Internal Audit Department
NeighborWorks® America

Audit Review of

IT Hardware Inventory Administration & Management

Project Number: NW.ITS.HARDWAREMGT.2019

Audit Review of IT Hardware Inventory Administration & Management

Table of Contents

February 6, 2020

To: NeighborWorks America Audit Committee

Subject: **Audit Review of IT Hardware Inventory Administration & Management**

Attached is our draft audit report for the **IT Hardware Inventory Administration & Management** review. Please contact me with any questions you might have.

Thank you.

Frederick Udochi
Chief Audit Executive

Attachment

cc: M. Rodriguez
S. Rice
R. Bond
R. Simmons

Function Responsibility and Internal Control Assessment
Audit Review of Hardware Inventory Administration & Management

Business Function Responsibility	Report Date	Period Covered
Information Technology & Services	February 6, 2020	October 1, 2018 to September 30, 2019
Assessment of Internal Control Structure		
Effectiveness and Efficiency of Operations		**Inadequate**[1]
Reliability of Financial Reporting		**Not Applicable**
Compliance with Applicable Laws and Regulations		**Not Applicable**

This report was reissued February 15, 2024 in accordance with a recommendation by the Government Accountability Office (GAO-23-105944, June 14, 2023).

[1] **Legend for Assessment of Internal Control Structure: 1. Generally Effective:** The level and quality of the process is satisfactory. Some areas still need improvement. **2. Inadequate:** Level and quality of the process is insufficient for the processes or functions examined and require improvement in several areas. **3. Significant Weakness:** Level and quality of internal controls for the processes and functions reviewed are very low. Significant internal control improvements need to be made.

Executive Summary of Observations, Recommendations and Management Responses

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
Observation 1 **Weak IT Hardware Inventory Administration and Management Practice** Internal Audit observed that the current IT&S Hardware Inventory Management Administration and Management to be weak in following aspects: A. Absence of Hardware Asset Management Process and Procedures; B. Lack of Annual Hardware Inventory Schedule C. Lack of Central Storage for Hardware Asset Data D. Lack of Integrity of Hardware Asset Data to form a Baseline Checkpoint. E. Failure to Track Old Laptops Returned from	**Yes**	Recommendation 1 Implementation of a formal IT Hardware Asset Management Practice Internal Audit strongly recommends that: A. IT&S formally assign the authority, responsibility and accountability of inventory administration and management. This formality should be adopted through the establishment of policies and standard operating procedures (SOP) across business units in custody of IT assets that would clarify and direct the inventory management process. This SOP should, at a minimum, include the following areas: specific	**Yes**	**A. IT&S recognizes the desirability to maintain a centralized hardware tracking inventory. IT&S will establish a policy for the management of in-scope assets.**	A 03/31/2021	Internal audit welcomes IT&S management's decision to adopt a Hardware Inventory policy which would amongst other issues include assets within and out of scope of the review with justification.

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
Staffers During Laptop Refresh. **Risk Rating**: [redacted]		data fields for the inventory, tagging and distribution, required environmental and access control (for instance, server rooms); maintenance of master data, disposals, write-offs and adjustments. It is also anticipated that this SOP is followed through with strict enforcement of this formal IT Hardware Asset Management Practice post implementation. With that being said, it is imminent that management takes immediate action to strengthen the current IT Hardware Asset Management practice as first step towards stronger and healthier cybersecurity for the corporation: o Immediate implementation of IT Hardware Asset Life				

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
		Cycle Management Business Process adhering to ITSM[2] best practice disciplines, to establish the following for starters: o Hardware Asset Administration and Management Guidelines to include performance requirements, hardware asset management team roles and responsibilities, asset naming conventions and vendor requirements. o Hardware Asset Identification Process and Procedures to set and maintain baseline and checkpoint.				

[2] IT Service Management (ITSM) refers to all the activities directed by policies, organized and structured in processes and supporting procedures performed by an organization in designing, planning, delivering, operating and controlling the lifecycle of information technology services offered to customer.

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
		○ Hardware Asset Controls to define the evaluation and approval process for hardware asset change requests, proposals as well as the annual hardware inventory schedule with key inventory activities and tasks. ○ Hardware Asset Status Accounting to record and report asset descriptions and all departures from the baseline in a consistent, uniformed format. ○ Hardware Asset Verification Process to assess compliance with established performance requirements. B. IT&S will provide Internal Audit with a				

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
		complete listing of hardware device, for record keeping purpose, in order to establish the baseline. We also expect IT&S to start scanning all hardware peripherals in accordance with newly developed SOP. C/D/E. Centralization of hardware asset data via implementing a Configuration Management Database (CMDB) using suitable IT asset management support tool for the integration between IT Asset Management procedures and IT Change Management procedures as well as Problem Management procedures to adhere to ITIL[3] ITSM best		**B. IT&S will focus on tracking devices with the capability of storing data (e.g. laptops, phones, servers) since they pose the greatest risk. IT&S will expand the assets tracked in its Asset Management system to include the laptops used for LIFT. IT&S does not manage the laptops, and NW does not own the laptops, used at NTIs. These devices will not be included in the Asset Management system. Additionally, IT&S will**	B 12/31/2021	Internal Audit accepts management's response.

[3] Information Technology Infrastructure Library (ITIL) is a globally recognized framework which includes a set of detailed best practices for IT Service Management (ITSM - see footnote 2)) that focus on aligning IT services with the needs of business. ITIL describes processes, procedures, tasks and checklists

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
		practice principles and guidelines.		**not track peripheral devices (monitors, keyboard, mice, docking station, etc. IT&S will also not track thumb drives, even though they can store data).**		Internal Audit accepts management's response.
				C. IT&S will store the in-scope devices information in the Asset Management system (CMDB). This system was implemented after the review period ended. It replaced a number of Excel spreadsheets that were previously being used.	C 12/31/2021	Internal Audit accepts management's response.
				D. IT&S will provide information in the Asset Mgmt system upon request to Internal Audit.	D 12/31/2021	Internal Audit accepts management's response
				E. IT&S did experience issues tracking and	E 12/31/2021	

which are not organization-specific nor technology-specific, but can be applied by an organization toward strategy, delivering value, and maintaining a minimum of competency.

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
				recovering old laptops after the rollout. IT&S has implemented tools to better track devices going forward. IT&S will review the Admin manual policy and update, if necessary, to ensure appropriate adherence to the HW Asset Mgmt policy.		

Risk Rating Legend

Risk Rating: High
A serious weakness which significantly impacts the Corporation from achieving its corporate objectives, financial results, statutory obligations or that may otherwise impair the Corporation's reputation.

Risk Rating: Moderate
A control weakness which could potentially undermine the effectiveness of the existing system of internal controls and/or operational efficiency, integrity of reporting and should therefore be addressed.

Risk Rating: Low
A weakness identified which does not seriously detract from the system of internal control and or operational effectiveness/efficiency, integrity of reporting but which should nonetheless be addressed by management.

Management Responses to The Audit Review of: Hardware Inventory Administration & Management		
# Of Responses	**Response**	**Recommendation #**
5	Agreement with the recommendation(s)	5
0	Disagreement with the recommendation(s)	0

Background

The last known physical IT Hardware Inventory was undertaken in 2015, there has been no other inventory activity since then, which resulted in the uncertainty of what hardware assets are present and their functions, thus cripples the effort in turning the asset data into actionable information to achieve more vigorous cyber security for the corporation.

Objective

The objective of this review was to obtain reasonable assurance that the corporation has documented process, procedures and internal controls for the administration and management of IT hardware asset inventory.

Scope

All company owned IT hardware of laptops and servers between 10/01/2018 and 09/30/2019 for the purpose of:

- Staff
- Non-staff
    - Temps
    - Consultants/Contractors
- NWA Laptop Refresh
- Loaners
- Storage
    - DC Office
    - Regional offices:
        - MWR (Midwest Region)
        - NOR (Northeast Region)
        - SOR (Southern Region)
        - WER (Western Region)
- Lost/stolen devices
- Donations
- Disposals
-

Methodology

Documents for Laptop Refresh tracking, Laptop Refresh Survey Results and master hardware inventory and individual hardware inventory tracking sheet in the category of appliance, router, laptop, network printer, print server, firewall, storage, switch, workstation, wireless controller and wireless access point were provided by IT Operations to Internal Audit.

Reviews and data analysis were subsequently performed to determine the hardware inventory administration and management is adequately adhered to IT Asset Management (ITAM) Hardware Asset Management (HAM) best practices[4]:

- Laptop Refresh:
  - Budget
  - Number of new laptops purchase (how many).
  - Number of new laptops deployed.
  - Number of old laptops retrieved from staff
  - Remaining balance of new laptops and location
  - Number of disposals.
  - Number of donations.
  - Reconcile differences.
- Overall health of IT hardware asset environment:
  - Tag ID to mark asset as corporate property
  - Physical location of the samples selected of DC office
  - Current lifecycle stage of asset in terms of obsolescence, version no longer supported, abandonment, trade-in for another asset, scrapped, etc. Network Connectivity Listing to identify existing HW equipment.
  - List of non-functional or non-network connected assets in the DC office and in the regional offices.
  - List of Roles and Responsibilities that support hardware inventory administration and management.
  - Comparison of scan review against known connected hardware at the beginning and the end of this audit review to compare results for discrepancies.
  - For DC office, 5 samples were picked to verify the following information to ensure they match the network listing:
    - Manufacture
    - Model
    - Serial #
    - Asset # (if used)
    - Physical location
    - Assigned user (if personal device)
    - Server name, if applicable
    - Purpose/function of the server
    - Server owner

Below are the observations and recommendations that resulted from the testing performed.

Observations and Recommendations

[4] 2017 ISACA Journal vol 3 IT Asset Valuation, Risk-Assessment and Control Implementation Model.pdf and ITIL 4 Foundations: IT Asset Management Process.

Observation 1 Weak Hardware Inventory Administration and Management Practice

Internal Audit observed that IT&S runs a weak Hardware Inventory Management Practice, which poses a significant threat to network systems availability and IT asset data integrity.

Specifically, there is no corporate policy and procedures defined in the Administrative Manual as guidance. Therefore, this audit review was based on the principles and guidelines provided by ITIL IT Asset Management (ITAM[5]) best practice processes. Under the circumstance, the correlation cannot be clearly established in a timely manner between configuration changes to enterprise systems, resources, networks and critical system outages. In other words, changing various components, such as desktop software, networks, middleware, system software for operating system and database, potentially introduces significant risk when system errors and deviations are not detected and corrected in timely manner due to lack of historical asset data. For example, during 2019 laptop refresh to upgrade from Windows 7 to Windows 10, TEAM users encountered numerous unpredictable system errors running TEAM in Windows 10. This resulted in the 18 TEAM users' reluctance to return the old laptop sustain the capacity as well as ability to provide continuous TEAM support without any disruptions.

This missing correlation leads to poor asset data integrity and poor information management for current and future decision making.

As a result, Internal Audit concluded the current IT&S hardware inventory administration and management practice to be weak in the following aspects:

1A – Absence of Hardware Asset Management Business Process

In order to have effective governance over a specific function, the existence of policies and procedures facilitate accountability over internal control responsibilities in the pursuit of Corporate objectives such as IT asset management. There was the absence of such policies and procedures that outline the authority, responsibility and frequency around inventory schedule, inventory activities, tasks supporting each activity, and resources identified to perform each inventory task, to track, manage and monitor hardware assets. A review of the Corporation's administrative manual found scant references to IT&S inventory management. As a result, IT&S was unable to provide a complete and comprehensive inventory of all hardware assets in the Corporation. Management relies on informal methods of communicating areas of responsibility in the Inventory management process instead of documented formal policies.

The effect of this absence of policies and procedures results in inconsistencies in practice, inefficiencies, and higher potential for inventory errors. This also potentially leads to insufficient information to support current and future procurement decision making.

1B: Lack of a Periodic Physical Inventory Schedule

[5] IT Asset Management (ITAM) is also referred to as Inventory Management. Assets include all elements of software and hardware that are found in the business environment. This audit review is based on the Hardware Asset Management standards and guidelines to build competent business practice to manage physical components of computers and computer networks, from acquisition to disposal. The key component is capturing the financial information about the hardware life cycle which aids the organization in making business decisions based on meaningful and measurable financial objectives.

It is best practice to conduct periodic physical inventory counts in order to reflect actual and accurate record keeping. This also helps in planning for obsolescence and eventual wear and tear of IT assets.

There has been no physical annual hardware inventory management in the subsequent fiscal periods to date since 2015. Currently, manual identification of hardware devices is performed by IT Operations staff members on as-needed basis both on site DC office and at regional offices, according to IT Operations. As a result, Internal Audit was unable to obtain a complete current master data file of hardware inventory in the Corporation. What was provided, in our estimation, was incomplete. Lacking the establishing of baseline master file inventory has not facilitated the use of the scanning tool to determine hardware peripheral devices on periodic basis.

1C: Lack of Central Repository for Hardware Asset Data

ITAM best practice calls for the implementation of a Configuration Management Data Base (CMDB)[6] to keep track of the state of IT assets, such as products, systems, software, facilities, people as they exist at specific points in time, and the relationship between all assets. A key component is capturing the financial information about the hardware life cycle which aids the corporation in making business decision based on meaningful and measurable financial objectives. At the time this review was conducted, hardware asset was tracked in separate spreadsheet by asset type, e.g. appliances, firewalls, laptops, wireless controllers, wireless access points, network printers, routers, servers, etc. We observed that the format of each tracking sheet is formatted inconsistently with different columns containing different data attributes (Appendix A). As a result, information collected cannot be integrated in order to obtain a universal profile of hardware asset data.

Lack of a centralized CMDB to track all relevant information for IT hardware assets presents challenges to verify and validate the completeness of hardware assets currently owned by the corporation, which potentially results in uncertainty of the accuracy of IT hardware asset data.

1D: Lack of Integrity of Hardware Asset Data to Establish Accurate Baseline Checkpoint

One of the IT internal controls File Integrity Monitoring (FIM)[7] is a process to be run periodically for the continuous monitoring of the aging of assets in order to plan for asset replacement in a proactive manner. Due to the fragmented hardware inventory tracking mentioned in 1C, this review had not been able to be performed since 2015 which compromises the integrity of the current and historical asset data that cannot be verified and confirmed in order to detect and to correct errors and deviations accordingly in a timely manner. The missing integration between IT Asset Management procedures and IT Change Management as well as Problem Management procedures may also dent the completeness and accuracy of hardware asset data.

[6] A Configuration Management Database (CMDB) is an ITIL database used by an organization to store information about hardware and software assets, commonly referred to as Configuration Items (CI), to provide a complete and accurate asset inventory. This database acts as asset data warehouse for the organization and also stores information regarding the relationship among its assets. The CMDB provides a means of recognizing the organization's critical assets and their relationship, such as information systems, upstream sources, dependencies of assets, and the downstream targets of assets.

[7] File Integrity Monitoring (FIM) – one of the security measures to monitor changes in system files by taking a snapshot of the system and then periodically compares that snapshot to the system's current state to detect sudden size changes caused by unauthorized intrusion to alert IT to minimize the threat in a timely manner.

1E: Failure to Track Old Laptops Returned by Staffers During Laptop Refresh

Internal Audit noticed that there was no tracking sheet for the information of old laptops returned by staffers during laptop refresh. Absence of these information fails to offer historical information in support of asset life cycle analysis and status reporting in terms of decommission, donation, disposal, theft and loss; it will have direct impact on future business decision making leading up to reduce total cost of ownership due to lack of baseline checkpoint.

Recommendation 1 Implementation of a formal IT Hardware Asset Management Practice

Internal Audit strongly recommends that:

1A. IT&S formally assign the authority, responsibility and accountability of inventory administration and management. This formality should be adopted through the establishment of policies and standard operating procedures (SOP) across business units in custody of IT assets that would clarify and direct the inventory management process. This SOP should, at a minimum, include the following areas: specific data fields for the inventory, tagging and distribution, required environmental and access control (for instance, server rooms); maintenance of master data, disposals, write-offs and adjustments. It is also anticipated that this SOP is followed through with strict enforcement of this formal IT Hardware Asset Management Practice post implementation.

With that being said, it is imminent that management takes immediate action to strengthen the current IT Hardware Asset Management practice as first step towards stronger and healthier cybersecurity for the corporation:

- Immediate implementation of IT Hardware Asset Life Cycle Management Business Process adhering to ITSM best practice disciplines, to establish the following for starters:
- Hardware Asset Administration and Management Guidelines to include performance requirements, hardware asset management team roles and responsibilities, asset naming conventions and vendor requirements.
- Hardware Asset Identification Process and Procedures to set and maintain baseline and checkpoint.
- Hardware Asset Controls to define the evaluation and approval process for hardware asset change requests, proposals as well as the annual hardware inventory schedule with key inventory activities and tasks.
- Hardware Asset Status Accounting to record and report asset descriptions and all departures from the baseline in a consistent, uniformed format.
- Hardware Asset Verification Process to assess compliance with established performance requirements.

1B. IT&S will provide Internal Audit with a complete listing of hardware device, for record keeping purpose, in order to establish the baseline. We also expect IT&S to start scanning all hardware peripherals in accordance with newly developed SOP.

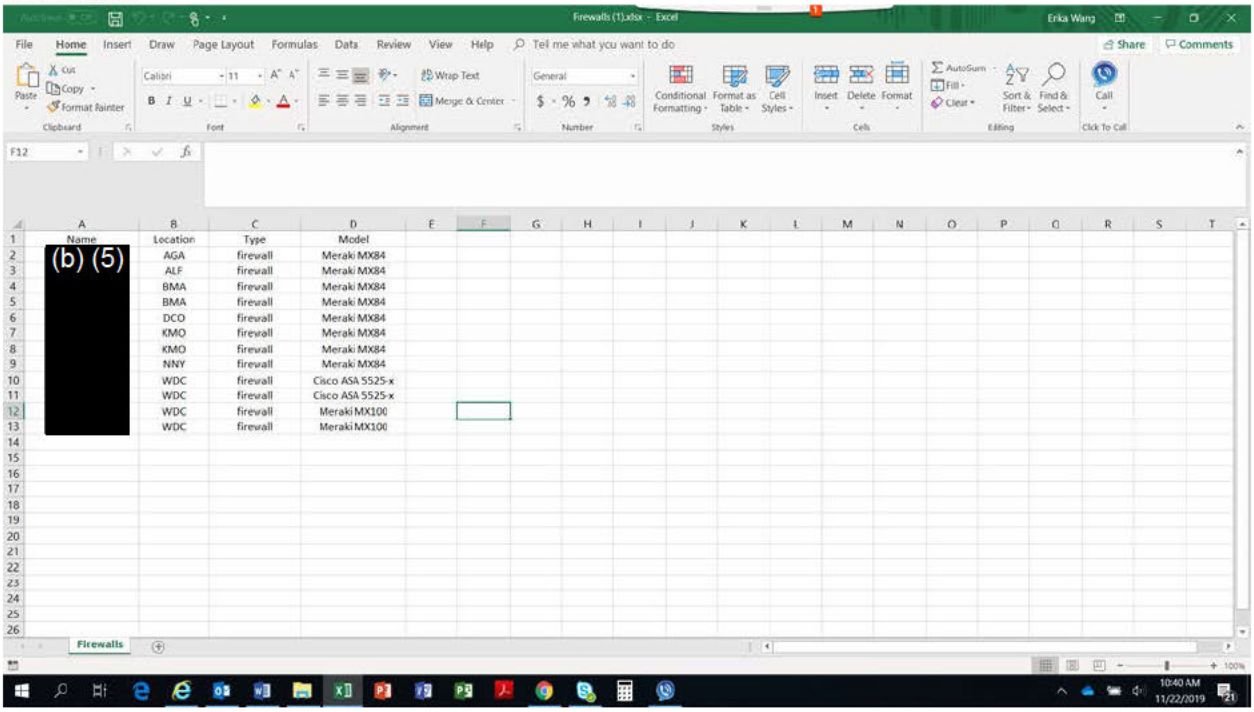
1C&1D. Centralization of hardware asset data via implementing a Configuration Management Database (CMDB) using suitable IT asset management support tool for the integration between IT Asset Management procedures and IT Change Management procedures as well as Problem Management procedures to adhere to ITIL ITSM best practice principles and guidelines.

Conclusion

To effectively administer, manage, utilize and secure IT hardware asset, the corporation must know the asset's location (Where) and function (What) first and foremost. Tagging the hardware asset by affixing a corporate Tag ID label to it does not answer the questions such as "What operating system are our laptops running?" and "Which devices are vulnerable to the latest threat?". In addition, the corporation also needs to tie existing data systems for physical assets, security systems and IT support into a comprehensive IT Asset Management System (ITAM) to further enable the corporation to dynamically apply business and security rules to better utilize information assets, as well as to protect enterprise systems and data to achieve effective tracking, monitoring and reporting on an information asset throughout its life cycle, thereby reducing the total cost of ownership by reducing the number on man-hours needed to perform tasks such as incident response and system patching. In essence, accurate hardware inventory is fast becoming a must-have first step in robust cybersecurity and asset management efforts, and therefore should be considered a top priority.

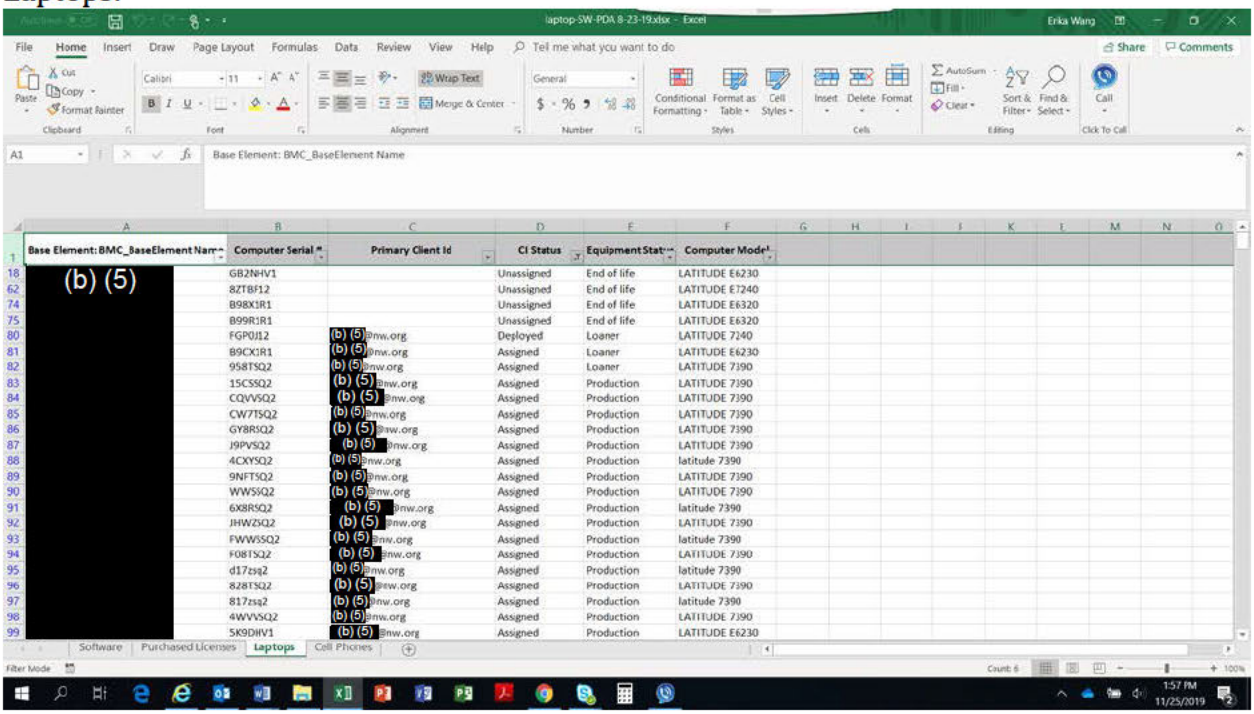
Appendix A Samples of Inventory Tracking Sheet with Different Data Attributes

Firewalls:



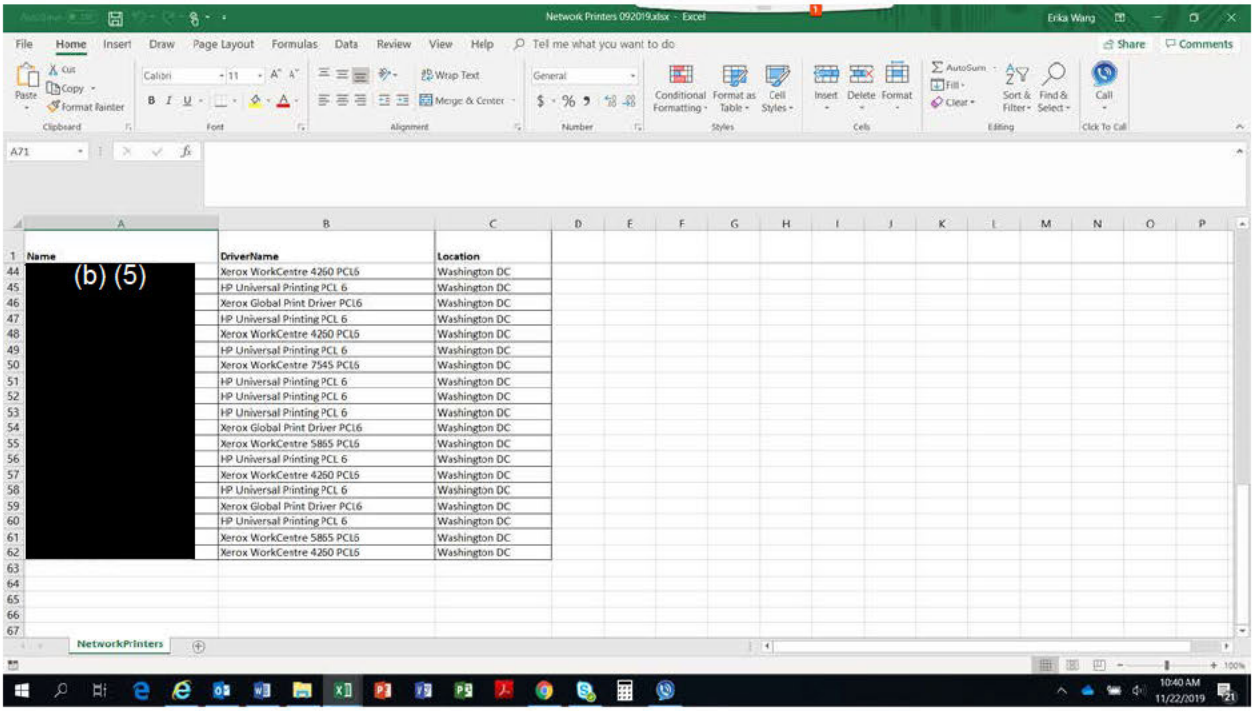
Name	Location	Type	Model
(b) (5)	AGA	firewall	Meraki MX84
	ALF	firewall	Meraki MX84
	BMA	firewall	Meraki MX84
	BMA	firewall	Meraki MX84
	DCO	firewall	Meraki MX84
	KMO	firewall	Meraki MX84
	KMO	firewall	Meraki MX84
	NNY	firewall	Meraki MX84
	WDC	firewall	Cisco ASA 5525-x
	WDC	firewall	Cisco ASA 5525-x
	WDC	firewall	Meraki MX100
	WDC	firewall	Meraki MX100

Laptops:



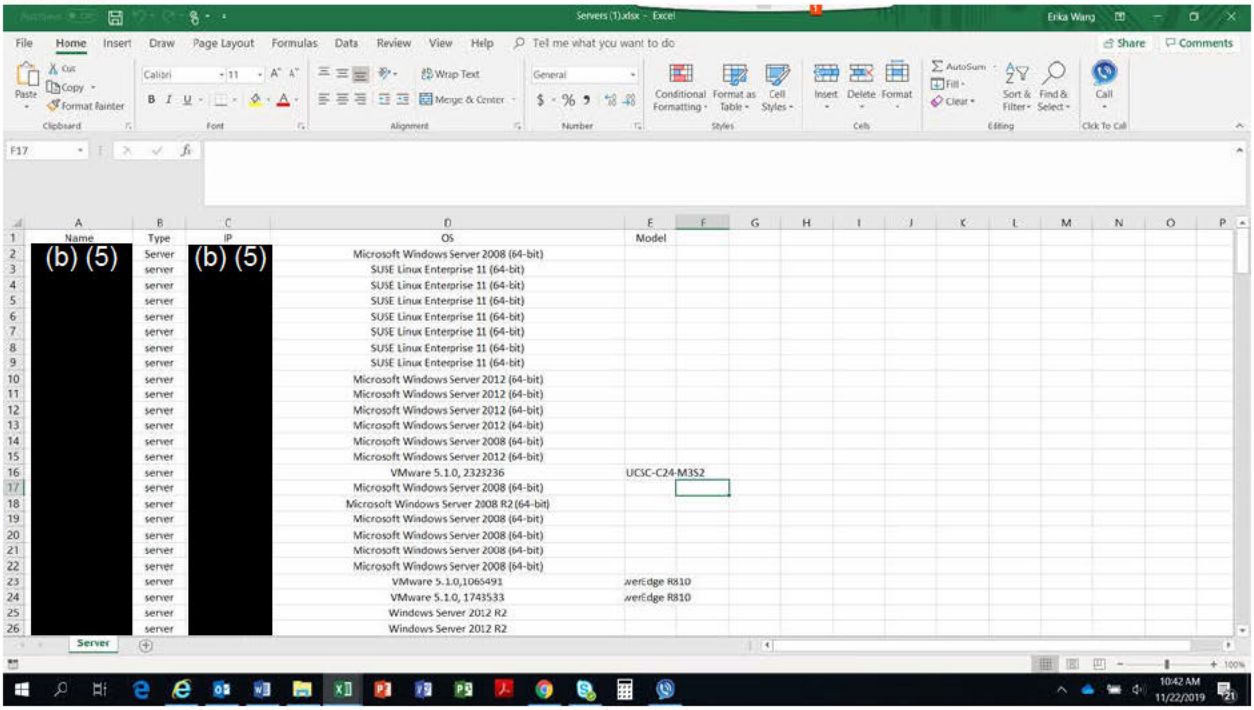
Base Element: BMC_BaseElement Name	Computer Serial #	Primary Client Id	CI Status	Equipment Status	Computer Model
(b) (5)	GB2NHV1		Unassigned	End of life	LATITUDE E6230
	8ZTBF12		Unassigned	End of life	LATITUDE E7240
	B98X1R1		Unassigned	End of life	LATITUDE E6320
	B99R1R1		Unassigned	End of life	LATITUDE E6320
	FGP0J12	(b) (5) @nw.org	Deployed	Loaner	LATITUDE 7240
	B9CX1R1	(b) (5) @nw.org	Assigned	Loaner	LATITUDE E6230
	958TSQ2	(b) (5) @nw.org	Assigned	Loaner	LATITUDE 7390
	15CS5Q2	(b) (5) @nw.org	Assigned	Production	LATITUDE 7390
	CQVV5Q2	(b) (5) @nw.org	Assigned	Production	LATITUDE 7390
	CW7T5Q2	(b) (5) @nw.org	Assigned	Production	LATITUDE 7390
	GY8R5Q2	(b) (5) @nw.org	Assigned	Production	LATITUDE 7390
	J9PV5Q2	(b) (5) @nw.org	Assigned	Production	LATITUDE 7390
	4CXY5Q2	(b) (5) @nw.org	Assigned	Production	latitude 7390
	9NFT5Q2	(b) (5) @nw.org	Assigned	Production	LATITUDE 7390
	WW55Q2	(b) (5) @nw.org	Assigned	Production	LATITUDE 7390
	6X8R5Q2	(b) (5) @nw.org	Assigned	Production	latitude 7390
	JHWZ5Q2	(b) (5) @nw.org	Assigned	Production	LATITUDE 7390
	FWW55Q2	(b) (5) @nw.org	Assigned	Production	latitude 7390
	F08TSQ2	(b) (5) @nw.org	Assigned	Production	LATITUDE 7390
	d17zsq2	(b) (5) @nw.org	Assigned	Production	latitude 7390
	828TSQ2	(b) (5) @ew.org	Assigned	Production	LATITUDE 7390
	817zsq2	(b) (5) @nw.org	Assigned	Production	latitude 7390
	4WVV5Q2	(b) (5) @nw.org	Assigned	Production	LATITUDE 7390
	5K9DHV1	(b) (5) @nw.org	Assigned	Production	LATITUDE E6230

Network Printers:



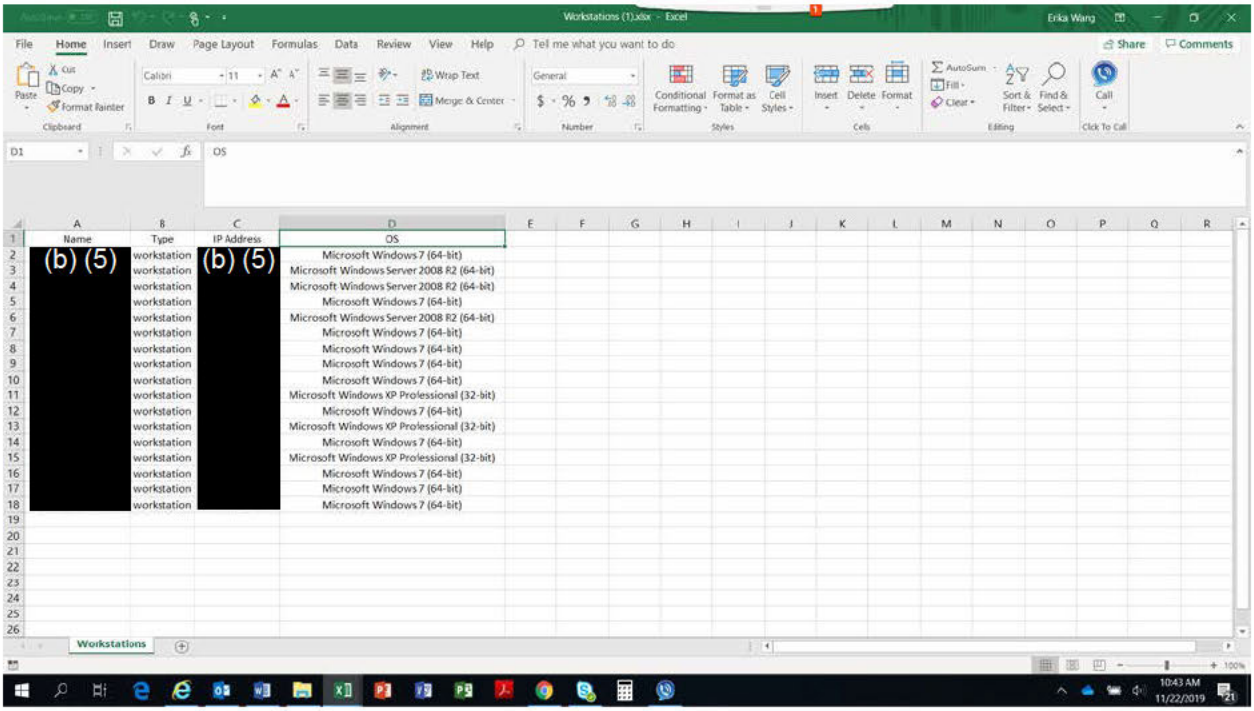
Name	DriverName	Location
(b) (5)	Xerox WorkCentre 4260 PCL6	Washington DC
	HP Universal Printing PCL 6	Washington DC
	Xerox Global Print Driver PCL6	Washington DC
	HP Universal Printing PCL 6	Washington DC
	Xerox WorkCentre 4260 PCL6	Washington DC
	HP Universal Printing PCL 6	Washington DC
	Xerox WorkCentre 7545 PCL6	Washington DC
	HP Universal Printing PCL 6	Washington DC
	HP Universal Printing PCL 6	Washington DC
	HP Universal Printing PCL 6	Washington DC
	Xerox Global Print Driver PCL6	Washington DC
	Xerox WorkCentre 5865 PCL6	Washington DC
	HP Universal Printing PCL 6	Washington DC
	Xerox WorkCentre 4260 PCL6	Washington DC
	HP Universal Printing PCL 6	Washington DC
	Xerox Global Print Driver PCL6	Washington DC
	HP Universal Printing PCL 6	Washington DC
	Xerox WorkCentre 5865 PCL6	Washington DC
	Xerox WorkCentre 4260 PCL6	Washington DC

Servers:



Name	Type	IP	OS	Model
(b) (5)	Server	(b) (5)	Microsoft Windows Server 2008 (64-bit)	
	server		SUSE Linux Enterprise 11 (64-bit)	
	server		SUSE Linux Enterprise 11 (64-bit)	
	server		SUSE Linux Enterprise 11 (64-bit)	
	server		SUSE Linux Enterprise 11 (64-bit)	
	server		SUSE Linux Enterprise 11 (64-bit)	
	server		SUSE Linux Enterprise 11 (64-bit)	
	server		SUSE Linux Enterprise 11 (64-bit)	
	server		Microsoft Windows Server 2012 (64-bit)	
	server		Microsoft Windows Server 2012 (64-bit)	
	server		Microsoft Windows Server 2012 (64-bit)	
	server		Microsoft Windows Server 2012 (64-bit)	
	server		Microsoft Windows Server 2008 (64-bit)	
	server		Microsoft Windows Server 2012 (64-bit)	
	server		VMware 5.1.0, 2323236	UCSC-C24-M3S2
	server		Microsoft Windows Server 2008 (64-bit)	
	server		Microsoft Windows Server 2008 R2 (64-bit)	
	server		Microsoft Windows Server 2008 (64-bit)	
	server		Microsoft Windows Server 2008 (64-bit)	
	server		Microsoft Windows Server 2008 (64-bit)	
	server		Microsoft Windows Server 2008 (64-bit)	
	server		VMware 5.1.0,1065491	werEdge R810
	server		VMware 5.1.0, 1743533	werEdge R810
	server		Windows Server 2012 R2	
	server		Windows Server 2012 R2	

Workstations:



Name	Type	IP Address	OS
(b) (5)	workstation	(b) (5)	Microsoft Windows 7 (64-bit)
	workstation		Microsoft Windows Server 2008 R2 (64-bit)
	workstation		Microsoft Windows Server 2008 R2 (64-bit)
	workstation		Microsoft Windows 7 (64-bit)
	workstation		Microsoft Windows Server 2008 R2 (64-bit)
	workstation		Microsoft Windows 7 (64-bit)
	workstation		Microsoft Windows 7 (64-bit)
	workstation		Microsoft Windows 7 (64-bit)
	workstation		Microsoft Windows 7 (64-bit)
	workstation		Microsoft Windows XP Professional (32-bit)
	workstation		Microsoft Windows 7 (64-bit)
	workstation		Microsoft Windows XP Professional (32-bit)
	workstation		Microsoft Windows 7 (64-bit)
	workstation		Microsoft Windows XP Professional (32-bit)
	workstation		Microsoft Windows 7 (64-bit)
	workstation		Microsoft Windows 7 (64-bit)
	workstation		Microsoft Windows 7 (64-bit)