DCM Policy Manual and the Purchase Card Policy with departments specific to the approved process to request and purchase IT assets.
5. Incorporate DCM action items resulting from IT asset inventory sweeps into a formal ServiceNow ticket for enhanced tracking and monitoring.
6. Design and implement alternative ways to perform asset inventory sweeps considering the current remote/telework environment.
7. Formalize the process for replacement of IT assets to ensure required documentation is available and retained for approval, acquisition, installation, and provisioning access.
8. Implement a formal reconciliation process to verify all disposed IT assets delivered to the contracted service provider are documented as destroyed within supporting documentation provided with the submitted Certificate of Destruction.

TABLE OF CONTENTS

Objectives

This report summarizes the information technology (IT) audit of Montgomery County's (the County) IT asset management processes. The audit was performed by SC&H Group, Inc. (SC&H), under contract with the Montgomery County Office of Internal Audit (MCIA).

The audit included meeting with members of the County's Department of Technology and Enterprise Business Solutions (TEBS) to build upon the knowledge obtained through the County's Information Technology Risk Assessment (ITRA), and to understand the following:

1. Documented policies, procedures, standards, and/or guidelines
2. Processes for acquiring, inventorying, and disposing of IT assets
3. IT asset management responsibilities
4. IT asset management lifecycle functions performed in a standardized manner

The audit objectives were to:

1. Ensure sufficient policies and procedures are in place for procuring, inventorying, and disposing of IT assets (e.g., computing devices including servers and data center equipment, laptops, and desktops).
2. Understand, document, and test the procurement processes/controls in place around in-scope IT assets.
3. Ensure the IT asset management process is controlled, monitored, and reviewed in compliance with industry best practices.
4. Ensure that procedures are in place for updating inventory upon IT asset retirement or employee transfer or termination.
5. Ensure that sufficient controls are in place over software asset management including identification of unauthorized software, documenting and evaluating controls over loaner laptops, documenting and evaluating controls over wiping devices that are no longer in active inventory, and understanding the process for remotely disabling machines that are non-recoverable.

We would note that findings related to mobile devices resulting from the IT audit are discussed in a separate MCIA report, MCIA-22-3.

Background

County-wide Information Technology Overview

The County manages hardware, software, and technology through a combination of centralized and decentralized functions to enable employees to provide quality services to citizens and businesses, deliver information and services to citizens, and increase productivity.

TEBS is responsible for assisting the County's departments with identifying innovative technology solutions, helpdesk support, IT security, and IT asset procurement and management.

Asset Management Overview

Asset Management is the overall process of procuring, distributing, monitoring, and retiring devices and software to limit exposure to risk throughout the lifecycle of a device. Established asset management processes and controls reduce the risk of devices and assets being inappropriately purchased, strengthen the overall enterprise IT security environment, and

ensure appropriate use of County funds. Failure to follow sufficient processes and controls throughout the asset's lifecycle could result in the potential for outdated devices and security controls and an increased risk of device failure.

Centralized IT Functions

TEBS provides asset management services and support through the following offices and divisions:

1. Office of Broadband Programs & Infrastructure Modernization
    a. Development Operations & Server Support
2. One Face Forward Initiative
    a. Device Client Management (DCM)

Device Client Management

DCM is responsible for the full lifecycle management of all approved endpoint assets authorized for use by County employees, contractors, and business associates (authorized users). DCM is tasked with the overall management, support, and acquisition of County IT assets utilized directly by authorized users. This includes, but is not limited to the following:

1. Planning
2. Standards and Documentation
3. Support Services
4. Innovation
5. Budgeting
6. Acquisition
7. Asset Management
8. Endpoint Device Management
9. Contract Administration and Coordination
10. Security

DCM utilizes Microsoft's System Center Configuration Management (SCCM) software to manage asset inventory listings.

Asset Management Processes

DCM has formal policy and procedure documents, *DCM Policy Manual* and *DCM Procedure Manual*, respectively, detailing the processes related to procuring and managing IT assets for authorized users. The following is an overview of the specific processes and IT asset types under DCM's (laptops, desktops, tablets, and workstations) and TEBS's (servers) responsibility:

Laptops, Desktops, Tablets, and Workstations

Acquisition and Management

DCM supervises, in conjunction with the Office of Procurement (PRO), all endpoint IT equipment acquisition activities in the County. Additionally, DCM tracks, approves, and processes all IT computer equipment expenditures for TEBS. Requests for equipment are initiated by authorized users by visiting DCM's SharePoint site and completing the online equipment order form (*DCM Standard Order Form*). Upon receipt of the completed equipment order form, DCM provides a quote based on contracted vendor pricing for all requested equipment for review by the requesting department. Following review and approval by a supervisory level employee from the requesting department, DCM requests department cost codes in order to finalize and place the order. The submitted order request form, the quote provided by DCM, and supervisor approval are all managed via email communications between the respective parties. Following approval, the Acquisitions Manager within the Telaforce

Deskside Team (third party service provider responsible for receiving and provisioning access to IT assets managed by DCM) places the order.

Purchased assets are received directly by the Telaforce Deskside Team at the DCM Warehouse, where purchased assets are stored within the Warehouse until provisioning of access occurs. Separate team members perform the following:

1. Receive and scan the new assets
2. Image assets (scan the barcodes) and ready them for deployment.

Authorized users schedule a pickup time for IT asset purchases via a ServiceNow ticket. Prior to providing the requested asset to the authorized users, the Telaforce Deskside Team installs/provisions the new IT asset with the appropriate software (utilizing a series of DCM developed network images). When the IT asset is ready for deployment, the authorized user picks up the new IT asset from the DCM Replacement Depot.[1]

DCM manages the inventory of IT assets via the DCM Configuration Management Database (CMDB). Criteria for each IT asset maintained within the CMDB includes, but are not limited to:

- Make
- Model
- Serial number
- PO number
- Barcode
- Tag ID
- Status
- Seat type
- Client ID
- Department
- Location
- User name
- Description
- Last Inventoried Date
- Warranty Expiry Date
- Last Logged On Date
- Last Logged On User

To maintain an accurate inventory, DCM updates the CMDB regularly through several channels, which are triggered by the following activities and mechanisms:

- IT Help Desk (ITHD) calls: Asset verification occurs with each call. Updates are performed as needed.
- Inventory Sweeps: At the request of County departments, and at the discretion of the DCM office, inventory sweeps may be conducted to ensure accurate inventory information.
- New Assets: New assets are added to the DCM inventory as soon as assets arrive at the DCM Warehouse.
- Field Activities: The DCM inventory is updated as assets are relocated and reassigned during field activities performed by DCM. If County departments elect to perform

[1] This process was put in place in the summer of 2020. Prior to the pandemic, the Telaforce Deskside Team would deliver the new IT asset to the authorized person's County location.

activities that affect the location, status, and/or user assignment of DCM managed assets, they are required to provide updated asset inventory information to the ITHD.
- Missing Asset Reports: Periodically, a report is run to identify assets that meet the criteria for missing assets (age over six years, has not been logged in within the last year, and has not been inventoried in the past four years). A list of assets that are identified as missing are provided to the County departments assigned to the asset(s). If no update on these assets is provided within 30 days, the assets are removed from the DCM inventory.
- Disposal: The DCM inventory is updated as assets move through the disposal process.

Pricing
The County has sub-contracted through a third party (Telaforce Deskside via CACI, Inc.) for acquisition of IT assets (e.g., laptops, desktops, tablets, workstations, and other hardware). IT asset requests are submitted to the Telaforce Deskside who utilizes additional sub-contractors (e.g., Greenpages Technology Solutions, Lenovo, Dell, and other manufacturers) for providing quotes and ordering IT assets.

At the beginning of each fiscal year, DCM meets with the sub-contracted third party to review new model types for certain IT assets (e.g., laptops, desktops, and tablets), including available specifications for those models, and negotiates and locks in pricing for the next year. On a quarterly basis, DCM reviews and verifies equipment specifications and pricing. Telaforce Deskside is responsible for purchasing IT assets purchase directly with manufacturers in order to obtain the requested asset specifications required by DCM. IT asset pricing provided by DCM also includes an extended warranty and costs associated with DCM servicing the asset throughout its lifetime. Additionally, for certain purchases, such as the replacement projects, DCM receives bulk purchase pricing, which can be lower than direct retail pricing.

Missing, Disposed, and Replaced Assets
The County utilizes CMDB and SCCM software to add assets to the County's asset inventory and update details regarding the asset's status (i.e., 'Missing', 'Disposed', etc.). Within the inventory platform, additional information for each asset includes the asset owner, device type, operating software used, and other essential information. DCM provides end-of-life hardware replacements for all DCM supported Full Seat (primary device) systems (laptop or business class tablet). The lifecycle of systems is determined annually based on multiple factors including the age, condition, and operating system, as well as input (available budget/resources) from the Office of Management and Budget (OMB).

DCM's comprehensive disposal process ensures that County data is not exposed to outside entities and is fully compliant with applicable environmental laws. DCM adheres to Department of Defense Data Security Standard 5220.22M by employing industry standard wipe stations to ensure all storage media devices are properly sanitized.
- DCM replaces and removes surplus IT electronic equipment (including, but not limited to desktop computers, laptops, mobile devices, printers, monitors, servers, networking equipment, and copiers) from any County facility.
- Surplus equipment is stored at the secure DCM Warehouse for two weeks.
- All removed equipment is completely sanitized of any County distinguishable labels, logos, and assets tags prior to being disposed of according to County guidelines.

Servers
Acquisition, Management, and Disposal

TEBS's Office of Broadband Programs and Infrastructure Modernization is responsible for the acquisition, management, and disposal of servers. Requests for purchasing new/replacement servers are initiated by the Office of Broadband Programs and Infrastructure Modernization through bulk requisition and purchase orders and approved by the Office of Management and Budget, based on available budget/resources. The Office of Broadband Programs and Infrastructure Modernization utilizes Potomac eCycle for facilitation of the wiping, sanitization, and destruction of servers.

Scope and Methodology

The audit was conducted from March 2021 to November 2021. The scope of this report is focused on the current asset management processes maintained and administered by DCM and TEBS. In-scope IT assets that DCM is responsible for include laptops, desktops, tablets, and workstations, while in-scope IT assets that TEBS is responsible for are servers. Processes included the following:

1. Asset management policies and procedures, content, and document development to ensure IT asset management lifecycle functions are performed in a standardized manner.
2. Asset management process and supporting activities from other processes necessary to manage procurement and acquisition of IT assets.
3. Asset management process and supporting activities supporting management / monitoring of use of IT assets.
4. Asset management process and supporting activities from other processes necessary to manage reclamation and IT asset destruction processes around in-scope assets.
5. Policies supporting mobile device acquisition and disposal.

The audit also included an analysis of the following for mobile devices *(results separately reported in MCIA-22-3)* related to the asset management processes from January 1, 2020 to July 31, 2021:

1. Acquisitions
2. Disposals
3. Inventory Management
4. Replacements

Scoping

SC&H performed the following procedures to obtain a preliminary understanding of the County's asset management functions.

Interviews

SC&H conducted detailed interviews and walkthroughs with DCM and the Office of Broadband Programs and Infrastructure Modernization. The purpose was to observe and document the internal controls and related risks associated with each of the following processes:

1. Policies and Procedures
2. Acquisitions
3. Disposals
4. Replacements
5. Inventory Management

Policy and Procedure Review

SC&H obtained and reviewed asset management policies and procedures, including the following documents:

1. Montgomery County Government DCM Policy Manual
2. Montgomery County Government DCM Procedure Manual
3. TEBS IT Commodities Policy

Test Plan Development

SC&H developed an audit plan to test the operational effectiveness of internal controls utilizing the information obtained during scoping, interviews, and walkthrough procedures.

Fieldwork

Fieldwork consisted of testing the operational design and/or operational effectiveness of internal controls identified during scoping and preliminary department assessment, interviews, and walkthrough procedures. SC&H prepared a document request listing for all information needed to satisfy the testing steps developed in the audit plan, including populations required to select samples for which additional information was requested. SC&H utilized both judgmental and haphazard selection methods for sampling. The following includes additional details regarding sample selections and test procedures performed.

Sample Selection

Laptops, Desktops, Tablets, and Workstations

Acquisition and Management

DCM-purchased equipment samples were selected based on the population of assets (laptops, desktops, tablets, and workstations) that were acquired during the in-scope period. The system generated population of 3,352 assets included a variety of departments and asset types. From this population, SC&H selected 25 samples of purchased equipment to complete acquisition testing.

Pricing

To evaluate the pricing comparison between IT assets purchased through DCM and via available online retailers, SC&H utilized the noted acquisition samples (with additional re-selections for duplicate asset types) above.

Additionally, to evaluate the pricing comparison between IT assets purchased independently by individual departments utilizing purchase cards (P-Cards) via online retailers, SC&H received a population report of P-Card transactions during the in-scope period. The population included 32,445 transactions, which were analyzed to identify IT asset acquisitions (laptops, computers, tablets, hardware, cell phones, etc.). From the original population, SC&H identified 1,549 IT asset purchases and selected 25 samples to complete the P-Card pricing evaluation.

Missing Devices

SC&H obtained a population of total assets and missing assets across 60 departments that DCM has records of within the CMDB. The listing included a total inventory of 17,955 assets and 1,088 missing assets. From this list of 60 departments, SC&H selected a sample of eight departments, which consisted of a total inventory of 2,650 assets and a missing inventory of 470 assets to complete the missing device testing.

Disposed Devices

SC&H obtained a population listing of assets that were disposed of by DCM during the in-scope period which consisted of 32 departments that DCM has records of within the CMDB. The listing of 32 departments included a total inventory of 1,487 assets that were disposed of across nine different dates during the in-scope period. From this population listing of disposed assets, SC&H

selected a sample of 50 disposed assets across departments and asset types (laptops, desktops, tablets, and workstations) to complete the disposed assets testing.

Replacements
From the disposed asset population above (laptops, desktops, tablets, and workstations), SC&H identified a population of five samples that had a disposal description of "FY21 Replacement." SC&H selected two of the five disposal (replacement) samples and conducted additional testing on these samples to complete the replacements testing.

Servers
Acquisition, Management, and Disposal
Server acquisitions during the in-scope period consisted of six separate transactions, with a total of 57 individual servers acquired. From the six transactions, SC&H selected a sample of two transactions, which consisted of 18 acquired servers to complete the servers acquisition, management, and disposal testing.

Documentation Review
SC&H obtained and reviewed the *DCM Policy Manual and Procedure Manual* for the IT asset types DCM is responsible for during the various lifecycle functions, such as acquiring, managing, and disposal. SC&H obtained and reviewed the following documentation created and maintained by DCM:

1. Equipment Order Form
2. Invoices generated for purchase
3. Self-installation checklists
4. Screenshots within Asset Management Database
5. Email communications between DCM and selected departments

Walkthroughs
Walkthroughs were performed with the DCM team to obtain an understanding of various sub-processes necessary to evaluate the effectiveness of internal controls, workflow between DCM and departments, and required documentation and approvals.

Internal Controls and Compliance Testing
Internal controls identified and detailed within the audit plan were tested to assess the design and operating effectiveness of the identified control activity.

1. Acquisitions: For each asset sampled, SC&H obtained supporting documentation to determine if appropriate approvals were documented and the asset was appropriately received and logged into the asset management system.
2. Pricing: For each asset sampled, SC&H obtained supporting documentation with the applicable quote from the vendor, purchase price and receipt, shipping cost, and any additional costs included within the purchase.
3. Missing Devices: For each missing asset sampled, SC&H obtained a log detailing the information associated with the asset to determine if the device was appropriately identified as 'Missing', including age of the device, last login date, and last inventoried date.
4. Disposals: For each disposed device sampled, SC&H obtained a listing of the assets which included a rationale for disposal. In addition, SC&H obtained screenshots from the asset management database detailing that the asset had been sanitized of data (or wiped) prior to the evidence of disposal.

5. Replacements: For each replacement device sampled, SC&H obtained documentation that the asset had been appropriately configured and provided to the party receiving the asset.

Validation
The preliminary test results were compiled and presented to the DCM team on August 31, 2021 and November 10, 2021. Appendix A is provided as reference for all controls tested as part of the audit.

Findings and Recommendations

Results

The audit determined the County's policies related to asset management provide insufficient governance to mitigate risks associated with managing the lifecycle of IT assets. The following seven findings were identified to strengthen and expand the County's asset management processes and controls.

Finding 1: Policy and Procedures

DCM has not formally documented and/or implemented policies and procedures to reflect the current processes in place to manage physical security at the DCM Warehouse and Replacement Depot. This includes, but is not limited to defined procedures specific to management's periodic review of physical security access to the DCM Warehouse and Replacement Depot.

Risks
Without formalized policies and procedures covering physical security requirements at the DCM Warehouse and Replacement Depot, the asset management process could:

1. Fail to hold Telaforce Deskside accountable to compliance with the policies and procedures;
2. Fail to achieve the intended objective of securing critical IT assets;
3. Not be repeatable;
4. Increase potential loss of data; and
5. Increase the risk of security breach.

Recommendation 1.1
TEBS should develop a detailed policy and procedures document that describes the required responsibilities of the team in managing physical security at the DCM Warehouse and Replacement Depot.

Finding 2: Acquisitions (Laptops, Desktops, Tablets, Workstations)

In accordance with the DCM Policy Manual, IT asset purchases require supporting documentation, including prior approval and evidence of receipt, and are required to be entered into the asset management database to ensure appropriate tracking of assets through their lifecycle. SC&H selected a sample of 25 IT asset acquisitions, and requested supporting documentation of the approval and support evidencing receipt of the asset.

The following was identified:

1. 1 of 25 samples: Standard purchase form documentation was not available.
2. 1 of 25 samples: Standard documentation showing receipt of the new asset, provisioning access, and adding the DCM bar code/asset ID was not available.
3. 2 of 25 samples: Inventory checklists were not updated completely or included inaccurate records of actual order numbers.

Risks

1. Assets being purchased without proper approval result in inappropriately acquired equipment.
2. Assets not appropriately documented when received and logged into the asset management database are more susceptible to the loss of the asset.

Recommendation 2.1

TEBS should update the DCM Manual Policy and enforce formal retention requirements for evidence of the following:

- Formal equipment order form documentation, including evidence of approval
- Documentation that IT asset purchases are received at the DCM Warehouse
- Evidence that inventory was updated to show new IT asset purchases are received and picked up by the appropriate authorized user
- Evidence of tagging and/or assigning DCM barcode/County Asset ID.

Finding 3: Acquisitions (Servers)

Acquisitions for new/replacement servers are requested by the Office of Broadband Programs and Infrastructure Modernization through bulk requisition and purchase orders and approved by the Office of Management and Budget, based on available budget/resources. Requests are submitted via an online request form and approval of servers is managed via email communication between the respective parties.

For 2 of 2 samples tested, documentation was provided supporting the request and approval of the sampled servers. However, there is no formal documentation requirement in place, such as a required IT purchase request form, to define and document minimum requirements and authorization of the request, prior to the purchase of the new servers.

Risks

1. Assets being purchased without proper approval result in inappropriately acquired equipment.
2. Assets not appropriately documented when received and logged into the asset management database are more susceptible to the loss of the asset.

Recommendation 3.1

TEBS should develop and enforce completion of standardized IT purchase request forms to be used by departments to help ensure proper approval has been obtained prior to server purchases.

Finding 4: IT Assets Acquisition Pricing

DCM utilizes Telaforce Deskside for acquisition of IT assets (e.g., laptops, desktops, tablets, workstations, and other hardware), based on agreed upon pricing at the beginning of each fiscal year. SC&H evaluated a sample of acquisitions to evaluate the actual purchase price of

the IT assets purchased directly through Telaforce Deskside against current market pricing and availability. SC&H also evaluated a sample of acquisitions made by departments via P-Card to compare the acquisition pricing to current market pricing and availability.

The following was identified:

1. For the 25 samples acquired via Telaforce Deskside, the average dollar difference between the lowest researched retail price and the Telaforce Deskside purchase price was 16% lower.
2. For the 25 samples acquired via Telaforce Deskside, the average dollar difference between the average researched retail price and the Telaforce Deskside purchase price was or 2.5% lower.
3. For the 25 samples acquired via P-Card, the average dollar difference between the lowest researched retail price and the P-Card purchase price was 9% lower.
4. For the 25 samples acquired via P-Card, the average dollar difference between the average researched retail price and the P-Card purchase price was 20% higher.

The acquisition pricing analysis included the following factors, such as: the timing of the IT asset purchase compared to current day pricing and availability; the supply and demand impacts related to the COVID-19 pandemic; the condition and availability of the IT asset (e.g. outdated model, refurbished or available for resale, or sold out/unavailable); and bulk purchase pricing and extended warranty and servicing costs.

Per the DCM Policy Manual, all IT asset purchase endpoints (laptops, desktops, workstations, and tablets) are required to be purchased directly through DCM. Upon review of P-Card transactions during the in-scope period, SC&H identified approximately 1,549 IT assets that were purchased by departments directly through the use of P-Cards instead of DCM.

Risks

1. Assets being purchased without proper approval may result in inappropriately acquired equipment.
2. Assets being purchased outside of the proper channels may result in assets being inappropriately purchased and misappropriation of County funds.

Recommendation 4.1

TEBS should communicate, train, and reinforce the requirements that departments are required to utilize the DCM SharePoint site and Order Form to request new and replacement endpoint purchases (endpoints being defined as: laptops, desktops, workstations and tablets). Further, TEBS should partner with the Department of Finance to review, update as needed, and monitor enforcement of the *P-Card Program Policy and Procedure Manual*, to ensure departments are not utilizing P-Cards for endpoint purchases.

Finding 5: Inventory Sweeps

As part of the on-going management of the CMDB, DCM conducts at least annual inventory sweeps to validate the total number of assets within each County department, and to confirm accuracy of inventory information for each asset. During the in-scope period, inventory sweeps were requested and initiated for the following departments:

- County Executive's Office (CEX)
- Department of Environmental Protection – Solid Waste Services Division (DEP-SWS)
- Office of Human Resources (OHR)

CEX:
DCM was not able to complete the requested inventory sweep due COVID-19 pandemic limitations and mandatory work from home requirements.

DEP-SWS:
For the requested inventory sweep, the process was completed and preliminary results were documented in the DCM Pre-Sweep Inventory Report, Post-Sweep Inventory Report, Department User Listing, and the Inventory Sweep Summary Sheet.

The Inventory Sweep Summary Sheet contains relevant information related to the inventory sweep, such as: dates performed, locations, point of contact, and a summary of devices in inventory pre-sweep and post-sweep. However, the Inventory Sweep Summary Sheet did not include required action items to be taken by DCM as a result of the inventory sweep. Additionally, based on follow-up discussions with DCM, there is not a formal process in place for monitoring and tracking action items that are required as a result of the of the inventory sweep.

OHR:
For the requested inventory sweep, initial steps in the process were completed through documentation of the DCM Pre-Sweep Inventory Report and a Department User Listing. The Post-Sweep Inventory Report and Inventory Sweep Summary Sheet were not completed, therefore no evidence to indicate the completion of the inventory sweep, or any action items that needed to be taken by DCM as a result of the inventory sweep were available. Additionally, there is not a formal process in place for monitoring and tracking action items that are required as a result of the of the inventory sweep.

Risks
Assets not being inventoried on a periodic basis create the possibility of loss or inappropriate use.

Recommendation 5.1
TEBS should incorporate required action items in the Inventory Sweep Summary Sheet within a ServiceNow ticket. This will allow for the tracking and monitoring of the status of inventory updates identified during the inventory sweeps.

Recommendation 5.2
TEBS should design and implement alternative ways to perform asset inventory sweeps during a remote/teleworking environment.

Finding 6: Replacements

From the population of disposed assets (laptops, desktops, tablets, and workstations), SC&H identified a population of five of the 50 samples that had a disposal description of “FY21 Replacement.” SC&H selected two of the five disposal (replacement) samples to determine if the required documentation was appropriately completed prior to replacement.

For 1 of 2 disposed IT asset replacement samples during the in-scope period, standard installation form documentation was not available.

Risks

Assets replaced without standardized installation documentation result in inappropriately acquired and/or configured equipment based on the intention of the asset being used.

Recommendation 6.1
TEBS should formalize the process for replacement of IT assets to ensure the supporting documentation is available and retained for approval, acquisition, installation, and provisioning access for replaced devices, and consistent with the County's formal requirements for newly purchased devices**.**

Finding 7: Disposals (Servers)

The Office of Broadband Programs and Infrastructure Modernization utilizes a contracted third party for facilitation of the wiping, sanitization, and destruction of servers. These IT asset types include servers, hard drives, and other IT equipment (e.g., printers, monitors, TVs, digital cameras, etc.).

After destruction of the delivered IT assets/equipment, the contracted third party provides the Office of Broadband Programs and Infrastructure Modernization with an invoice, certificate of destruction, and report including the following information: Date, Item, Order #, Serial #, Method, Computer Type, Computer Make, Computer Serial #, Removed (Y/N), Specialist, Verification, and location.

SC&H obtained and reviewed a sample invoice, certificate of destruction, and corresponding report to evaluate the servers that were disposed of. However, the Office does not maintain a corresponding internal report of disposed servers/hard drives. Therefore, SC&H was not able to reconcile the individual IT assets/equipment destroyed against the IT assets/equipment delivered to the contracted third party.

Risks
1. Assets being disposed without proper rationale are inaccurately noted to be removed from the inventory.
2. Assets being disposed without being appropriately sanitized of data create the risk of sensitive data being retrievable from the device.

Recommendation 7.1
TEBS should implement a formal reconciliation process to verify that all units delivered to the contracted third party are documented as destroyed within the supporting documentation provided with the Certificate of Destruction.

Comments and MCIA Evaluation

We provided the Department of Technology and Enterprise Business Services (TEBS) with a draft of this report for review and comment. TEBS responded with comments on January 14, 2022. The TEBS response has been incorporated in the report at Appendix B. TEBS concurred with the findings of the audit and stated that they have taken steps already to make enhancements in their processes, consistent with the recommendations contained in the report; and will work to fully implement the report recommendations. No changes have been made in the report based on the responses.

Appendix A – Areas of Focus: Asset Management

Domain	Control #	Control Description
Governance	C1	Asset management policies and procedures are documented, reviewed, and updated on a periodic basis.
Acquisitions (Laptops)	C2	All laptop and desktop requests must be approved by an employee's supervisor prior to purchasing.
	C3	Make, model, serial number and PO# are recorded for new laptops within the DCM Configuration Management Database (CMDB) by DCM staff.
Acquisitions (Servers)	C4	All server requests must be approved by an employee's supervisor prior to purchasing.
	C5	Make, model, serial number and PO# are recorded once the new server is received.
Acquisitions (Mobile Devices)	C6	All new mobile device requests must be approved by an employee's supervisor prior to purchasing.
	C7	Key information for each mobile device (such as make, model, phone number, location) is recorded by the department supervisor in an internal tracking spreadsheet
Acquisitions (Hardware)	C8	All hardware (e.g. phones and radios) requests must be approved by the appropriate supervisor in accordance with policy prior to purchasing.
	C9	Key information for each piece of hardware (make, model, serial number and PO #) are recorded by the department supervisor.
Acquisitions (Software)	C10	All new software requests must be approved by the appropriate supervisor in accordance with policy prior to purchasing.
Acquisitions	C11	IT assets are procured through the use of appropriate procurement method.
	C12	Receipt of purchased IT asset is recorded.
Inventory Management	C13	IT assets are managed and maintained via asset inventory on a periodic basis. The inventory details include, but are not limited to, barcode, employee name, department, and asset location).
Awareness Training	N14	DCM performs on-site inventory sweeps (e.g. scan asset barcodes) to ensure inventory is complete and accurate.
	C15	Assets labeled as 'Missing' in Missing Assets Report are reviewed for accuracy. If no update on these assets is provided within 30 days, the assets will be removed from the inventory.
Replacements	C16	Prior to the initiation of a hardware replacement project, the following must be confirmed with the designated County Department office:

Domain	Control #	Control Description
		1. Review of hardware configuration 2. Review of current image configuration 3. Review of current onsite installation instructions 4. Once completed, the designated County official must sign-off on the image and install instruction, prior to scheduling the project.
Disposals	C17	DCM determines the lifecycle of system based on factors including: (1) age, (2) condition, (3) operating system, (4) input from the Office of Management and Budget (OMB). Only Full Seat hardware that meets the end-of-lifecycle conditions are eligible for replacement.
Disposals (Laptops)	C18	Laptop and desktop inventory are monitored to identify laptops that are available to be replaced and/or excessed. Once the decision has been made to excess or replace, DCM retains laptops for two weeks in case any data needs to be recovered from the drive. After two weeks, all storage devices are sanitized per Department of Defense (DoD) standards. All county labels are also removed from these assets at this time.
Disposals (Mobile Devices)	C20	Supervisors collect employee's old cell phone and stores it in case an employee needs a replacement phone outside of their phone upgrade window (1 year).
Disposals (Servers)	C21	DTS staff removes the server being replaced and stores it in in the basement storage. DTS retains servers for two months in case any data needs to be recovered. After two months, all storage devices are sanitized per Department of Defense (DoD) standards and asset labels are removed.
Disposals (Hardware)	C22	DTS removes and retains hardware for two weeks in case the old hardware is needed for any reason. After two weeks, if any hardware contains storage devices, they are sanitized per Department of Defense (DoD) standards and asset labels are removed.
Inventory Management – Physical Security	C23	Deskside (Telaforce) receive, unbox, and prepare assets for deployment at the DCM Warehouse and the Replacement Depot. The Warehouse and Replacement Depot have physical security controls, such as badge/keycard access, security cameras (inside and outside), alarm system, motion sensor lighting, and fire equipment.

Appendix B – Department Comments

DEPARTMENT OF TECHNOLOGY AND ENTERPRISE BUSINESS SOLUTIONS

Marc Elrich
County Executive

Gail M. Roper
Chief Information Officer/Director

MEMORANDUM

January 14, 2022

TO: **Bill Broglie, Internal Audit Manager**
Office of the County Executive

FROM: **Gail Roper, Director** *Gail M. Roper*
Department of Technology and Enterprise Business Solutions (TEBS)

SUBJECT: Formal Comments on Draft Report: Information Technology Audit – Asset Management – January 2022

Enclosed please find the Department of Technology and Enterprise Business Solutions formal response to the Information Technology Audit – Asset Management draft final report issued by Internal Audit.

If you or the audit firm working with you have any questions, please contact Ivan Galic or myself.

cc: Ivan Galic, Division Chief, One Face Forward Initiative, TEBS
Michelle Rinaldi, DCM Program Manager, TEBS
Alison Dollar, Chief Budget Officer, TEBS

101 Monroe Street • 13th Floor, Rockville • Maryland 20850 • 240-777-2900 • 240-777-2831 FAX

Starting in fiscal year 2022, TEBS received increased funding for additional device replacements and TEBS is on track to complete the highest number replacements in a single year on record. The Device Client Management (DCM) program within TEBS has supported the transition to telework during the pandemic, provided hundreds of loaner laptops, shifted to providing laptops as a default for device replacements, increased virtual support for users via the IT Help Desk and other methods of communication, and worked to resume thousands of device replacements during a continuing pandemic with new processes that no longer require an employee to return to their office.

The DCM program and TEBS staff are committed to always working to better serve our customers. With the change in our processes, TEBS recognizes the need to establish further controls and to continue adapting to the remote/telework environment, such as finding new ways to perform inventory sweeps.

TEBS concurs with the findings of the audit and will work to implement the following recommendations:

1. Develop policy and procedure documentation that defines the roles and responsibilities of the Telaforce Deskside team and physical security requirements at the DCM Warehouse and Replacement Depot.
2. Update and enforce formal policy requirements, including retaining equipment order forms, transferring of assets to the end user, and evidence of tagging and/or assignment of appropriate means of asset identification.
3. Develop and enforce completion of standardized IT purchase request forms.
4. Reinforce the DCM Policy Manual and the Purchase Card Policy with departments specific to the approved process to request and purchase IT assets.
5. Incorporate DCM action items resulting from IT asset inventory sweeps into a formal ServiceNow ticket for enhanced tracking and monitoring.
6. Design and implement alternative ways to perform asset inventory sweeps considering the current remote/telework environment.
7. Formalize the process for replacement of IT assets to ensure required documentation is available and retained for approval, acquisition, installation, and provisioning access.
8. Implement a formal reconciliation process to verify all disposed IT assets delivered to the contracted service provider are documented as destroyed within supporting documentation provided with the submitted Certificate of Destruction.

Since the period of the Audit TEBS and the Teleforce Deskside team have already begun to document a DCM Warehouse Security Policy as well as the roles and responsibilities of the Telaforce Deskside team. A draft of these documents are being reviewed and finalized.

In addition, during the period of the audit, improvements have been made to the use of ServiceNow as an asset management tool such as the use of ServiceNow to create automated workflows for asset validation every time a call is made to the IT Help Desk. Through ServiceNow, DCM is also working to digitize the inventory checklist forms which will allow for easily accessible asset tracking and asset records for all DCM replacements. DCM has also implemented an innovative PC replacement self-service application that gives employees the ability to self-schedule the pickup of their replacement devices which went live July of 2021.

Related to Finding 7: Disposal (Servers), this audit did not find that there was any improper disposal of server hard drives nor that there was any data still retrievable after disposal. All magnetic media such as hard drives disposed of by TEBS has been destroyed and all data on them was rendered unretrievable. TEBS receives a detailed report which includes serial number of magnetic media along with the Certificate of Destruction from the contracted service provider. However, TEBS will conduct a formal documented reconciliation process and retain supplemental documentation for the destruction and disposal of servers and magnetic media going forward.