UT Health San Antonio
Internal Audit & Consulting Services

Internal Audit & Consulting Services
7703 Floyd Curl Dr. MC#7974
San Antonio, Texas 78229-3900
210-567-2370 Fax: 210-567-2373
www.uthscsa.edu

Date: December 29, 2022

To: Ginny Gomez-Leon, VP & CFO
Yeman Collier, VP & CIO

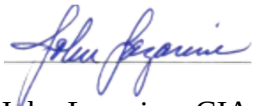
From: John Lazarine, Chief Audit Executive
Internal Audit & Consulting

Subject: Audit Report – Information Technology (IT) Asset Management

As part of our FY 2022 Audit Plan, we completed an audit of Information Technology (IT) Asset Management Audit. Attached is the report detailing the results of this review. Management's Action Plans are included in the report.

We appreciate the cooperation and assistance we received from Information Technology and Business Affairs throughout the review.

Respectfully,



John Lazarine, CIA, CISA, CRISC
Chief Audit Executive
Internal Audit & Consulting Services

Distribution:

cc: Dr. William Henrich, President
Andrea Marks, Sr. EVP & COO
J. Michael Peppers, Chief Audit Executive, UT System

External Audit Committee Members:
Randy Cain
Carol Severyn
Ed Garza

UT Health San Antonio
Internal Audit & Consulting Services

Audit Report (21-04)

Information Technology (IT) Asset Management

December 29, 2022

Executive Summary

Objective and Scope

We completed an audit of Information Technology (IT) Asset Management, as part of our approved audit plan. The objective of this audit was to determine whether adequate processes and controls are in place to safeguard IT assets in accordance with State and Institutional requirements and guidelines.

Controlled IT assets[1] are recorded in the Property Management Module of PeopleSoft. The controlled IT assets maintained within this module have been expensed and are actively maintained as required by the State of Texas Comptroller. Records of sensitive/protected data stored on controlled IT assets are maintained outside of PeopleSoft. The scope of this audit was primarily focused on controlled IT assets five years and older, to review the processes and controls relating to the management and security of the assets both from a record keeping and data security perspective. In addition, we reviewed the methods used to manage physical assets and its data to include tracking methodologies and actions taken on missing computing devices with sensitive/protected data.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and *Government Auditing Standards*.

Summary of Results

Overall, we determined processes and controls relating to the management of IT assets could be better integrated and improved to provide reasonable assurance that:

- computing devices that have sensitive/protected data are appropriately identified, updated, and tracked
- records of physical assets are complete, accurate, and adjusted timely
- validation processes of physical assets are standardized and consistent with state guidelines and/or requirements
- computing devices no longer in service are appropriately disposed of to reduce the risk of misappropriation of sensitive/protected data
- institutional policies and procedures regarding the management of IT assets, software, and data provide sufficient detail and reference state guidelines and/or requirements

Based on data retrieved from the Property Management system provided by Business Affairs, the Institution has approximately 9,045[2] computers that are listed as five years and older, of which we identified 301 that did not have any information on whether sensitive/protected data was stored on the asset.

---

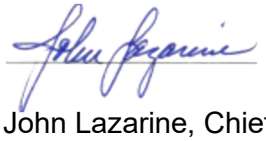
[1] Controlled assets are defined by the State of Texas Comptroller's Office as items valued between $499-$5,000 that are not capitalized.

2 Number of assets upon reviewing the data is 9,044, one asset identification number was duplicated.

The Institution has grown significantly within the past five years, and so has its use of computing devices. As a result, the use of resources such as the controlled IT asset inventory housed within the Property Management Module, is now used as a repository of information for other departments such as Information Technology for tracking IT assets that may have sensitive/protected data that if compromised could damage the brand and reputation of the Institution. IT has an initiative to reduce the number of aging computers across the Institution to safeguard data from loss and/or theft and to better serve the users with current technology maintenance and upgrades.

It is important to note that the Institution has experienced challenges in completing the physical inventory validation process and in obtaining information related to the type of data maintained on IT assets as it relies on department participation. Both Business Affairs and Information Technology are diligently working through these challenges collaboratively toward a solution and have been very responsive to suggested procedural changes to improve controls over the management of IT Assets.

Distribution
Dr. William Henrich, President Andrea Marks, Senior Executive Vice President, and Chief Operating Officer Yeman Collier, Vice President and Chief Information Officer Ginny Gomez-Leon, Vice President, and Chief Financial Officer Dr. Gerard Long, Associate Vice President, Business Affairs J. Michael Peppers, Chief Audit Executive, UT System
Auditors: Kimberly Weber, Audit Director, CIA, CFE, CRMA, CGAP, MPA Carol Salassa, Lead Auditor, CPA, CIA, CFE

Approved for Release	 John Lazarine, Chief Audit Executive, Internal Audit & Consulting Services

Summary of Results

Information Technology (IT) Asset Management

Observation/Condition	
A	Processes and Controls Relating to Inventory Management
	Overall, we determined the processes and controls relating to the management of controlled[3] IT assets needs improvement since the information is utilized and relied upon in several ways to include safeguarding of Institutional sensitive/protected data, compliance with applicable policies, rules, and regulations, and departmental record keeping of physical IT assets and software. Based on the work performed, inventory records regarding controlled IT assets were found to contain errors and missing information as it related to inventory and monitoring activities. From the controlled IT asset record list of 9,045[4] computing devices five years and older, we identified the following as it pertained to the data stored within PeopleSoft: ▪ one asset record was duplicated which assigned the same computer to two different departments (both listed the asset as missing) ▪ four asset records had custodians recorded that resigned between 2-3 years ago ▪ 7,071 records did not have a custodian assigned to them ▪ 1,019 records indicated that the assets had not been validated (scanned or electronically pinged) as of May 2022. ▪ 909 records indicated that the item may be missing (newly missing field), but the data fields that normally reflect a missing item were not completed or had conflicting information ▪ inventory records are not adjusted timely o two instances were noted where paperwork submitted to remove assets from inventory was delayed or lost o assets thought to be missing may remain on record for a three-year period as per Institutional policy, which could put the organization at risk should a computing device with sensitive/protected information be compromised, and is not compliant with state regulations/guidelines Inventory validation processes need improvement to better secure IT asset data and software in order to be compliant with applicable policies, rules, and regulations. Inventory validation may take up to year to complete, therefore creating an unintentional liability should an asset containing sensitive/protected information go missing. According to the State Comptroller's Office, controlled asset inventory validations should be conducted within a few months after the close of the current fiscal year.

[3] *The State Property Accounting System (SPA) define "Controlled Asset" to include IT devices that cost $500 to $4,999.99. The State of Texas policy allows management to determine if lower priced IT devices should be considered a "Controlled Asset" based on risk. Controlled Assets are to be tracked by the Institution but are not capitalized*

[4] *Audit's sample was 9,045 records in which one record was found to be a duplicate but had a different department assigned with the same date of entry into the system. The duplicate transaction is not included in data tables but is included in the sample number since this transaction is counted as an error/exception.*

Processes identified to validate inventoried IT assets include, scanning the physical asset, providing pictures, or scanning the picture of the asset tag, and/or pinging the asset. Some of the issues identified while reviewing this process include:

- sensitive equipment and intangible assets (i.e., software) are not maintained in Institutional records with an inventory number nor physically identified by their manufacturer's serial or license number
- methods for IT asset verification (i.e., ping reports, scanning tool, pictures, etc.) are not consistent with Institutional policies and procedures
- scanning devices are not adjusted when errors are noted, such as properly identifying the verifier or method of data collection (scan or manual input)
- condition of the asset and location are not appropriately validated

Upon discussions with State Comptroller's Office's staff, numerous inquiries have been made by other state agencies regarding alternate methods of validation and tracking of inventory based on the new post-COVID environment. The State Comptroller's Office is in the process of revising current guidelines that will allow for alternative validation processes such as pinging, as long as the process controls are documented in detail within the organizations policies and followed as prescribed.

However, the use of pinging as a stand-alone validation methodology will not be completely effective in safeguarding data since pinging only validates the IT asset has connected through VPN and/or the internet. It does not identify the user or the location of the asset. With the number of assets that are five years and older and that may not be in service, pinging alone is not sufficient in lowering the risk of items with sensitive/protected data that may become lost or stolen.

The figure depicted below is a summary of the records by department of the 9,044 IT assets reviewed that were five years and older. More detailed charts are listed in **Appendix A**.

Summary of Assets by Department and Testing Category
Based on Sample of 9,044

Dept	Department Name	Total IT Assets	Total Original Cost of IT Assets	Age Range by Year of Assets	Assets with Custodians Noted	Missing	Scanned Inv Tag	Ping Report	Not Verified
M1000	School of Medicine	5830	$ 7,565,152	1989-2017	1159	66	2785	2488	491
D1000	School of Dentistry	1133	$ 1,535,827	1991-2017	170	32	550	388	163
T5000	Chief Information Officer	471	$ 809,335	2001-2017	102	2	297	125	47
B5000	Chief Financial Officer	425	$ 523,074	2001-2017	141	1	193	85	146
I5000	Facilities, Planning, Operations	252	$ 407,039	2000-2017	37	3	100	144	5
A1000	School of Health Professions	322	$ 253,987	2002-2017	79	3	285	34	0
N1000	School of Nursing	210	$ 236,799	2007-2017	58	2	96	112	0
R1000	Research	99	$ 202,265	2005-2017	29	0	61	38	0
P5000	Officer of the President	68	$ 184,785	2011-2017	24	0	23	21	24
H1000	Academic, Fac & Student Affairs	91	$ 91,574	2012-2017	22	2	11	55	23
U5200	Marketing & Communication	42	$ 90,141	2008-2017	10	4	31	5	2
G1000	Graduate School	51	$ 79,732	1987-2017	23	0	31	13	7
U5000	Development	27	$ 25,630	2011-2017	14	0	16	11	0
V5000	Strategic Industry Ventures	16	$ 25,536	2008-2017	1	0	10	6	0
Other	(I5006), (B6000), (L5000), (P5510)	7	$ 580,746	2009-2017	5	1	3	2	1
	Total	**9044**	**$ 12,611,622**		**1874**	**116**	**4492**	**3527**	**909**
	Percentage of Total	**100%**			**21%**	**1%**	**50%**	**39%**	**10%**

The Texas Comptroller's Office requires institutions to ensure that property is tracked and secured in a manner that is most likely to prevent theft, loss, damage, or misuse. Agencies are required to know where all property under its control is stored (on-site or off-site) and be able to locate the inventory item upon request.

The process for procuring, securing, tracking, and disposing of IT assets is decentralized and involves multiple departments. Current policies and procedures lack guidance on the overall process and do not reflect proper authority and responsibility. The Institution's SharePoint (Intranet site) and Institutional Handbook of Operations (HOP) pertaining to property control are outdated (last updated 2010-2012) and lack information and references to pertinent state guidelines and/or requirements (i.e., State Comptroller's Office SPA Guidelines and Texas Government Code § 403.272. Responsibility for Property Accounting). Without proper policies and procedures, all impacted management and staff do not have clear expectations and/or guidance on how to appropriately safeguard the Institution's assets, specifically "controlled" IT assets, resulting in increased risks of financial loss, or more significantly, theft of sensitive/protected data. References to specific State regulations and guidelines, along with Institutional policies and procedures are listed in **Appendix B.**

It is important to note that the Institution has experienced challenges in which they are diligently working through. The pandemic has forced changes in business practices that are not currently reflected in state regulations. The Institution has undergone a high rate of turnover which may have played a role, resulting in reduced efficiencies and effectiveness regarding the management of controlled assets. Management continues to work through these challenges and has been very responsive to suggested procedural changes and has already begun the process of implementing some of those changes.

Recommendation:

To improve the controls and processes regarding managing IT assets, data, and software, leadership should create a cross-functional team that includes Business Affairs, Informational Technology, Compliance, and representatives of asset owners from across the organization to determine the appropriate controls needed to effectively maintain the record keeping and security of the Institutions IT assets and data. In addition, once the cross-functional team determines the appropriate actions to take, detailed policies and procedures should be documented and communicated that encompass the entirety of the asset management function as to avoid confusion, undue risk to the Institution, and non-compliance with pertinent rules and regulations.

Risk High

Management Response:

Action Plan:

Recent audits have identified the need to focus on safeguarding assets, especially IT assets that may store sensitive data. As such, the Property Control team will or has made the following enhancements to improve internal controls, reduce the risk of asset misappropriation, and centralize the process of procuring, securing, tracking, and disposing of IT assets.

The Property Control team has shortened the annual inventory process to three months spanning December to February whereby departments validate an updated controlled asset listing as of the commencement of the process. During the annual inventory training to department inventory contacts,

	*Property Control now highlights the importance of IT assets and reiterates the state requirements for all controlled assets. By **September 1, 2023**, Handbook of Operating Policy (HOP) 6.3.5 and all training guides will be modified to explicitly reference the applicable Texas Government Code, Sections 403.271-403, along with the institution's responsibilities codified in the State Property Accounting (SPA) System.* *By **September 1, 2023**, the Property Team will adopt Team Dynamix as the primary mechanism for departments to submit inventory changes. This will improve timeliness of updating asset records as well as provide metrics on response times and confirmation of the changes.* *Beginning in **January 2023**, the Property Control team will provide metrics to senior leadership using a Power BI dashboard. The dashboard will display the department's progress with the annual inventory. In addition, several missing fields, such as the custodian assignment, location, and mechanism used to validate the controlled asset, have been populated or will be updated by the department for all controlled assets and reside within the PeopleSoft Asset Module. By **May 2023**, the dashboard will also include filterable details on IT assets specifically identifying those that have aged greater than five years. This will enhance the transparency and accountability of responsible personnel for all controlled assets.* *The Property Control Office will implement a spot audit asset review process subsequent to the annual inventory with emphasis on IT assets. The spot audits will consist of a thorough review of the asset record to ensure completeness and accuracy with respect to documented location, custodian, etc.* *Finally, the Property Control team will continue to collaborate with IMS to develop policies and procedures that identify, document and safeguard IT assets that contain data with a targeted implementation date of **November 2023**, prior to the commencement of the next annual inventory process. Through the establishment of a Task Force team, IT and Property Control will partner to:* - *Review IT asset metrics quarterly* - *Improve control processes for newly procured and received IT equipment* - *Improve control processes for the disposal of IT equipment.* - *Evaluate and remedy finding from internal spot audit reviews* ***Owner:*** *Yvette Martinez, Director of Accounting* ***Implementation Date:*** *Various, as noted within the action plan (January 2023, May 2023, September 1, 2023, and November 2023).*
	Observation/Condition
B	Data Security of IT Assets Five Years and Older
	Through the course of our review, we evaluated a sample[5] of computing devices (desktop/PC, laptop, and iPad/Tablet) five years and older and determined controls regarding data security needed improvement. Although older computing devices may have outdated operating systems, these devices can still maintain sensitive/confidential data to include possibly proprietary information from the Institution's databases creating a significant unquantified security risk. According to records obtained from Property

[5] *Internal Audit requested a list of all IT Assets computers (desktop/PC and laptops) and iPads/Tablets and was provided a listing of items five years and older to use for sample testing. IA was unable to validate whether all records of IT Assets five years and older were received from the Property Management System within PeopleSoft.*

Management, the Institution has approximately 9,044 computers that are listed as five years and older. The oldest computer has an in-service date of 10/01/1986 (36 years old). A detailed summary of the computing devices reviewed from the sample selection is in ***Appendix A.***

During this review, we noted Information Technology (IT) has an initiative to reduce the number of aging computers across the Institution to safeguard data from loss and/or theft and to better serve the users with current technology maintenance and upgrades. While the monetary value of the assets can be quantified, the information on these devices is far more valuable with potentially significant repercussions should the data be compromised. Although, IT has already identified this issue and is working with the departments to reduce the number of unused computing devices, computer controls are decentralized to the departmental level and IT has no authority to enforce data security procedures.

Currently, departments are not required to surrender old/obsolete/stale computers when they receive new computing devices. According to IT management, a significant number of the older computers are not in use and could pose a security risk should the assets become lost or stolen. In addition, most, if not all of these computers will become inoperable due to Microsoft Windows 10 reaching its end-of-life in 2025 and requiring a Windows 11 platform upgrade. According to IT management, Windows 11 platform upgrade will require specific hardware and software upgrades making older computers useless without additional expense.

Also identified during this review was the collection and reporting of sensitive/protected data stored on computing devices. According to IT management, IT Risk Assessments are performed on all IT assets on an annual basis to determine whether sensitive data may be stored on computing devices. However, the responsibility to provide this critical information is solely on the individual departments to self-report and classify the data housed directly on its computers. The information is classified in one of eight data risk category types:

1. Health/PHI
2. Intellectual Property
3. Federally sponsored grant/contract/project
4. Research
5. Student /FERPA
6. Credit card
7. Other – (may have controlled data that is not necessarily sensitive but is not for public knowledge either)
8. None of the above – (no sensitive data)

Testwork[6] performed by Internal Audit regarding sensitive/protected data encompassed the eight data risk category types. Based on the sample of 9,044 assets, we identified 301 items that did not have any information on whether sensitive/protected data was stored on the asset. In addition, from our sample, 116 computing devices were identified as missing, of which 65 assets were noted to have sensitive/protected data and 31 asset records were noted as *"Unknown Data Status"*. The figure listed below depicts the missing data summary results and totals. More detailed charts are listed in ***Appendix A***.

[6] Data within the Table representing the testwork performed were consolidated as follows: items falling into categories listed in 1-6 and labeled it "Reported Data (Sensitive)", items falling under 7 listed above as "Reported Data (Other)", and 8 as "Reported Data (None)". All items that were not accounted for were labeled as "Unknown Data Status." All data referred as sensitive/protected is all assets falling into line items 1-8.

Table Representing the Number of Missing Assets and Related Data Identified by IA

Missing items identified from sample testing of 9,044 asset/records selected (all assets in sample recorded as 5+ years old)

Dept	Business Unit or School	Total Missing	Total Cost	Missing Custodian Name	Reported Data (Sensitive)	Reported Data (Other)	Reported Data (None)	Unknown Data Status
A1000	Health Professions School	3	$ 1,704.09	0	0	2	0	1
B5000	Chief Financial Officer	1	$ -	1	0	0	1	0
D1000	School of Dentistry	32	$ 47,089.12	29	13	13	0	6
H1000	Acad, Fac, & Stud Affairs	2	$ 2,446.39	2	0	0	0	2
I5000	Facilities, Planning & Operations	3	$ 2,872.93	2	0	0	0	3
M1000	School of Medicine	66	$ 85,917.75	49	35	0	14	17
N1000	School of Nursing	2	$ 1,338.00	1	0	0	1	1
T5000	Chief Information Officer	2	$ 1,207.60	2	2	0	0	0
U5200	Marketing & Communication	4	$ 6,326.70	3	0	0	3	1
C5000	Institutional Admin Function	1	$ 621.00	1	0	0	1	0
	Total	116	$ 149,523.58	90	50	15	20	31

Due to the increased number of cyber-attacks on healthcare organizations it is critical for the Institution to ensure data is appropriately secured. However, due to the decentralized processes for managing IT assets, increased coordination and clearly drafted policies and procedures are needed. Currently the large number of older, possibly unused, computers that may have unknown sensitive data on them could pose a significant security risk should they be lost or stolen.

Recommendations:

The CIO should consider requesting all Vice Presidents and Deans or their designee review a list of all IT Assets not currently in use as to the whether the items should be salvaged.

The CIO should ensure IT Risk Assessments for all pertinent assets are conducted on a periodic basis to ensure information is appropriately obtained and updated if sensitive information is saved on specific IT Assets.

Management should consider flagging IT assets with sensitive/protected data to ensure these items are physically verified during the annual inventory to ensure Institutional data is appropriately safeguarded.

Risk: High

Management Response:

Action Plan:

The Office of the CIO will complete IT Risk Assessments for all pertinent assets are conducted on a periodic basis to ensure information is appropriately obtained and updated if sensitive information is saved on specific IT Assets.

Owner:

Yeman Collier, Vice President & Chief Information Officer

Implementation Date:

	Completed

	Summary of Risk Ratings	
	The UT System Internal Audit finding classification system includes Priority, High, Medium, or Low classifications.	
	Priority	An issue identified by an internal audit that, if not addressed on a timely basis, could directly impact the achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.
	High	A finding identified by an internal audit that is considered to have a medium to high probability of adverse effects to a UT institution or UT System as a whole.
	Medium	A finding identified by an internal audit that is considered to have a low to medium probability of adverse effects to a UT institution or UT System as a whole.
	Low	A finding identified by an internal audit that is considered to have minimal probability of adverse effects to a UT institution or UT System as a whole.
	n/a	No reportable findings or observations were identified during the course of the audit.

APPENDIX A

Tables listed within this Appendix reflect the detailed data that was summarized within the body of the report.

Note: All data within the tables reflect a sample size of 9,044 which omits 1 duplicate transaction that was noted as an error but included in the overall audit sample testing selection of 9,045 noted in the body of the report. The duplicate transaction was purposely omitted from the data depicted in the following tables.

Summary of Assets by Department and Testing Category
Based on Sample of 9,044

Dept	Department Name	Total IT Assets	Total Original Cost of IT Assets	Age Range by Year of Assets	Assets with Custodians Noted	Missing	Scanned Inv Tag	Ping Report	Not Verified
M1000	School of Medicine	5830	$ 7,565,152	1989-2017	1159	66	2785	2488	491
D1000	School of Dentistry	1133	$ 1,535,827	1991-2017	170	32	550	388	163
T5000	Chief Information Officer	471	$ 809,335	2001-2017	102	2	297	125	47
B5000	Chief Financial Officer	425	$ 523,074	2001-2017	141	1	193	85	146
I5000	Facilities, Planning, Operations	252	$ 407,039	2000-2017	37	3	100	144	5
A1000	School of Health Professions	322	$ 253,987	2002-2017	79	3	285	34	0
N1000	School of Nursing	210	$ 236,799	2007-2017	58	2	96	112	0
R1000	Research	99	$ 202,265	2005-2017	29	0	61	38	0
P5000	Officer of the President	68	$ 184,785	2011-2017	24	0	23	21	24
H1000	Academic, Fac & Student Affairs	91	$ 91,574	2012-2017	22	2	11	55	23
U5200	Marketing & Communication	42	$ 90,141	2008-2017	10	4	31	5	2
G1000	Graduate School	51	$ 79,732	1987-2017	23	0	31	13	7
U5000	Development	27	$ 25,630	2011-2017	14	0	16	11	0
V5000	Strategic Industry Ventures	16	$ 25,536	2008-2017	1	0	10	6	0
Other	(I5006), (B6000), (L5000), (P5510)	7	$ 580,746	2009-2017	5	1	3	2	1
	Total	**9044**	**$ 12,611,622**		**1874**	**116**	**4492**	**3527**	**909**
	Percentage of Total	**100%**			**21%**	**1%**	**50%**	**39%**	**10%**

Summary of IT Controlled Asset Testing

Responsible Business Unit		Inventory Record Results			Data Security Results		
Dept	Department Name	Total IT Assets Sampled	Inv. Not Verified	Assets with NO Custodian	Sensitive Data	Other Data	Unknown Data
M1000	School of Medicine	5830	557	4671	**4593**	360	**101**
D1000	School of Dentistry	1133	195	963	**881**	124	**55**
T5000	Chief Information Officer	471	49	369	**147**	5	**31**
B5000	Chief Financial Officer	425	147	284	**201**	29	**82**
I5000	Facilities, Planning, Operations	252	8	215	**0**	104	**11**
A1000	School of Health Professions	322	3	243	**25**	259	**0**
N1000	School of Nursing	210	2	152	**38**	5	**6**
R1000	Research	99	0	70	**27**	0	**0**
P5000	Officer of the President	68	24	44	**24**	0	**4**
H1000	Academic, Fac & Student Affairs	91	25	69	**52**	1	**5**
U5200	Marketing & Communication	42	6	32	**1**	0	**1**
G1000	Graduate School	51	7	28	**24**	0	**5**
U5000	Development	27	0	13	**0**	0	**0**
V5000	Strategic Industry Ventures	16	0	15	**0**	0	**0**
Other	(I5006), (B6000), (L5000), (P5510)	7	2	2	**4**	0	**0**
	Total	**9044**	**1025**	**7170**	**6017**	**887**	**301**
	Percentage of Total	**100%**	**11%**	**79%**	**67%**	**10%**	**3%**

APPENDIX A (Cont.)

Summary of Assets by School
Based on Sample of 9,044

Dept	Schools	Type of Asset	Quantity	Total Cost	Date Range	Missing	Scanned Inv Tag	Ping Report	Not Verified
M1000	School of Medicine	Laptops	1310	2,136,135.17	1994-2017	32	831	273	174
		Desktops	4140	5,056,302.80	1989-2017	22	1662	2196	260
		IPAD/Tablet	367	264,200.24	2010-2017	12	283	17	55
		Other	13	108,513.32	1995-2016	0	9	2	2
			5830	**$ 7,565,151.53**		**66**	**2785**	**2488**	**491**
D1000	School of Dentistry	Laptops	259	469,808.93	1993-2017	21	155	36	47
		Desktops	793	1,013,173.95	1991-2017	8	341	352	92
		IPAD/Tablet	80	49,566.75	2010-2017	3	53	0	24
		Other	1	3,277.50	2016	0	1	0	0
			1133	**$ 1,535,827.13**		**32**	**550**	**388**	**163**
A1000	Health Professions School	Laptops	52	76,086.42	2009-2017	2	35	15	0
		Desktops	54	79,856.85	2002-2017	0	35	19	0
		IPAD/Tablet	214	91,734.00	2011-2017	1	213	0	0
		Other	2	6,310.00	2016	0	2	0	0
			322	**$ 253,987.27**		**3**	**285**	**34**	**0**
N1000	School of Nursing	Laptops	55	77,062.91	2008-2017	0	40	15	0
		Desktops	120	135,639.59	2007-2017	0	24	96	0
		IPAD/Tablet	35	24,096.40	2011-2017	2	32	1	0
			210	**$ 236,798.90**		**2**	**96**	**112**	**0**
G1000	Graduate School	Laptops *	20	39,122.01	2003-2017	0	16	2	2
		Desktops	24	36,391.35	1987-2017	0	12	11	1
		IPAD/Tablet	7	4,218.70	2011-2017	0	3	0	4
			51	**$ 79,732.06**		**0**	**31**	**13**	**7**

** Laptop listed as scanned and assigned to an employee to use off-campus - employee is no longer with the Institution for a period over 24 months*

APPENDIX A (Cont.)

Summary of Business Unit
Based on Sample of 9,044

Dept	Business Units	Type of Asset	Quantity	Total Cost	Date Range	Missing	Scanned Inv Tag	Ping Report	Not Verified
T5000	Chief Information Officer	Laptops	210	281,242.00	2010-2017	1	155	30	24
		Desktops	218	407,289.70	2001-2017	1	107	93	17
		IPAD/Tablet	35	25,530.47	2011-2017		29	2	4
		Other	8	95,272.42	2012-2014		6	0	2
			471	**$ 809,334.59**		**2**	**297**	**125**	**47**
B5000	Chief Financial Officer	Laptops	137	200,226.01	2004-2017	1	57	20	59
		Desktops *	231	267,811.45	2001-2017	0	114	63	54
		IPAD/Tablet	57	55,036.75	2011-2017	0	22	2	33
			425	**$ 523,074.21**		**2**	**193**	**85**	**146**
I5000	Facilities, Planning & Operations	Laptops	41	70,217.32	2002-2017	1	21	19	0
		Desktops	168	230,382.70	2000-2017	1	42	121	4
		IPAD/Tablet	30	19,891.98	2012-2017	1	25	3	1
		Other	13	86,546.61	2000-2015		12	1	0
			252	**$ 407,038.61**		**3**	**100**	**144**	**5**
R1000	Research	Laptops	30	49,710.87	2009-2017	0	24	6	0
		Desktops	57	76,373.97	2005-2017	0	26	31	0
		IPAD/Tablet	11	11,173.50	2013-2017	0	10	1	0
		Other	1	65,007.13	2013		1	0	0
			99	**$ 202,265.47**		**0**	**61**	**38**	**0**
P5000	Office of the President	Laptops	22	30,067.64	2011-2017	0	11	7	4
		Desktops	29	33,898.01	2013-2017	0	9	13	7
		IPAD/Tablet *	15	13,223.19	2011-2017	0	3	1	11
		Other	2	107,596.21	2013-2014	0	0	0	2
			68	**$ 184,785.05**		**0**	**23**	**21**	**24**
H1000	Acad, Fac, & Stud Affairs	Laptops	26	32,893.29	2012-2017	2	4	11	9
		Desktops	60	54,750.57	2012-2017	0	3	43	14
		IPAD/Tablet	5	3,930.00	2016	0	4	1	0
			91	**$ 91,573.86**		**2**	**11**	**55**	**23**
U5200	Marketing & Communication	Laptops	11	13,643.89	2012-2017	3	7	1	0
		Desktops	24	73,084.36	2008-2017	1	19	4	0
		IPAD/Tablet	7	3,413.00	2013-2016	0	5	0	2
			42	**$ 90,141.25**		**4**	**31**	**5**	**2**
U5000	Development	Laptops	5	6,996.29	2013-2017	0	3	2	0
		Desktops	11	12,219.95	2015-2016	0	2	9	0
		IPAD/Tablet	11	6,414.00	2011-2016	0	11	0	0
			27	**$ 25,630.24**		**0**	**16**	**11**	**0**
V5000	Strategic Industry Ventures	Laptops	2	2,019.00	2015-2016	0	2	0	0
		Desktops	13	22,588.22	2008-2017	0	7	6	0
		IPAD/Tablet	1	929.00	2012	0	1	0	0
			16	**$ 25,536.22**		**0**	**10**	**6**	**0**
Other	I5006 - AHEC	Computer	1	621.00	2009	1	0	0	0
	B6000 - Human Resources	Laptops	4	$ 578,110.96	2014-2017	0	3	1	0
	L5000 - Office for Governmental Relations	Desktop/PC	1	1005.44	2017	0	0	1	0
	P5510-Office of Strategic Planning	Laptops	1	1008.25	2016	0	0	0	1
			7	**$ 580,745.65**		**1**	**3**	**2**	**1**

** Laptop/IPAD listed as not-scanned and assigned to an employee from P5100 but listed in P5000/B5000 - employee resigned over 36 months*

APPENDIX A (Cont.)

Table Representing the Number of Missing Assets and Related Data Identified by IA

Missing items identified from sample testing of 9,044 asset/records selected (all assets in sample recorded as 5+ years old)

Dept	Business Unit or School	Dept Code	Type of Asset	Total Missing	Total Cost	Missing Custodian Name	Reported Data (Sensitive)	Reported Data (Other)	Reported Data (None)	Unknown Data Status
A1000	Health Professions School	A1200	Laptops	2	1,325.09	2		1		1
		A1200	IPAD/Tablet	1	379.00	0		1		
				3	$ 1,704.09	0	0	2	0	1
B5000	Chief Financial Officer	B5451	Laptops	1	-	1			1	
				1	$ -	1	0	0	1	0
D1000	School of Dentistry	D1800	Laptops	1	1,099.00	1				1
		D5100	Laptops	20	36,266.08	18	9	9	0	2
		D2100	Desktops/PC	2	1,233.10	2				2
		D5100	Desktops/PC	6	6,353.94	5	3	2		1
		D5100	IPAD/Tablet	3	2,137.00	3	1	2		
				32	$ 47,089.12	29	13	13	0	6
H1000	Acad, Fac, & Stud Affairs	H1000	Laptops	1	1,418.71	1				1
		T6100	Laptops	1	1,027.68	1				1
				2	$ 2,446.39	2	0	0	0	2
I5000	Facilities, Planning & Operations	B5630	Laptops	1	1,543.93	1				1
		I5000	Desktops/PC	1	650.00	1				1
		B5800	IPAD/Tablet	1	679.00	0				1
				3	$ 2,872.93	2	0	0	0	3
M1000	School of Medicine	G1200	Laptops	3	3,875.00	3	3			
		M1300	Laptops	2	3,135.16	2				2
		M1504	Laptops	1	2,407.00	0	1			
		M1505	Laptops	1	1,606.80	1				1
		M1510	Laptops	1	1,611.82	1			1	
		M1514	Laptops	3	3,541.28	1	3			
		M1522	Laptops	3	5,595.00	2	3			
		M1600	Laptops	1	2,837.99	0	1			
		M1800	Laptops	3	2,715.00	3			1	2
		M2502	Laptops	1	1,319.48	0				1
		M3106	Laptops	3	2,893.44	3	3			
		M3134	Laptops	1	1,057.75	1	1			
		M4602	Laptops	6	12,907.00	6			6	
		M4870	Laptops	1	1,133.28	0	1			
		M4900	Laptops	2	1,803.60	2				2
		G1200	Desktops/PC	1	1,800.00	0				1
		G1300	Desktops/PC	1	1,113.28	0	1			
		G1600	Desktops/PC	1	1,699.00	1	1			
		M1503	Desktops/PC	1	1,189.20	1	1			
		M1514	Desktops/PC	1	2,897.00	1	1			
		M1517	Desktops/PC	1	399.99	1	1			
		M1522	Desktops/PC	2	1,574.53	2	2			
		M2300	Desktops/PC	3	4,955.22	3	3			
		M2502	Desktops/PC	2	2,570.10	2				2
		M3106	Desktops/PC	3	1,936.98	3	3			
		M3193	Desktops/PC	1	2,662.78	1	1			
		M4602	Desktops/PC	3	5,975.39	3			3	
		M4900	Desktops/PC	2	1,372.28	2			1	1
		M1011	IPAD/Tablet	1	329.00	1				1
		M1024	IPAD/Tablet	1	579.00	0				1
		M1100	IPAD/Tablet	1	829.00	0	1			
		M1300	IPAD/Tablet	1	499.00	0				1
		M1519	IPAD/Tablet	1	829.00	0				1
		M1700	IPAD/Tablet	1	709.00	1	1			
		M2300	IPAD/Tablet	2	1,018.00	1	2			
		M2400	IPAD/Tablet	1	829.00	0			1	
		M2502	IPAD/Tablet	1	829.00	0				1
		M2513	IPAD/Tablet	1	483.40	0	1			
		M4602	IPAD/Tablet	1	399.00	1			1	
				66	$ 85,917.75	49	35	0	14	17
N1000	School of Nursing	N1300	IPAD/Tablet	2	1,338.00	1			1	1
				2	$ 1,338.00	1	0	0	1	1
T5000	Chief Information Officer	T6700	Laptops	1	500.00	1	1			
		T6700	Desktops/PC	1	707.60	1	1			
				2	$ 1,207.60	2	2	0	0	0
U5200	Marketing & Communication	U5200	Laptops	3	3,290.70	2			3	
		U5200	Desktops/PC	1	3,036.00	1				1
				4	$ 6,326.70	3	0	0	3	1
C5000	Institutional Admin Function	I5006 - AHEC	Computer	1	621.00	1			1	
				1	$ 621.00	1	0	0	1	0
Total				116	$ 149,523.58	90	50	15	20	31

APPENDIX B

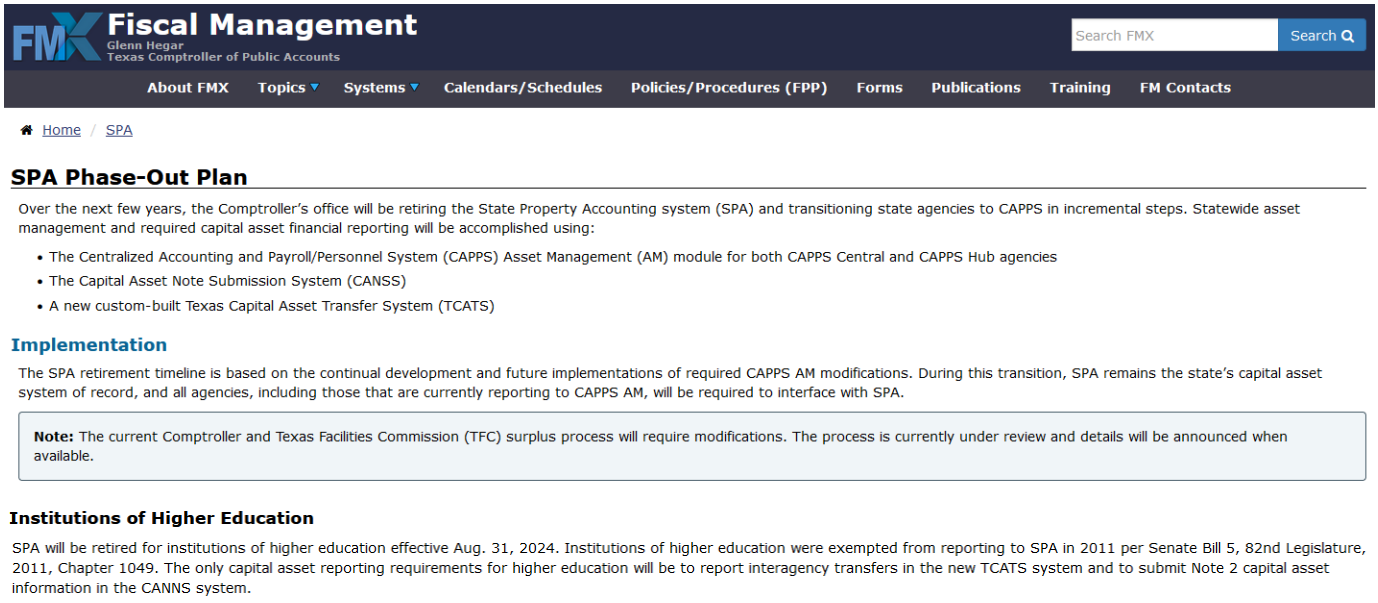
Texas Government Code § 403.272

Responsibility for Property Accounting, all personal property owned by the state shall be accounted for by the agency that possesses the property. In accordance with State Comptroller's policy, the responsibility for the custody and care of state agency property lies with the agency head. Each agency head must designate a property manager and the agency head should ensure that the agency maintains adequate internal control procedures. The agency head must ensure that the procedures for accountability and safeguarding of the agency's property are distributed. All agency procedures must comply with Comptroller's office rules and requirements. Informal procedures for the department are deferred to SPA guidelines, which as per Government Code, Chapter 403, Subchapter L, Section 403.2715, institutions of higher education (institutions) are exempt from reporting to the State Property Accounting System but must still comply with Comptroller state property accounting policies and procedures.

Texas Comptroller's Office- State Property Accounting (SPA) Process User's Guide – Chapter 2

Policies adopted by the Comptroller's Office. Although Institutions of higher education are exempt from populating their assets in the SPA database, an agency's responsibility for reporting and maintaining capital asset information is specified in Chapter 2 of the SPA Users Guide which contains policies adopted by the Comptroller's office to ensure consistency in the reporting of capital assets by state agencies.

The State Comptroller's Office has also posted information regarding a SPA Phase-Out Plan. Information from the State's website is depicted below:



FMX Fiscal Management
Glenn Hegar
Texas Comptroller of Public Accounts

Search FMX | Search

About FMX | Topics | Systems | Calendars/Schedules | Policies/Procedures (FPP) | Forms | Publications | Training | FM Contacts

Home / SPA

SPA Phase-Out Plan

Over the next few years, the Comptroller's office will be retiring the State Property Accounting system (SPA) and transitioning state agencies to CAPPS in incremental steps. Statewide asset management and required capital asset financial reporting will be accomplished using:

- The Centralized Accounting and Payroll/Personnel System (CAPPS) Asset Management (AM) module for both CAPPS Central and CAPPS Hub agencies
- The Capital Asset Note Submission System (CANSS)
- A new custom-built Texas Capital Asset Transfer System (TCATS)

Implementation

The SPA retirement timeline is based on the continual development and future implementations of required CAPPS AM modifications. During this transition, SPA remains the state's capital asset system of record, and all agencies, including those that are currently reporting to CAPPS AM, will be required to interface with SPA.

Note: The current Comptroller and Texas Facilities Commission (TFC) surplus process will require modifications. The process is currently under review and details will be announced when available.

Institutions of Higher Education

SPA will be retired for institutions of higher education effective Aug. 31, 2024. Institutions of higher education were exempted from reporting to SPA in 2011 per Senate Bill 5, 82nd Legislature, 2011, Chapter 1049. The only capital asset reporting requirements for higher education will be to report interagency transfers in the new TCATS system and to submit Note 2 capital asset information in the CANNS system.

https://fmx.cpa.texas.gov/fmx/spa/phaseout.php

Texas Administrative Code 202, Security Controls Standards Catalog, MEDIA SANITIZATION

State agencies shall keep a record/form (electronic or hard copy) documenting the removal and completion of the process with the following information:

- *date.*
- *description of the item(s) and serial number(s);*
- *inventory number(s);*
- *the process and sanitization tools used to remove the data or method of destruction; and*
- *the name and address of the organization the equipment was transferred to.*

Institutional Property Control General Policy 6.3.1

Policies and Procedures – The president of the Health Science Center has appointed the director of the Office of Accounting as property manager. The director has assigned the responsibility for Health Science Center property and for an annual physical inventory of this property to department chairs and administrative heads. The property manager sets the time, as directed by the state Materials Management Commission, and provides the procedures for conducting the annual property inventory. Department chairs and administrative heads are responsible for ensuring that disposal of Health Science Center equipment is accomplished in accordance with the appropriate procedure established within Section 6.3 of the Handbook of Operating Procedures for Property Control.

Institutional Policy 5.8.21 Data Classification

Data classification is necessary to identify critical data that is essential for business operations. Security control measures are established and maintained based on data criticality and associated vulnerabilities. Refer to policy for details regarding Classification Standards for various types of data

Institutional Policy 5.8.22 Data Protection

The UT Health San Antonio Policies, Standards and Procedures must describe and require steps to protect University data using appropriate administrative, physical, and technical controls in accordance with the Information Security Program, Handbook of Operating Policy (HOP) 5.8.21 (Data Classification), UT System Policy 165 (Information Resources Use and Security), and its associated Standards, and any federal or state law and regulation that may apply to the data's classification.