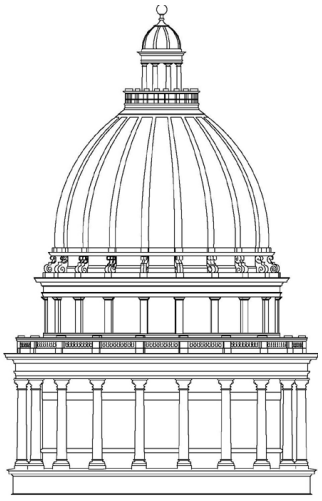
REPORT TO THE

UTAH LEGISLATURE

Number 2018-05



A Performance Audit of Inventory and Security Controls at Institutions of Higher Education

July 2018

Office of the
LEGISLATIVE AUDITOR GENERAL
State of Utah

STATE OF UTAH

Office of the Legislative Auditor General

315 HOUSE BUILDING • PO BOX 145315 • SALT LAKE CITY, UT 84114-5315
(801) 538-1033 • FAX (801) 538-1063

JOHN M. SCHAFF, CIA
AUDITOR GENERAL

July 2018

TO: THE UTAH STATE LEGISLATURE

Transmitted herewith is our report, **A Performance Audit of Inventory and Security Controls at Institutions of Higher Education** (Report #2018-05). A digest is found on the blue pages located at the front of the report. The objectives and scope of the audit are explained in the Introduction.

We will be happy to meet with appropriate legislative committees, individual legislators, and other state officials to discuss any item contained in the report in order to facilitate the implementation of the recommendations.

Sincerely,

John M. Schaff, CIA
Auditor General

JMS/lm

Digest of
A Performance Audit of Inventory and Security Controls at Institutions of Higher Education

In November 2016, the Office of the Legislative Auditor General released *A Performance Audit of the University of Utah Athletics Department*, a report that included recommendations for stronger management of inventory control and building access. After this report was released, the Legislature requested further audit work at Utah System of Higher Education (USHE) institutions to determine whether institutions' policies were "…adequately designed to safeguard assets." The request also asked us to "…determine if buildings are adequately secured and controlled."

Chapter II
Most Institutions Lack Noncapital Inventory Controls

Noncapital Assets Are Not Tracked. Seven of the eight institutions have not consistently tagged and tracked noncapital assets, which is concerning, given that they purchased at least $27 million in noncapital assets in fiscal year 2017 alone. Each institution's policy attempts to safeguard noncapital assets differently; over half rely on departments to track assets, two do not require controls over noncapital asset inventories, and one has no inventory policies governing either capital or noncapital assets. Because there are very few standardized requirements at institutions or from the Regents, there is little accountability for noncapital assets.

Institutions Are Not Monitoring Noncapital Asset Policy Compliance. Because there is little institutional oversight, departments in charge of noncapital asset inventories are frequently out of compliance with their own policy. We found 86 percent of reviewed departments to be noncompliant with policy or to be lacking policy requirements. Of the eight institutions, only two list policy consequences that hold departments accountable for noncompliance. Best practices used at some institutions to increase inventory compliance include standardized inventory methods, access to common inventory tracking tools, and designated noncapital asset liaisons.

Vague Institutional Policies Do Not Provide Sufficient Guidance. Three institutions had outdated policies that have not been revised or approved for more than ten years. Additionally, policies do not clearly define the type of inventory that should be tracked, leaving institutional policy requirements open to interpretation. Outdated and vague policies have contributed to varying inventory practices within each institution and high rates of noncompliance.

Chapter III
Auditors Easily Gained Unauthorized Access to a Significant Number of Institution Facilities

Audit Staff Accessed Institutional Facilities After Nightly Lockup Procedures. Audit staff successfully entered 31 facilities during our after-hours tests of building security. Auditors were able to access facilities at each institution. The ease with which auditors entered buildings is concerning, given that exterior entrances are the first line of defense in protecting assets in the building. These tests were conducted between 12 a.m. and 5 a.m. after the nightly lockup of buildings and did not involve forceful entry.

Unlocked Interior Rooms Leave Assets Vulnerable and Show Lack of Security Awareness. Over 150 unsecured rooms allowed access to many valuable and critical assets during auditor's after-hours security tests. The prevalence of unsecured rooms demonstrates the need for personnel security training. While exterior doors should be secure, our access to assets was completely based on whether interior rooms were locked. Locking interior doors is vital for the security of assets. Burglary reports from these institutions suggest that criminal access could have been gained using the same vulnerabilities that auditors found during the security tests.

Security Training and Policies Would Better Protect Institution Property. Valuable assets left vulnerable because of unlocked interior rooms and unlatched exterior doors reflect inadequate security awareness from institution personnel. Institutional security training on existing policies is lacking despite professional guidelines recommending staff be trained in security practices. Security training is especially important for institution personnel who work after building operating hours. Additionally, policies requiring regular maintenance of exterior doors are important for building security.

Institutions Should Base Security Decisions on Assessed Risks. Most institutions' public safety personnel do not formally assess and document potential security risks to all their facilities. As a result, public safety personnel may be reactionary rather than proactive in preventing building security risks. Guidelines suggest that risk assessments should be used to guide security decisions. We recommend these guidelines be followed and security measures be established and required of facilities based on risk assessments.

Chapter IV
Security at Institutions Is Compromised By Poor Access Management

Many Master Keys Have Been Lost or Are Unaccounted For. Data from the institutions show that many master keys are issued with questionable controls. This has led

to many master keys being lost or unaccounted for, and for physical security to be compromised. Access control, including mechanical keys and locks or electronic access, is the primary form of physical security at most institutions. The controlled distribution of keys is critical to maintaining institutional security.

Rekeying Buildings Is Rare Despite Many Lost Master Keys. Despite guidelines recommending locks be rekeyed once keys have been lost, the majority of institutions have not rekeyed despite the loss of master keys. We are concerned that the security of buildings and rooms may be compromised. Additionally, rekeying decisions should be based primarily and methodically on the security risk that the lost key imposes. Because both the costs to rekey or install electronic access are high, mechanical key distribution should be limited.

Institutions Need to Better Track and Collect Keys. Most institutions are not conducting regular key inventories. Institutions need up-to-date, accurate information on access that has been granted through mechanical or electronic key distribution. Key inventories and audits provide this necessary information. Additionally, keys should be collected from employees when their employment no longer requires that access.

Chapter V
Institutions Generally Lack IT Inventory Controls, But Closely Monitor Data Security

Most Institutions Do Not Adequately Inventory IT Assets. Five of the eight institutions do not perform an annual inventory of information technology (IT) assets. These items are some of the most frequently pilfered assets; about half of the 115 loss claims recently submitted by institutions are for IT assets. It is concerning that these items are not more closely tracked. Some institutions compensate for the lack of a physical inventory by conducting a digital asset inventory.

Institutions Closely Monitor Data Security. Institutions have been continually vigilant in their efforts to secure sensitive data. Because institutions generally do not physically inventory IT equipment, securing the data that IT equipment accesses is doubly important. Utah institutions are making efforts to secure their data using national standards and have created a group to do biennial security and penetration tests to detect weaknesses.

REPORT TO THE
UTAH LEGISLATURE

Report No. 2018-05

A Performance Audit of Inventory and Security Controls at Institutions of Higher Education

July 2018

Audit Performed By:

Audit Manager	Brian Dean, CIA, CFE
Audit Supervisor	Leah Blevins, CIA
Audit Staff	Nicole Luscher
	Matthew Taylor

Table of Contents

Chapter I
Introduction

In November 2016, the Office of the Legislative Auditor General released *A Performance Audit of the University of Utah Athletics Department*, a report that included recommendations for stronger management of inventory control and building access. After this report was released, the Legislature requested further audit work at Utah System of Higher Education (USHE) institutions to determine whether institutions' policies were "…adequately designed to safeguard assets." The request also asked us to "…determine if buildings are adequately secured and controlled."

Institutions Do Not Adequately Control Noncapital Assets

Capital assets are more tightly controlled, while noncapital assets are subject to more flexibility.

Capital assets are those purchased for $5,000 or more, while noncapital assets cost less than $5,000. After our initial review, we decided to focus primarily on noncapital assets in the inventory control portion of this audit.[1] This decision was made for two reasons. First, the University of Utah Athletics audit, which focused on noncapital assets, was the basis for this audit request. Second, our initial review of three institutions of higher education found little concern with capital asset policies. Capital assets were, in general, tightly controlled by institutional policy, while noncapital assets were frequently subject to more flexibility in asset tracking and inventory.

To prevent data loss, institutions should control and secure data that can be accessed through IT assets.

Our review of inventory controls led to the conclusion that, while controlling physical information technology (IT) assets (such as computers, iPads, and tablets) is important, it is more important to control and secure data accessed through those assets. A loss of data can be significantly costlier than the loss of a computer. Because there were weaknesses in institutions' inventory controls over IT assets, our scope was broadened to include a review of data security measures.

[1] The physical access and security sections of this audit report (Chapters III and IV) discuss both capital and noncapital assets.

Building Access Is Inconsistently Controlled

Our review of building access and security includes both hard keys and electronic key cards.

The Legislature also requested that this audit look at the related issue of physical access to campus buildings. In response, we reviewed the security of buildings after-hours, the number of keys issued, and the incidence of lost keys and corresponding rekeying. Our review of building access included both hard keys and electronic key cards.

Audit Scope and Objectives

This audit reviewed all eight institutions overseen by USHE, namely Dixie State University, Salt Lake Community College, Snow College, Southern Utah University, the University of Utah, Utah State University, Utah Valley University, and Weber State University. Because of the broad nature of this audit, this report is intended to primarily provide best practices to the institutions. This intent does not preclude the report from pointing out necessary improvements or current defects in practices.

We would also like to note that because of the broad nature of this audit, concerns expressed about a specific institution (in both inventory and building security) may or may not be unique to that institution. Other institutions should review their own policies, processes, and procedures to determine whether weaknesses exist and, if so, take the necessary steps to remedy the weaknesses. The objective of this audit was to determine:

Concerns expressed about specific institutions may or may not be unique to that institution.

- Do institutions appropriately track and inventory noncapital assets?
- Are institutional asset inventory policies adequately designed to safeguard assets?
- Is access to campus buildings adequately controlled through security practices?
- Are institutions adequately controlling access to their buildings through key and electronic access control policy?
- Do institutions follow data-security best practices to compensate for potentially lost or stolen IT assets?

Chapter II
Most Institutions Lack Noncapital Inventory Controls

Utah institutions of higher education purchased at least $27 million in noncapital assets[2] in fiscal year 2017, much of which is unlikely to have been tagged and tracked. Institutional property should bear a physical asset tag that can be used to track (inventory) the asset. Several institutions' policies delegate noncapital asset inventory responsibilities to departments, but do not then monitor whether departments track these assets. Eighty-six percent of reviewed departments were found to be noncompliant with existing policies or absent of policy requirements. The Utah State Board of Regents (Regents) should create policy to address the system-wide lack of noncapital inventory controls. Outdated and ambiguous policies lack accountability measures to hold departments responsible. Vague and unclear policies have contributed to inventory practices that are difficult to control.

Noncapital Assets Are Not Tracked

Institutions of higher education purchased at least $27 million in noncapital assets in fiscal year 2017.

Seven of the eight institutions have not consistently tagged and tracked noncapital assets, which is concerning given that they purchased at least $27 million in noncapital assets in fiscal year 2017 alone. Each institution's policy attempts to safeguard noncapital assets differently; over half rely on departments to track assets, two do not require controls over noncapital asset inventories, and one has no inventory policies governing either capital or noncapital assets. Because there are very few standardized requirements at institutions or from the Regents, there is little accountability for noncapital assets.

[2] The Utah State Board of Regents has set the capitalization limit at $5,000 for equipment purchases. An individual equipment purchase under the $5,000 threshold is considered a noncapital asset.

Millions of Dollars of Noncapital Assets Are Not Tagged or Tracked

Seven of eight institutions have not consistently tagged and tracked noncapital assets.

Seven of the eight institutions are not consistently tagging or inventorying noncapital assets, exposing millions of dollars of property to the risk of loss or theft. This is especially concerning as many noncapital assets are highly pilferable. Figure 2.1 provides institutional estimates of noncapital asset purchases.

Figure 2.1 Noncapital Asset Purchases Totaled More Than $27 Million for Fiscal Year 2017. Institutions report noncapital asset expenditure totals between $582,400 and $9,952,700 for fiscal year 2017.

Institution	Noncapital Asset Purchases (FY 2017)
Dixie State University (DSU)	$617,000
Salt Lake Community College (SLCC)	4,150,300
Snow College (Snow)	Unknown
Southern Utah University (SUU)	582,400
University of Utah (U of U)	9,952,700
Utah State University (USU)	5,615,000
Utah Valley University (UVU)	5,818,200
Weber State University (WSU)	1,153,600
Total	**$27,889,200**

Source: Auditor analysis of institutional data

The accounting structure at Snow College does not capture noncapital asset expenditure totals.

As shown, the total estimated value of noncapital asset expenditures in fiscal year 2017 was more than $27 million. These totals are based on broad and conservative estimates but represent millions of dollars in assets that may have not been properly tracked. Currently, the accounting structures at Snow and UVU do not have accounts specifically designated for noncapital asset purchases; however, staff at UVU could provide itemized noncapital asset purchase data[3]. Rather than reporting a "best guess" estimate for Snow, their noncapital asset expenditure totals remains "unknown." It is concerning that Snow is

[3] Although UVU does not have account codes specifically designated for noncapital asset purchases, staff applied filters and parameters to campus-wide purchase order data to provide a noncapital asset expenditure total for fiscal year 2017.

not able to accurately account for the total number or the total value of noncapital assets.

The numbers in Figure 2.1 do not represent all noncapital assets purchased by each institution.[4] Apart from WSU, institutions either do not require noncapital asset inventories or do not know whether departments have conducted the required inventories. This lack of oversight increases the risk of losing valuable assets, including the $27 million in asset purchases represented in Figure 2.1. To better protect state property, institutions should ensure that all assets are appropriately tagged and accounted for.

Increased inventory controls over noncapital assets could assist institutions in discovering missing or stolen assets and in identifying patterns for highly pilferable assets. During calendar years 2013 to 2017, 7 institutions submitted 115 claims of burglary and theft totaling $477,038 to the Utah Division of Risk Management. Almost half the claims included computer assets such as laptops. Remaining claims included heavy equipment, flatbed trailers, cameras, digital video recorders, iPads, tablets, and projectors.

Over the last five years, the Utah Division of Risk Management has received 115 claims of burglary and theft from institutions of higher education, totaling $477,038.

The Utah Division of Risk Management requires important claim information such as the "Date of Loss" for claim submission. Institutions that are not regularly tracking assets may not have the claim information required to submit an insurance claim, which could result in unrecoverable losses. As an example, a recent U of U internal audit found costumes in the theater department valued at $2.6 million that did not have the necessary supporting insurance documentation. Although the costumes were not reported as missing, the audit advises the institution to maintain records of its noncapital assets with documentation to support asset valuation for insurance purposes if anything were to be lost or stolen.

Institutions that are not regularly tracking assets may not have the claim information required to submit an insurance claim, which could result in unrecoverable losses.

Moreover, we observed untagged assets at institutions such as projectors, desktops, laptops, microscopes, TVs, a tablet, and a mobile monitor. Without proper inventory controls in place, assets may be

[4] Institutional totals in Figure 2.1 are conservative estimates based on select noncapital asset account codes. Because departments typically determine what constitutes a noncapital asset, selected account codes do not reflect all noncapital asset purchases. In addition, data was not itemized and noncapital assets purchased with purchasing cards are not included in the data.

lost or stolen without institutions knowing about it. Figure 2.2 shows some untagged assets observed during auditor walkthroughs.

Figure 2.2 Most Institutions Are Not Tagging All Valuable Assets. We observed assets such as microscopes, projectors, desktops, and laptops without asset tags.

Source: Auditor observation from January – April 2018

The assets shown in this figure and discussed throughout this report are both valuable and easily pilferable.

Institutional Inventory Tracking Controls Vary

Varying inventory controls have resulted in a lack of accountability and oversight.

The lack of standardized inventory practices and controls among institutions has resulted in varying levels of accountability. WSU is the only institution that tracks noncapital assets centrally. Four other institutions' policies require departments to track noncapital assets; however, these institutions lack the oversight and accountability to ensure those policies are followed. The absence of these inventory controls raises concerns. Figure 2.3 outlines institutional noncapital inventory structures and inventory practices.

Figure 2.3 Institutional Noncapital Inventory Policy Structures Vary. Inventory controls listed in policies vary from central asset tracking to no requirements for tracking noncapital assets.

	Require Tracking	Tracked Centrally	Require Central Oversight
DSU	No	No[1]	No
SLCC	Yes	No[1]	No
Snow[2]	No	No	No
SUU	Yes	No	No
U of U	Yes	No	No
USU[3]	No	No	No
UVU	Yes	No	No
WSU	Yes	Yes	N/A

Source: Auditor analysis of institutional policies April 2018
[1] *DSU and SLCC have a policy to centrally audit noncapital computer assets only.*
[2] *Snow does not have inventory policies, however, informal procedures to track capital assets are in place.*
[3] *USU's noncapital asset inventory policy is elective and is not counted as policy since it is not required.*

As Figure 2.3 shows, three institutions do not require noncapital asset inventory tracking. Snow does not have formal policies governing either capital or noncapital asset inventories.

Three institutions do not require noncapital asset tracking.

Although Snow conducts an annual inventory of capital assets, nowhere is that process codified in policy or written procedure, and none is conducted of noncapital assets. In September 2017, a proposed noncapital asset policy was presented to Snow's College Council.[5] The proposed policy was met with resistance from the council, and the policy creators were asked to revise the policy to one "…that finds a better balance between accountability and practicality." Snow's policy creation process was put on hold pending the results of this audit.

Snow does not have formal policies governing either capital or noncapital asset inventories.

A lack of administrative oversight and accountability has resulted in diverging inventory practices, both within and among institutions. To provide guidance and consistency, the Regents should issue a policy specifying requirements for noncapital asset tracking procedures. Regent policy does not currently mention noncapital assets with the exception of IT equipment. Any policy issued should include thresholds for tracking and requirements for ensuring the responsibilities in these procedures are clearly accounted for. The

The GAO advises that inventory accountability should exist at all levels of an organization.

[5] The College Council is a governing body that reviews and approves policies that are then sent to the Board of Trustees. It consists of faculty, staff, and administrative members of Snow's community.

Government Accountability Office (GAO) states that "[inventory] accountability within an organization should exist from the top of the organization to the lowest level." Establishing a method of oversight and a robust reporting system increases accountability levels, ensures that inventories are conducted on a regular basis, and verifies that inventory performance goals are being met.

Noncapital asset inventory tracking is a state-wide concern.

The Regents have the duty and authority to provide this guidance. ***Utah Code*** states that "…the board [of Regents] shall control, manage, and supervise the institutions of higher education…" Statute further requires the Regents to "enhance the impact and efficiency of the system."[6] According to Regents staff, the policies issued by the Regents are intended to be more broadly based, focused on bigger issues. However, Regents staff also believe that the exception to a broad policy approach is when an issue has been identified as a state-wide concern. Because this audit identifies noncapital asset tracking as a state-wide concern, we recommend the Regents review and create a policy providing guidance for all institutions of higher education.

In 2009, our office released a manual entitled *Best Practices for Good Management.* One of those best practices includes implementing good policy and procedures. The manual advises entities to "develop procedures to guide your staff in the implementation and day-to-day decision making relevant to your program's goals and objectives." The guidance continues by stating:

> Perhaps the most important advice that comes out of our performance audit experience is that program policies:
>
> - Need to be in writing
> - Need to be distributed and readily available to all interested parties
> - Need to be kept current through regular review and updating, and
> - Above all, need to be adhered to.

Without formal policies, institutions cannot ensure the consistency of the inventory process.

[6] ***Utah Code*** 53B-1-103(1)(a) & (3)(b)

Lack of Inventory Tracking Leads to Increased Risk

Assets that are not properly tagged or consistently tracked are difficult to control and may result in increased institutional costs. Currently, no statewide policies requiring institutions to track noncapital assets exist; however, there are some relevant guidelines shown in Figure 2.4.

Figure 2.4 State Guidelines Identify Best Practices for Noncapital Asset Inventories. Inventories should be conducted or reasons for not conducting inventories should be documented.

Governing Body	Guideline Language
USHE[7]	"Institutions shall maintain an inventory of all internal or third-party IT Resources that store, process or transmit Personally Identifiable Information."
Division of Finance[8]	"Agencies are encouraged to track information-only asset items such as cameras, radios, firearms, electronic equipment, data processing equipment, **and anything that may be considered pilferable."** [Emphasis added]
Division of Finance[9]	A questionnaire sent to state agencies asks "Are pilferable (information-only) assets, including non-capitalized assets under $5,000 (cameras, laptops, printers, smart phones, etc.) tracked, maintained, and inventoried in accordance with Finance Policy…? …If applicable, **please explain** in the "Comments" column **why your agency has chosen not to track certain types of pilferable assets."** [Emphasis added]

Source: Auditor analysis of state policies and guidelines November 2017 – April 2018

Though institutions are not subject to state agency requirements, the guidelines in Figure 2.4 demonstrate the importance of maintaining records and safeguarding purchases made with tax dollars.

Maintaining inventory accuracy rates allows institutions to identify weaknesses and risk areas.

Institutions use inventory methods to track capital assets that could be used to track noncapital assets. For example, SLCC maintains a three-year trend analysis of capital assets that allows the college to determine weaknesses and risk areas. The trend analysis can pinpoint asset custodians who frequently lose a higher than average number of assets and alert administrators to custodians who may need additional training or removal. USU determines the effectiveness of its capital

[7] USHE: R345, Information Technology Resource Security
[8] FIACCT 09-12.00
[9] Division of Finance: Capital (Fixed) Assets Internal Control Questionnaire

inventory control system by calculating annual loss rates.[10] While SLCC's and USU's methods currently apply solely to capital asset inventories, their approaches should be considered best practices for use in noncapital inventory as well.

Failing to properly account for assets places institutions in the vulnerable position of not knowing the extent to which assets are being lost or stolen. Conversely, accurately tracking assets provides the data necessary for institutions to measure inventory performance, identify risk areas, and identify any other areas that may need improvement.

Institutions Are Not Monitoring Noncapital Asset Policy Compliance

86 percent of reviewed departments were noncompliant with institutional policy or lacked policy requirements.

Because there is little institutional oversight, departments in charge of noncapital asset inventory are frequently out of compliance with their own policy. We found 86 percent of reviewed departments to be noncompliant with policy or to be lacking policy requirements. Of the eight institutions, only two list policy consequences that hold departments accountable for noncompliance. Best practices used at some institutions to increase inventory compliance include standardized inventory methods, access to common inventory tracking tools, and designated noncapital asset liaisons.

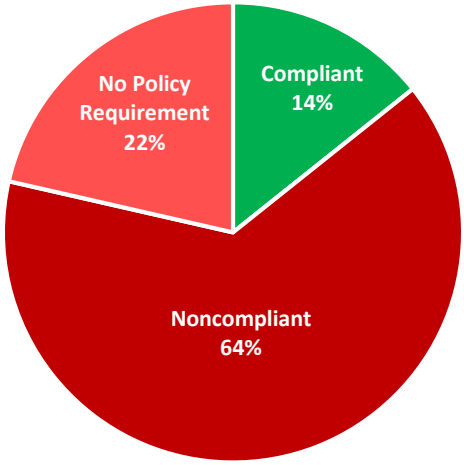
Institutions Need an Established Method of Inventory Oversight

12 of 14 departments were found to be noncompliant with their institution's policy requirements or lacked policy requirements.

Four institutions' inventory policies delegate inventory responsibilities to departments. However, the lack of institutional oversight and failure to provide departments with adequate procedures, tools, and resources have resulted in high rates of noncompliance. In our review of 14 departments, 12 were found to be noncompliant with their institution's policy requirements or lacked policy requirements, and 2 were found to be compliant. The varying levels of compliance and lack of policy requirements can be seen in Figure 2.5.

[10] Annual loss rates measure the key results of a physical inventory. An annual loss rate is calculated by comparing inventory results (found assets) with inventory records during the physical inventory reconciliation phase.

Figure 2.5 Departmental Policy Compliance Levels. We reviewed a total of 14 departments, and 9 were found to be noncompliant.



Source: Auditor analysis April 2018

Among the departments reviewed in Figure 2.5, we reviewed five biology departments, three of which were found to be noncompliant with their institution's inventory policy. Our concern with science departments is the amount and value of equipment for which they have responsibility. For example, one biology department reported having a total of $462,692 in noncapital assets that had never been inventoried. Additionally, three athletic departments admitted to having a pitching machine, a desktop computer, cameras, and camera lenses that had no asset tags and were not tracked.

Although required in policy, one biology department reported having $462,692 in noncapital assets that had never been inventoried.

Decentralized inventory practices have contributed to departments adopting a wide array of inventory methods and high rates of noncompliance. One department was unaware of institutional policies to track noncapital asset items, three could not provide complete inventory lists, four did not perform regular inventories, and one was tagging items as auditors were conducting a walk through.

One department was unaware of institutional policy to track noncapital assets.

Central administration staff could not tell us with any certainty whether departments were conducting noncapital asset inventories according to policy requirements. Furthermore, there is no requirement in institutional policy for departments to report inventory results or methods. While we are not recommending that all

institutions adopt centralized inventory practices, we do recommend that institutions increase oversight and reporting measures for departmental inventories.

Policy Fails to Hold Departments Accountable for Missing Assets

Only two institutions have policies in place that hold departments accountable.

Of the eight institutions, only two have policies in place that hold departments accountable for missing assets. USU specifies that the responsibility for uninsured losses rests with its departments but leaves the choice of tracking noncapital assets to those departments. Central administrative staff at USU report that each department operates from their own budget, which staff feel is a built-in incentive to safeguard noncapital assets. However, USU's Equipment Management Office (EMO) reports that only 4 percent of the institution's departments (9 of 213) have elected to track noncapital assets. An additional 2 percent of departments (5 of 213) have elected to track computer assets only. USU's policy of placing the responsibility of uninsured losses back on departments that are subject to an elective noncapital asset tracking policy has provided little incentive for departments to track those assets.

The opposite problem exists with the remaining five institutions that have inventory policies. Rather than consequences without policies, they have policies without consequences. Failing to list consequences in policy does not allow institutions to hold departments accountable for noncompliant action.

Additional Best Practices Could Improve Departmental Inventory Compliance

Barcode scanners, web-based tracking systems, or other electronic devices could improve inventory accuracy rates.

Some institutions employ two other best practices that institutions should consider implementing. First, three institutions offer a barcode or web-based tracking system to be used either by their central tracking department or by individual departments. Departments agree that their institutions have no common tool to help them comply with institutional noncapital asset inventory policies. In fact, internal audit divisions at institutions have noted the value of these systems on a department level.

- A 2017 U of U internal audit recommended replacing a departmental inventory system because of software reporting and storage issues.

- An audit at UVU reported that a department "…lacks an adequate inventory system," and that "The department does not regularly reconcile inventory."

Because this issue has come up multiple times, institutions should consider implementing an institution-wide solution. In addition, the American Society for Testing and Materials (ASTM)[11] recommends the use of barcode scanners or other electronic devices for physical inventories of durable, moveable property to ensure data accuracy.

A second best practice involves designating a noncapital asset liaison, a practice used by WSU. Although WSU tracks noncapital equipment centrally, the institution also uses campus technology coordinators (CTCs), who are embedded and work in certain departments. CTCs are "A campus committee comprised of IT specialists and technical support staff from across campus…" These employees request, tag, and track IT assets and are a type of inventory liaison for departments. To ensure that noncapital asset inventories are conducted on a regular basis, institutions could consider designating noncapital asset liaisons to oversee decentralized inventory practices.

Designating a noncapital asset liaison could ensure that inventories are conducted on a regular basis.

Vague Institutional Policies Do Not Provide Sufficient Guidance

Three institutions had outdated policies that have not been revised or approved for more than ten years. Additionally, policies do not clearly define the type of inventory that should be tracked, leaving institutional policy requirements open to departmental interpretation. Outdated and vague policies have contributed to varying inventory practices within each institution and high rates of noncompliance.

Institutional policy is largely left open to departmental interpretation.

[11] ASTM is an international standards developing organization referenced by governments around the world in code, regulation and law.

Some Noncapital Asset Policies Are Outdated or Nonexistent

Three institutions have not approved or revised their inventory policies for more than ten years.

Three institutions have not approved or revised their individual inventory policies for more than ten years. For example, one policy contains outdated tracking thresholds and places responsibility for property inventories on an administrative office that no longer conducts the inventories. Because outdated policies do not reflect what should be happening in practice, policy compliance may be compromised. Figure 2.6 shows each institution's most recent policy approval or revision dates.

Figure 2.6 Many Institutions' Inventory Policies Are Outdated. Most recent revision of policy was six months ago, while the oldest policy has not been revised for 20 years.

Institution	Most Recent Policy Approval/Revision Date	Number of Years Since Last Revision
DSU[1]	March 1998	20
SLCC[2]	December 2017	0
Snow	No Policy	N/A
SUU	June 2001	17
U of U[3]	June 2014	4
USU[1]	May 2015	3
UVU	June 2013	5
WSU	September 2007	11

Source: Auditor analysis of institutional policies – April 2018
1 DSU and USU do not require noncapital asset tracking in their policies with the exception of IT equipment at DSU.
2 SLCC revised its inventory policy during the audit (12/2017). Prior to the audit, SLCC's last policy approval was 09/2001.
3 U of U is the only institution whose policy for noncapital asset inventory is separate from its capital asset policy.

Although outdated policies can increase the risk of noncompliance, institutions with more recent revisions have also seen several policy violations as mentioned previously. Policies that do not exist, are out of date, or are not being followed are concerning because inconsistent enforcement and lack of oversight have allowed a complacent attitude toward the safeguarding of valuable assets. Several institutions reported that they would like to see increased departmental accountability for noncapital asset tracking; however, the absence of proper policy guidance has become a roadblock in departmental inventory practices.

Many Institutions Do Not Clearly Define Noncapital Assets

Of the five schools that require noncapital inventory tracking, only two provide noncapital asset dollar tracking thresholds. Other institutional policies provide an incomplete list of suggestions, criteria, or vague definitions. For example, UVU's policy reads

> … department administrators shall maintain memorandum lists of '*sensitive*' equipment within their own departments in order to maintain better control over such items. [Emphasis added]

A UVU department representative stated that this policy language was a "loophole" since it left policy open to departmental interpretation. Another institution's policy gives each department the ability to determine what property they will track, once again leaving policy open to interpretation. To clarify, we are not recommending that all institutions adopt dollar tracking thresholds; however, we are recommending that assets to be tracked are clearly defined.

Institutions need to balance the risk of loss with the cost of noncapital asset tracking.

Methods that the Regents and institutions could use to balance the risk of loss with the cost of more closely tracking noncapital assets include

- A risk-based approach that prioritizes the tracking of certain types of assets over others, such as computer or IT assets, and other highly pilferable assets.
- A cost-benefit analysis approach that may include selecting a dollar threshold whereby the monetary benefits of safeguarding those assets are offset by the total cost of tracking those assets.

Institutions should select and document an approach that best accounts for the total number and the total value of noncapital assets. Any policy issued by the Regents should follow the same process and clearly document the decision process of which assets will be tracked.

It is important for institutions to firmly decide and clearly define the type of assets and equipment that they will track. Best practices released by the GAO explain that

> Policies and procedures demonstrate management's commitment to the inventory physical count process and

provide to all personnel clear communication and comprehensive instructions and guidelines for the count.

Well-written policies can contribute to better compliance rates.

Establishing well-written policies with clear instruction can contribute to better compliance rates. Institutions that do not have established tracking procedures or inventory timelines in their policies increase the risk of declining compliance rates. We recommend that institutions examine and update their policies to both match guidance provided by the Regents and provide departments with clear reporting and accountability measures, procedures, and guidelines. We also recommend that the Regents and institutions clearly determine the types of assets that they will track while plainly communicating these definitions in policy and related trainings.

Recommendations

1. We recommend that the Utah State Board of Regents create and document a policy specifying requirements for noncapital asset tracking procedures. This policy should plainly define the value and types of assets to be tracked and the methods to be used.

2. We recommend that all institutions of higher education ensure that noncapital assets are appropriately tagged and that inventories are then conducted on a consistent and regular basis, based on the policy set by the Utah State Board of Regents.

3. We recommend that all institutions of higher education revise their policies to reflect those set by the Utah State Board of Regents. These policies should include noncapital asset accountability and reporting measures that enable the institution to ensure departments are appropriately safeguarding noncapital assets.

4. We recommend that institutions of higher education review the best practices listed in this audit report and determine which should be included in their policies. Best practices could include

    a. Developing inventory accuracy rates or trend analyses to better account for the number and value of noncapital assets.

b. Providing departments with a barcode scanning system, a web-based system, or another common tool for more accurate inventory results.

c. Designating a noncapital asset liaison as a point of contact for inventory compliance.

5. We recommend that institutions of higher education examine their policies to ensure that they are up to date.

Chapter III
Auditors Easily Gained Unauthorized Access to a Significant Number of Institution Facilities

Audit staff was able to clandestinely enter multiple facilities at each of Utah's institutions of higher education. Auditors found valuable assets left unsecured within the rooms of these facilities. These vulnerabilities in building access, in conjunction with findings in campus burglary reports, demonstrate that institutions need to train personnel on basic security procedures. It also demonstrates the need for institutions to conduct risk assessments of facilities' security weaknesses and act based on these assessments.

Audit Staff Accessed Institutional Facilities After Nightly Lockup Procedures

Audit staff successfully entered 31 facilities during our after-hours tests of building security. The ease with which auditors entered buildings is concerning, given that exterior entrances are the first line of defense in protecting assets in the building. These tests were conducted between 12 a.m. and 5 a.m. after the nightly lockup of buildings and did not involve forceful entry.

Attempts to Access Locked Facilities Were Consistently Successful in a Short Amount of Time

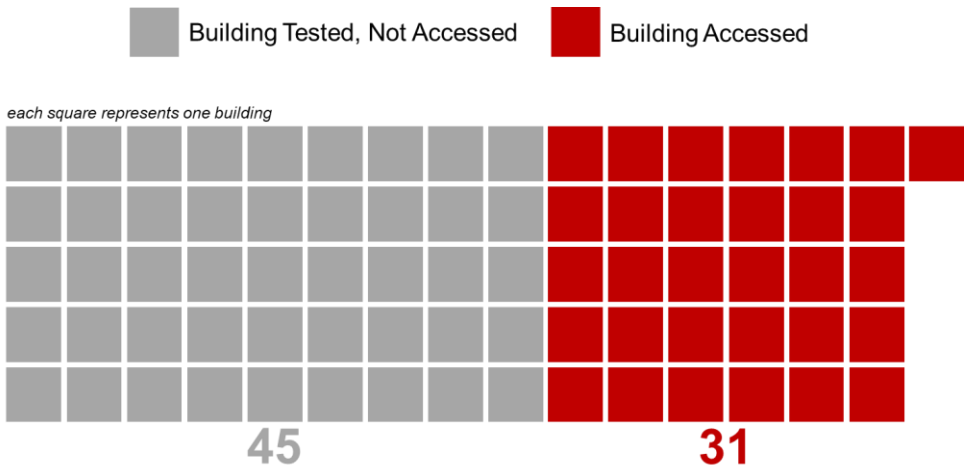
While testing building security at Utah's institutions, we successfully entered facilities at each institution after nightly lockup procedures had been performed. The institutions' chief public safety officers knew about these attempts at entry, but staff responsible for securing the buildings did not.

We gained access to 41 percent of the buildings we attempted to enter as shown in Figure 3.1. Each audit team accessed multiple buildings on each campus, spending about 1.5 hours at each institution. Our attempts to enter buildings were merely opportunistic—simply walking around building perimeters trying to open doors to see if they were unlocked or not completely closed. We did not try to bypass any doors that were latched and locked with any

Auditors accessed 41 percent of all buildings they attempted to enter during after-hours security tests.

kind of tools or excessive force, nor did we have any extensive knowledge of building floorplans.

Figure 3.1 Audit Staff Accessed 41 Percent of All Buildings They Attempted to Enter. Auditors accessed 31 of 76 campus buildings they attempted to enter after-hours.



Source: Auditor generated
Auditors did not test all exterior doors on 11 of the 45 buildings that were not entered.
Of the 31 buildings that were accessed, 3 were accessed via unsecured hallways from other buildings.
Buildings accessed during after-hours audit tests between January and April 2018

During our after-hours security tests at all 8 institutions, we gained access to 31 major institutional buildings.[12] We primarily tested main academic buildings with potentially high-value assets, such as buildings that housed science, automotive, medical, and fine art departments. The buildings that were accessed included ten science buildings, six technology/trades buildings, four administration buildings, and three engineering buildings.

More than Half of All Accessed Buildings Were Entered Through Incompletely Latched Exterior Doors

18 of the 31 buildings entered during after-hours security tests were accessed through doors not fully latched.

Audit staff frequently gained access to buildings after hours through doors that were locked but not completely latched. Of the 31 buildings accessed, 18 were entered through doors that were not closed completely and therefore not fully latched. These unlatched doors were likely caused by personnel passing through them after lockup and not ensuring they were secure. Auditors had to push on

[12] We also accessed a storage shed and a mechanical room not connected to the rest of the interior of the building it was housed within. These were not counted in the 31 accessed building total.

these doors after passing through to get them to completely latch. To prevent these breaches, personnel with after-hours access should be limited and trained on securing facilities.

Doors on six of the buildings that we accessed had been left unlocked. Two of those doors were left unlocked by janitorial staff, making janitors the next most common means by which auditors accessed building exteriors after-hours. In total, janitors allowed auditors to enter five buildings at two institutions by unlocking, propping, or opening doors for us (even though we did not identify ourselves). These actions, along with the fact that we conducted most of these tests without being reported to public safety, are concerning and demonstrate institution personnel's inadequate security awareness.

The Majority of After-hours Security Tests Went Unreported. The majority of these after-hours security tests went unreported to public safety despite our suspicious activities on these campuses in the middle of the night. Most tests were conducted when public safety officers were on duty.[13] However, we were approached and questioned by public safety personnel at only two institutions. We assume that officers would attempt to question and identify us had they noticed our activities. Additionally, we encountered janitors during the majority of the tests, though only one janitor reported us to their institution's public safety department.

We are concerned with the consistent vulnerabilities found at each institution. While we agree with a Utah System of Higher Education security report[14] that "…no physical controls are completely impregnable," we feel that our tests demonstrated an alarming weakness in building security and security awareness. Furthermore, it was concerning how many interior rooms in these buildings, even ones containing valuable assets, were left unsecured.

While we agree that no physical controls are completely impregnable, the security weaknesses our tests found are alarming.

[13] Six of the eight after-hours security tests were done while public safety or security personnel were on campus.

[14] This refers to Information Security Assessment and Penetration Testing reports conducted by Utah State System of Higher Education that will be discussed in Chapter V.

Unlocked Interior Rooms Leave Assets Vulnerable and Show Lack of Security Awareness

Over 150 unsecured rooms allowed access to many valuable and critical assets during auditor's after-hours security tests. The prevalence of unsecured rooms demonstrates the need for personnel security training. While exterior doors need to be secured, our access to assets was completely based on whether interior rooms were locked. Locking interior rooms is vital for the security of assets. Burglary reports from these institutions suggest that criminal access could have been gained using the same vulnerabilities that auditors found during the tests.

Audit staff accessed over 150 rooms during after-hours security tests. Some of these contained valuable or dangerous assets.

Unsecured Rooms Allowed Access to Valuable, Hazardous, and Critical Assets. Audit staff gained entry to over 150 unlocked rooms in the 31 buildings accessed during our after-hour security tests.[15] Five of these rooms alone contained assets worth hundreds of thousands of dollars.[16] Not only did we gain access to rooms with costly assets but also to rooms that contained biohazard or radioactive materials, live animals, or utility assets.

Our access to these valuable assets was based on whether interior rooms were secured. For instance, in one building, only one instruction room was unlocked, while in another building, we accessed seven research labs on one floor containing highly valuable assets. Figures 3.2 and 3.3 describe the various open rooms and unsecured assets we found.

[15] Not all rooms were checked in every building that auditors accessed during these tests.

[16] This value is based on a limited analysis of inventory records available for the rooms auditors accessed.

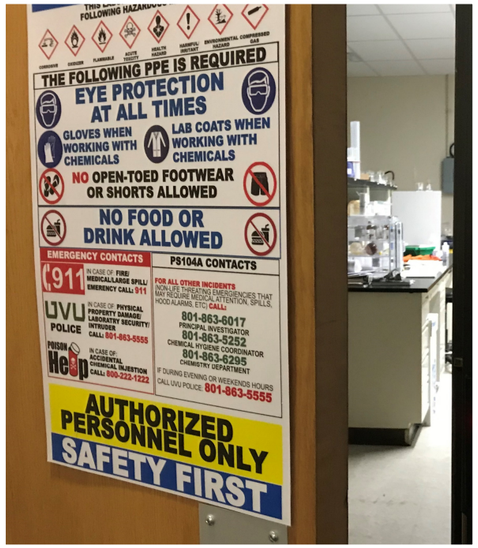
Figure 3.2 Number and Risks of the Rooms Audit Staff Accessed During Security Tests. Each type of interior room that auditors accessed contained valuable or sensitive items, some of which are shown in the figure.

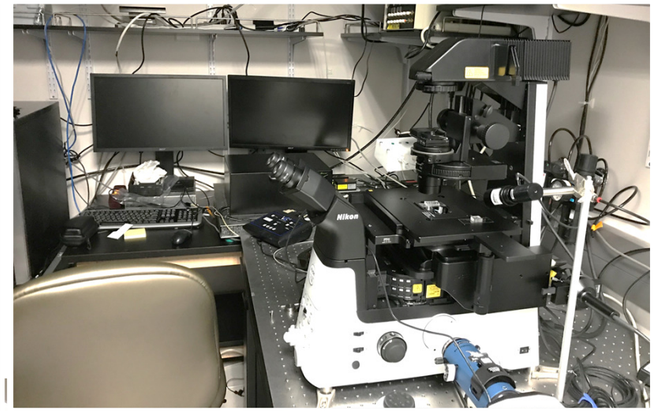
Room Type	Description	# Unsecured	Risks
Classroom	General classrooms	70	Most had at least one computer and a TV or projector. Some classrooms had credentials written on the computers that allowed us to log on.
Research	For conducting research. Includes cold rooms and an equipment corridor	19	Five of these areas contained equipment costing a total of $290,000. Signs on some indicated biohazardous, radioactive, or other dangerous materials.
Office	Faculty offices or general department office areas	17	Most of these offices contained IT equipment.
Science Lab	Science labs primarily for teaching	12	Some contained hazardous materials or live animals. One contained a piece of equipment costing over $30,000.
Storage	For storing institution items	9	One storage room contained 5 pieces of equipment costing over $17,000.
Utility	Structural system equipment, telecom closets, etc.	7	These rooms contained valuable equipment critical to a building's operation. Unsecure telecom closets may expose IT network.
Computer Labs	Multiple computers for providing computer services to patrons	6	One contained equipment costing over $33,000, another's equipment cost over $36,000.
Trade/ Shop Area	Instruction rooms, labs, or work areas for automotive, electrical, sewing, etc.	6	Some contained heavy equipment. The automotive area we accessed contained cars with keys left inside them.
Art Area	Rooms such as recital halls, dance studios, theatre & practice rooms	5	Some of these contained assets such as musical instruments.

Source: Auditor generated
Rooms accessed during after-hours security tests between January and April 2018

Figure 3.3 Audit Staff Found Unsecured Access to Many Rooms within Buildings . Pictured below is only a small sampling of some of the rooms we accessed during after-hours security tests.

Research Labs/Areas





Computer Labs

Trade/Shop Areas

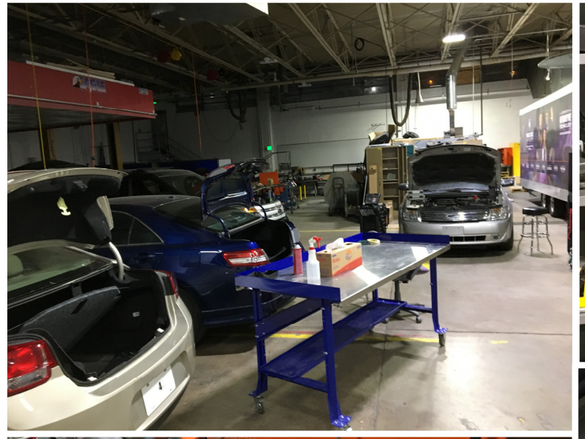
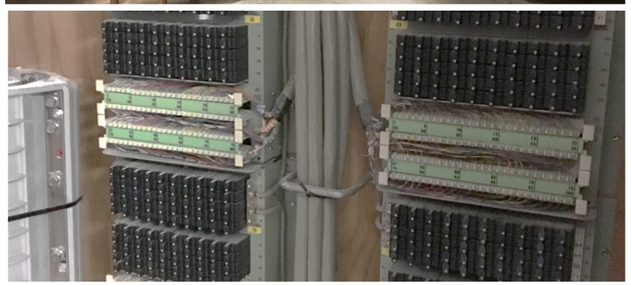


Figure 3.3 Audit Staff Found Unsecured Access to Many Rooms within Buildings . Pictured below is only a small sampling of some of the rooms we accessed during after-hours security tests.

Science Labs

Utility Areas



Storage Rooms

Classrooms

Though the timing of some after-hours security tests may have overlapped with janitorial or other staff activities in the buildings (who may have left rooms unlocked), it is extremely concerning that we were able to access as many rooms and valuable assets as we did.

Burglary Reports Also Suggest Unsecured Buildings Are a Problem

Burglary is defined as the unlawful entry into a structure to commit a felony or theft; past campus burglaries can provide insight into building vulnerabilities. Institutions' public safety department reports suggest that burglars found security vulnerabilities at institutions like those found by auditors. While we were not able to review all police records of the last five years at Utah's institutions due to time constraints, public safety departments reported that 139 cases recorded burglary as one of the offenses.[17, 18] Of those, 95 cases or 68 percent, were classified as unforced entries, indicating that a person did not use force, such as breaking windows or using tools to force locks or doors, but rather trespassed through an unlocked or open door or window. Many burglars may have entered buildings through vulnerabilities similar to what we found. This is very concerning.

Of the 139 reported burglary cases at institutions in the last five years, at least 95, or 68 percent, were classified as unforced entries.

These burglaries might have been less successful, even prevented, had interior doors been locked. During our night security tests, most assets were kept in interior rooms, highlighting the need to secure all interior spaces. Locked interior rooms would discourage burglars and protect assets. To help prevent unauthorized entry, institution personnel, especially those with after-hours access, need to be trained regarding their security responsibilities.

Security Training and Policies Would Better Protect Institution Property

Valuable assets left vulnerable because of unlocked interior rooms and unlatched exterior doors reflect inadequate security awareness from institution personnel. Institutional security training on existing policies is lacking despite professional guidelines recommending staff

[17] These cases were limited to burglaries from main campuses (not student housing/residential facilities) and where property that was damaged or stolen belonged to the institutions.

[18] Calendar years 2013 through 2017.

be trained in security practices. Security training is especially important for institution personnel who work after building operating hours. Also, policies requiring regular maintenance of exterior doors are important for building security.

Institutions Are Responsible for Training Personnel to Secure Facilities

Security guidelines recommend employees be trained in security practices.

Security guidelines from the National Fire Protection Association (NFPA) state that employees at colleges and universities should be trained on their security responsibilities. Specifically, these guidelines say that "Training should provide up-to-date information covering security practices, employee security awareness, personal safety, and so forth."[19, 20] At least five of the eight institutions have an institutional policy highlighting personnel's responsibility for maintaining security. Specifically, they mention personnel's role in securing doors and buildings as shown in Figure 3.4.

[19] Reproduced with permission from NFPA 730-2018, Guide for Premises Security, Copyright© 2017, National Fire Protection Association. This reprinted material is not the complete and official position of the NFPA on the referenced subject, which is represented only by the standard in its entirety which can be obtained through the NFPA web site at www.nfpa.org.

[20] This guide is a primary resource used by Division of Risk Management employees when assessing building security.

Figure 3.4 Five Institutions' Policies Specifically Detail Personnel's Roles in Securing Building Access. These policies detail personnel's responsibility to secure doors to both buildings and rooms.

Policies Regarding Individual Responsibility to Secure Doors	
Salt Lake Community College	Each individual is also responsible for the security of his/her own department, building(s), office, class labs or shop areas. These areas are to be secured before leaving each area.
Dixie State University	The last instructor using any room each day will be responsible for locking the door(s) to that room and securing the window(s) where appropriate. All University personnel will assume personal responsibility for turning off lights and locking doors in their assigned areas and buildings.
University of Utah	It is the responsibility of all personnel using buildings after regular hours to see that lights are turned off in the rooms they are vacating and that office doors and outside doors are secured.
Snow College	Individuals will assume responsibility for turning off lights, locking of doors and closing windows in their assigned areas and buildings.
Utah State University	All employees must turn off lights and equipment and lock office doors, outside doors and windows at the close of office hours.

Source: Auditor compilation of institution policies as of November 2017

We asked all institutions' public safety departments about efforts to encourage or educate personnel about their security responsibilities. Most replied that encouragement was given verbally when needed or that they knew of no official effort being made. The U of U, however, reported giving two to four presentations a month to various university personnel on campus safety and keeping their areas secure. The presentations included awareness about locking doors, not propping doors open, and not letting other people in building unless they are authorized to be there.

U of U's Department of Public of Safety gives 2 to 4 presentations a month to university personnel regarding access security practices.

It is important that all institutions begin official efforts to train personnel regarding their security responsibilities, which should be established in policy. Given the findings from our after-hours security tests, training should include personnel's responsibility to ensure doors are both locked and latched after passing through them. Security training is especially necessary for both public safety personnel and janitorial staff who have security responsibilities or an after-hours presence.

Because janitorial staff typically work after-hours, we believe it is important for them to have better procedures and policies for securing interior and exterior doors. While janitorial staff at institutions report employing practices that require keeping rooms and facilities secure during their shifts, the majority of institutions do not have documented janitorial policies or procedures. Custodial managers reported that security procedures are spread verbally. This practice is concerning given janitors' activities in buildings after-hours.

Utah Valley University provides new custodians with an orientation on custodial procedures at the beginning of their employment. These procedures include lockup of facilities and not allowing other individuals into locked areas. We believe this orientation is a good example of training employees on their role with building security, and may be a reason why we were approached by custodians during the after-hours security tests at UVU.

Preventative Maintenance on Doors Is a Good Practice. We are concerned with how consistently we were able to enter campus buildings after-hours through unlatched doors. Most institutions' public safety departments reported that a major cause of unlatched doors is personnel entering and exiting buildings after hours without ensuring that the doors close completely. Given the hundreds of exterior doors on campuses, and the fact that all institutions reported allowing faculty, staff, or students in buildings after operating hours, this poses a significant security risk. [21]

Preventative maintenance can address many issues that may prevent a door from fully latching.

A malfunctioning door closer or lock, building air pressure (a major concern), worn hinges, or misalignment from door sagging could all be addressed by preventative maintenance. Three institutions' facility management departments reported not performing regular preventative maintenance on all doors. The other five institutions reported inspecting every door at least annually. Facility Management at Southern Utah University, for instance, reported having a part-time employee whose primary duties consist of checking every door at least annually for key function, hinges, closer, and lever/panic function.

Guidelines and standards from the NFPA, federal Interagency Security Committee (ISC), and industry companies suggest conducting and logging regular maintenance on doors and locks for

[21] Excluding student housing and hospital buildings, U of U reports at least 945 doors and WSU reports at least 545 exterior doors on their main campus buildings.

security measures.[22] We believe that this is a best practice for building security as a non-latching door compromises all access management with that door. Institutions should establish and continue regular preventative door maintenance, especially on exterior doors, to ensure they close completely when used.

Institutions Should Base Security Decisions on Assessed Risks

Most institutions' public safety personnel do not formally assess and document potential security risks to all their facilities. As a result, public safety personnel may be reactionary rather than proactive in preventing building security risks. Guidelines suggest that risk assessments should be used to guide security decisions. We recommend these guidelines be followed and security measures be established and required of facilities based on risk assessments.

Public safety personnel at most institutions do not formally assess and document potential risks to their facilities' security.

Institutions Do Not Conduct and Document Methodical Risk Assessments of Facilities

Public safety staff at most institutions report not conducting a documented risk assessment of all facilities. Some institutions are currently developing a facility risk assessment or have done them sporadically when requested by departments. Government and professional guidelines advise performing, documenting, and acting on methodical risk assessments of institutions' property and assets.

Security assessments provide a basis for security planning.

Security Decisions Should Be Based on Assessed Risks. The NFPA guide on security recommends conducting a vulnerability assessment as a basis for security planning, using a methodical process to analyze security risks. The NFPA guide states that such an assessment is central to its recommended security planning.[23]

Additionally, federal security guidelines[24] state that risks to a facility must be identified and assessed to determine the security

[22] *NFPA 730 Guide for Premise Security*, ASSA ABLOY's *Key Control Design Guide*, and the ISC's *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard Appendix B: Countermeasures*. The ISC security guidelines are for all non-military federal facilities.

[23] *NFPA 730 Guide for Premise Security*

[24] ISC's *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*.

countermeasures needed to address those risks. This is important as a building's characteristics can create unique risks that require customized security measures. Further, these federal guidelines state that "It is extremely important to completely document the rationale for accepting risk, including alternate strategies considered or implemented, and opportunities in the future to implement the necessary level of protection."

Security assessments conducted at the U of U found the same vulnerabilities that auditors found in their after-hours security tests.

Security assessments occasionally conducted by U of U security officers identified some of the same security vulnerabilities that audit staff found during their after-hours security tests. These risks included unlatched doors and unlocked interior doors, two factors that enabled auditors to enter buildings and rooms containing valuable assets. This is further evidence of the ability that risk assessments could provide to public safety departments to proactively prevent breaches in building security. Methodical and documented risk assessments can provide structure for decisions made by public safety officers, including the justification to implement or not implement security measures as discussed in the following section.

Some Institutions Report that Security Measures are Foregone for Budget Concerns

A few institutions reported that security measures (such as surveillance cameras and electronic access control) have been omitted from new buildings due to competing financial interests and limited budgets. This raises concerns similar to those discussed in the following chapter regarding failing to rekey doors, in that security decisions are based on funding limitations rather than on the risks they address.

While security measures have to be carefully balanced against limited budgets, the justification for forgoing security measures, especially when recommended by public safety personnel, should be thoughtfully considered and documented. As stated by the ISC:

> The decision to accept risk is not one to be taken lightly … For that reason, it is critical that decision-makers obtain all the information they deem necessary to make a fully informed decision…

> In some cases, accepting risk is unavoidable. Multiple competing requirements, standards, and priorities cannot always be reconciled. All budgets have some limitation, and political and mission requirements cannot be ignored. In all cases, the project documentation must clearly reflect the reason why the necessary level of protection cannot be achieved.[25]

While accepting risk may be unavoidable, the reasons to do so must clearly be documented.

The need to justify why a security measure is not taken is another reason for having a documented risk assessment. However, when certain security measures are assessed as necessary on all facilities, they should be implemented. One method observed during the audit that provides surety for a certain level of security is seen in the U of U's Design Requirements for new or remodeled buildings. These requirements which are approved by an institutional committee, for instance, require electronic access on all exterior doors. Established security requirements for facilities may prevent security measures from being eliminated by budgetary and political forces as cited by some institutions and the ISC.

We recommend that institutions conduct and use risk assessments of facilities to establish security measures needed to protect institution assets. Additionally, we encourage institutions to establish basic security measures that should be required on buildings.

[25] ISC's *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*.

Recommendations

1. We recommend that institutions of higher education establish clear policies detailing personnel's security roles and responsibilities.

2. We recommend that institutions of higher education implement routine preventative maintenance on all exterior doors.

3. We recommend that institutions of higher education require interior door security awareness training of personnel.

4. We recommend that institutions of higher education routinely conduct and document formal risk assessments of facilities and implement security measures to mitigate the assessed risks.

Chapter IV
Security at Institutions Is Compromised By Poor Access Management

Our review of data from Utah institutions of higher education found inadequate controls over master key distribution. Many master keys have been lost or unaccounted for, which may compromise building security. Institutions have not addressed the risks of these lost keys by sufficiently rekeying their facilities. This is concerning because access management is the primary form of security for each institution's assets. Institutions need to better track keys to learn of lost or transferred keys and to collect them from personnel when appropriate.

Many Master Keys Have Been Lost or Are Unaccounted For

Data from the institutions show that many master keys are issued with questionable controls. This has led to many master keys being lost or unaccounted for,[26] which may compromise physical security. Access control, including mechanical keys and locks or electronic access control (electronic access), is the primary form of physical security at most institutions. The controlled distribution of keys is critical to maintaining security.

Many Master Keys Are Issued and Lost

Many master keys are issued at the institutions that were able to provide data. Many of these master keys have been lost. This is concerning due to security risks and costs that these keys would cause if lost or misused. We recommend that institutions review their controls over the issuance of master keys and use alternate ways to provide access to individuals with an official need.

[26] The remainder of this chapter will refer to keys that institutions cannot find as "lost." This includes current employees who report lost keys, former employees who never returned their keys, etc.

Data on keys issued or lost was unavailable or limited at some institutions.

Key Records Should Be Accessible. It is extremely concerning that half of institutions could not provide the full data on master keys issued and lost needed for this report. One institution was unable to produce any basic information on the number of master keys issued or lost. Three other institutions were only able to provide partial data on the number of issued and lost master keys. We will discuss our concerns with the many master keys that are distributed or lost later in this chapter; however, our ability to evaluate the access management at these institutions is limited. This is very concerning to us, as we believe that their ability to evaluate their own systems is similarly limited.

Master Keys Should Be Strictly Limited. Institutions' key systems have multiple levels of keys with various levels of access. Other than keys that open a single classroom or office door, institutions' key systems generally include the following master level keys:

- **Grandmaster/Campus Master Key** – Opens most or all interior doors, usually for an entire campus, though it may have some restrictions; may also open exterior doors
- **Selective Master Key** – Opens all or most doors of a certain type of room across multiple buildings, such as telecom or mechanical rooms
- **Building Master Key** – Opens most doors within a building; may also open exterior doors

Professional and government guidelines encourage restricted distribution of master keys.

Guidelines from professional and government sources such as the National Fire Protection Association (NFPA), ASSA ABLOY, and the Interagency Security Committee (ISC) urge strictly limiting these master keys, recommending that they be issued only when there is a legitimate need, not desire.[27, 28] One guideline specified limiting top master key distribution to "only a few" keys. Strict limitation of master

[27] *NFPA 730 Guide for Premise Security*, ASSA ABLOY's *Key Control Design Guide*, and the ISC's *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard Appendix B: Countermeasures*.

[28] The NFPA guide is a primary resource used by Division of Risk Management employees when assessing building security. ASSA ABLOY is an international leader in door hardware, and most of Utah's institutions use key systems manufactured by them or their subsidiaries. The ISC security guidelines are for all non-military federal facilities.

keys is understandable given that all these guidelines suggest that any doors accessible by keys that are lost should be rekeyed. While this may seem an unrealistic expectation due to the hundreds of doors that would need to be rekeyed for a lost grandmaster, it highlights the serious compromise of physical security that occurs from a lost key. Some of the burglary cases at these institutions mention the unauthorized use of keys. Despite these occurrences, institutions have issued master keys at concerning levels.

Institutions Have Issued Many Master Keys. We were concerned with the number of grandmaster, selective master, and building master keys issued at those institutions that could provide data. Given the sheer number of master keys issued and the security and financial risk of losing a master key, we believe their distribution should be more limited. The examples of master key distribution shown in Figure 4.1 cause concern.

Figure 4.1 Many Master Keys Have Been Issued at Each Institution.* Many issued master keys are concerning given the security risks if lost.

Key Type	Institution	Space Accessed	Number Issued
Grandmaster /Campus Master	Salt Lake Community College (SLCC)	Three campuses	151-180 each
	Utah Valley University (UVU)	Main campus	236
	Southern Utah University (SUU)	Main campus	105
Selective Master	Weber State University (WSU)	Some building exteriors, mechanical rooms	255
	University of Utah (U of U)	Telecom rooms[1, 2]	131
	Utah State University (USU)	Electrical, mechanical, and telecom rooms[1, 2]	113
Building Master	USU	Two buildings	54-63 each
	U of U	Four buildings	113-142 each
	UVU	Four buildings	53-81 each

Source: Auditor generated from institutions' data
**Of the institutions that were able to provide data. Institution data current at time of retrieval, occurring between December 2017-May 2018.*
[1]Access to telecommunication closets has been highlighted as an exploitable cyber security risk.
[2]The majority of these types of rooms are accessible by the key, though some may not be.

Multiple institutions have issued over 100 grandmasters each.

We are concerned with the quantity of master keys issued in these examples given the costs and security risks if one of these keys is lost. Previously mentioned guidelines recommend a tightly controlled distribution of master keys. Additionally, it appears that some of the master keys have been issued for convenience rather than need.

Some Master Key Issuances Raise Questions of Whether They Were Issued for Need or Convenience. All institutions have key issuance controls in place, such as requiring authorizing signatures for certain keys. However, we are concerned that these controls may not be limiting key distribution only to those who have an official need for access that cannot be accommodated another way. We question the need to issue master keys, for example, in the following instances:

- One institution issued a grandmaster key to their general counsel that can access all interior and exterior doors.
- One institution reported that all full-time facilities management employees (with a few exceptions) receive grandmaster keys.
- Two institutions have issued dozens of selective master keys or multiple grandmaster keys to contractors or vendors.
- Two institutions reported issuing building master keys to students.

These key issuances may represent valid needs for access; however, our concern is with the controls that authorize the need for keys with such expansive access. While some lock shops reported that they might question an employee on their need for requested master keys, multiple lock shops reported that they are not a policing force and must issue keys if the request has the correct authorizing signatures. We are concerned that some employees who authorize personnel's needs for master keys may be quick to issue a master key as a convenience without seeking alternative ways to provide access. As NFPA guidelines warn, while master keys can be a convenience (in not having to be issued multiple lower-level keys), their distribution increases security risks and therefore should be carefully managed.[29] We recommend institutions implement training for those who authorize keys to avoid issuing master keys for convenience.

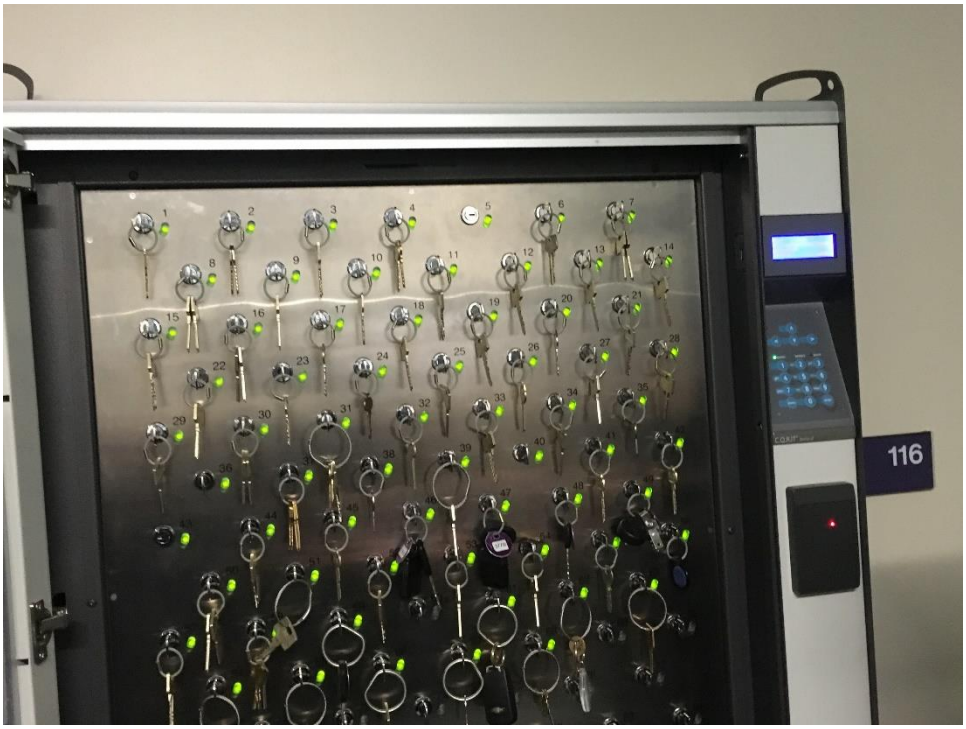
Those who authorize key issuances need training to avoid issuing master keys when unnecessary.

[29] *NFPA 730 Guide for Premise Security*

Alternatives to Issuing Keys Should Be Sought. Some institutions use alternative ways to provide access that should be considered before permanently issuing keys. For example, two institutions use lockboxes that allow facility management employees to check out specific keys when they need access to certain buildings. These lockboxes can only be accessed by authorized personnel to check out only the specific, preauthorized keys needed for their job duties. The lockboxes keep track of who checks out which keys, notes when they are returned, and can report via email if keys are not returned by a specific time. Figure 4.2 shows an example of one of the institutions' lockboxes.

Institutions should seek alternate ways to provide access where possible.

Figure 4.2 Lockboxes Provide an Alternative to Permanently Issued Keys. This opened lockbox allows employees to get the access they need without keys being permanently issued.



Source: Auditor photo from Weber State University – December 2017

The lockbox in Figure 4.2, similar to lockboxes at another institution, controls key access and prevents employees from always carrying around keys that they only need periodically.

Another alternative to issuing keys includes having university personnel escort those with temporary or occasional needs, such as contractors or vendors, to restricted locations they need to access.

Electronic access offers unique abilities to control and limit access.

Electronic access also offers unique ways to provide more controllable access. One key card can have as much, or as little, access as has been assigned to it. This access can include temporary needs or limited access to specific rooms during specific times. And while electronic access keys can be lost, introducing the risk of unauthorized entry, the key cards can be deactivated immediately when reported as lost. However, as will be discussed in the next section, the cost of electronic access prevents it from being a practical solution for all doors. The cost makes the management of mechanical keys, especially master keys, still vital to physical security. Because the loss of a master key can create serious risk, institutions should consider these and other alternatives to issuing master keys.

Institutions Have Lost Many Master Keys

Lost keys threaten the physical security of all spaces they access.

The number of lost master keys that we saw is concerning. A lost physical key compromises the security of the spaces it accesses. Whereas an electronic access key can be deactivated when reported lost, a lost physical key is a threat to security until the locks it accesses have been rekeyed. It is important to track lost keys as this should be an indicator of the risk posed to physical spaces. However, half of the institutions' lock shops could not provide lost key data either because they did not track it or because the information was not easily accessible.[30] This is very concerning. Examples of available data from institutions for the last five years shows the following:

- USU reported 95 lost building master keys.
- UVU reported 136 lost building master and 26 lost grandmaster keys.
- SLCC records showed 13 lost campus masters or grandmaster keys.

Additionally, we found that all other institutions that could provide data had lost multiple copies of master keys (except SUU who reported not having lost any building masters or grandmasters).[31]

[30] We requested data on master keys that had been lost between 2013 and 2017. Some institutions had this information located only in individuals' files that would be onerous to compile.

[31] SUU's low number of lost master keys appears to be an anomaly. The large scope of this audit prevented us from spending additional time to discover why.

These keys may be physically lost or simply unaccounted for due to personnel who have left the institutions without returning keys. The latter situation, which will be addressed in this chapter, suggests a lack of access management controls. These results are concerning but can be rectified through better key collection controls and by rekeying the locks. However, institutions have performed little rekeying in response to lost keys.

Rekeying Buildings Is Rare Despite Many Lost Master Keys

Despite guidelines recommending locks be rekeyed when keys have been lost, the majority of the institutions have not rekeyed despite the loss of master keys. We are concerned that the security of buildings and rooms may be compromised. Additionally, rekeying decisions should be based primarily and methodically on the security risk that the lost key imposes. Because both the costs to rekey or install electronic access are high, mechanical key distribution should be limited.

Rekeying Locks Is Rare Despite Lost Keys

At the majority of institutions, rekeys have rarely been performed in response to lost master keys. This is concerning given the security risks of a lost key. Rekeying locks is the means of rectifying a lock system after a key has been lost.[32] Guidelines from professional and government sources recommend that all locks should be rekeyed when a key to those locks is lost.[33] One guideline even recommends rekeying at regular intervals whether or not keys are lost. However, in the last five years, rekeying has rarely occurred despite the number of lost master keys. Below are some examples.

Guidelines recommend rekeying locks when keys are lost.

[32] Rekeying entails changing the pin combination in lock cylinders or replacing the lock cylinders altogether, requiring the issuing of new keys (and preventing any lost keys from being usable).

[33] *NFPA 730 Guide for Premise Security*, ASSA ABLOY's *Key Control Design Guide*, and the ISC's *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard Appendix B: Countermeasures*.

- **UVU.** Despite 162 building master and grandmaster keys lost in the last 5 years, no affected buildings have been fully rekeyed.

- **USU.** Despite 95 building master keys lost in the last 5 years, only 2 entire buildings have been rekeyed.

- **U of U.** An inventory of keys in August 2017 found that 77 keys were lost from a U of U health science building. This building was not rekeyed.

- **SLCC**. Despite 13 lost campus and grandmaster keys in the last 5 years, none of the affected buildings have been fully rekeyed.[34]

While the cost of rekeying must be balanced against the security risk resulting from the lost key and available budget, it is concerning that so few rekeys have been done when so many master keys have been lost. Given the lost keys and the lack of rekeying, assets in these buildings are likely not secure. Doors may not be rekeyed often because the cost and decision of rekeying is often left up to the department.

Decision to Rekey Should Be Based on Security Risk

The majority of institutions have the departments pay for *and* decide whether or not to rekey.

When keys have been reported lost, departments at the majority of institutions are responsible to pay for *and* decide whether or not to rekey. While the practice for a department to pay for the rekey follows guidelines for access management, leaving the decision to the department may be one reason so few rekeys have been performed. Guidelines are clear in recommending the rekeying of spaces accessed by lost keys, yet departments are given the option to delay or decline the costs of rekeying and thereby accept increased security risks. Rekey costs should be built into the budgets of institutions and their departments so that they do not neglect needed security maintenance.

"In some cases," states the ISC, "accepting risk is unavoidable." However, the ISC states that it "…is extremely important to

[34] While SLCC reports not rekeying entire buildings in the last five years, they report rekeying most of their classroom doors when upgrading them to electronic access.

completely document the rationale for accepting risk." Similarly, the risk posed by lost keys may not always demand a rekey, but a methodical approach and documentation of why the risk was accepted would better inform security decisions.

WSU has started developing a risk assessment procedure for lost keys. The developing assessment weighs the kind of key, whether it was lost or stolen, where it was believed to be lost (close or far geographically), and whether the spaces it accessed contain valuable assets or sensitive information. We recommend that institutions develop a method to evaluate the risk posed by lost or stolen keys, especially master keys, to better guide rekeying decisions.

Costs to Rekey Should Encourage Limited Key Distribution and Adoption of Electronic Access. Rekeying an entire building can be costly. Two institutions estimate the cost to rekey to be between $60 to $200 a for an interior door lock, depending on the type of key and the manner and complexity of the rekey. Hence, for a medium sized building of about 200 interior doors, a rekey of these door locks may cost anywhere between $12,000 to $40,000. The high costs, and the fact that security experts recommend rekeying when keys are lost, are reasons to restrict master keys distribution. Building master and grandmaster keys should be treated as highly valuable assets with strictly controlled distribution. This is also true at institutions that have electronic access.

Rekeys of buildings are very costly and should encourage the strict control of master keys.

Some institutions have cited the benefits of electronic access over rekeying doors. If an access card is lost, for example, that card can be deactivated through the software program rather than rekeying a system of doors. However, the installation of electronic access on a door can cost a significant amount and could include door hardware, card readers, cabling, backup batteries, and other electronic hardware (as well as labor for installation). Professional quotes for institutions to upgrade a single door to electronic access range from $1,100 to over $4,100, the latter including everything mentioned in the previous list. Despite the benefits of electronic access, the high cost may make it an impractical solution for all doors.

To encourage the adoption of electronic access, USU's facility management department, for example, has incentivized departments to make the costly upgrade to electronic access hardware on interior doors by offering to cover future maintenance, replacement, and

software costs. Other institutions could employ similar strategies to encourage adoption of electronic access control where needed.

Though upgrades to electronic access control are costly and may not always be practical, it provides exceptional solutions for lost keys.

Because of the high cost of electronic access, institutions should base the decision to switch to electronic access on assessed risks. Risks addressed through electronic access could include doors with many issued keys that could be lost, doors that need to have regulated hours of operation, etc. While not conducting a formal risk assessment, SLCC has addressed certain risks by equipping most exterior doors and most classroom doors with electronic access. The upgrade cost over one million dollars. While electronic access is a useful solution for certain risks, because of its cost, mechanical locks and keys will still be a major component of building security and thus should be well managed.

Institutions Need to Better Track and Collect Keys

Most institutions are not conducting regular key inventories. Institutions need up-to-date, accurate information on access that has been granted through mechanical or electronic key distribution. Key inventories and audits provide this necessary information. Additionally, keys should be collected from employees when their employment no longer requires that access.

Most Institutions Are Not Performing Regular Inventories of Keys

Guidelines recommend that all keys are inventoried regularly.

Most institutions are not conducting regular inventories of all keys. Guidelines from the ISC and NFPA indicate that all mechanical and electronic keys should be inventoried regularly.[35] Like asset inventories discussed in Chapter II of this report, key inventories inform management of the accuracy of key records and whether personnel still have the keys issued to them. Inventories are conducted in various ways, such as requiring the keyholder to physically present their keys to authorized staff or simply having keyholders declare over email what keys they have in their possession.

[35] *NFPA 730 Guide for Premise Security* and ISC's *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard Appendix B: Countermeasures*.

Four of the eight institutions have policies requiring annual key inventories or auditing of access. Other institutions inventory sporadically or when requested by individual departments. However, only two institutions report that they regularly inventory all keys as highlighted in Figure 4.3

Figure 4.3 Half of Institutions Have Policies Requiring Key Inventories. Only two institutions report conducting regular inventories of all keys.

	Inventory of All Keys Required in Policy?	Regular Inventory of All Keys	Compliance with Key Policy
WSU	No	No	Compliant
Snow	Yes	No	**Noncompliant**
USU	Yes	**Yes**	Compliant
SLCC	No	No	Compliant
SUU	No	**Yes**	Compliant
DSU	Yes	No	**Noncompliant**
U of U	Yes	No	**Noncompliant**
UVU	No	No	Compliant

Source: Auditor generated
According to current policies as of November 2017.

Three institutions are noncompliant with requirements in their policies to inventory keys.

As highlighted in red in Figure 4.3, three of the four institutions with policies requiring an annual key inventory were noncompliant with their own policies. Staff at one of the noncompliant institutions stated that poor key management software precluded them from conducting regular inventories. Specifically, they reported that they could not pull reports of keys by department but would have to review individual personnel files. This is similar to a report from another institution that does not conduct inventories regularly. We encourage all institutions to use software that will allow for accurate inventories as these are critical for effective access management.

Inventories Are Critical Controls for Accurately Tracking Keys

Inventories and audits provide necessary safeguards for key management. Procedures to report lost keys or report job changes to access management may fail. Inventories and audits identify lost keys, inaccurate records, and personnel who no longer need access due to transfers, resignations, or terminations. Below are results from two

inventories conducted in the last five years that caught issues that may have otherwise gone unnoticed.

Inventories can provide necessary safeguards by identifying lost keys, inaccurate records, and employee changes.

- In a key inventory of a single U of U department, management found that 77 keys had been lost. It also found over 100 employees who had either transferred or left the department and still had keys, as well as 20 employees who had keys that were not on the lock shop' s records.

- An annual inventory of a department at USU found at least 36 missing keys. Additionally, they found other keys that were issued to employees that were not on key records.

These inventory results highlight the importance of conducting such procedures. Without the audits, access management personnel might not have identified these issues.

Audits Are Needed with Increased Use of Electronic Access. While inventories of electronic keys are helpful in determining whether they have been lost and need to be deactivated, unlike inventories of mechanical keys they do not inform management about a person's access. A key card for electronic access, as mentioned previously, can have as much or as little access as has been assigned to it. Because of this, and because of the increased use of electronic access at institutions, verifying personnel's access with their management is very important. Below are results from two audits conducted in the last five years that caught issues that might have otherwise gone unnoticed.

- A DSU audit of their business building's access found that 46 percent of individuals with various levels of electronic access to interior and outside doors should no longer have access. Some of the change in access was caused by termination of employees.

- An SLCC audit of electronic access to two classrooms found that 5 of 16 department personnel needed to have their access removed.

Institutions should not only implement regular physical inventories of mechanical and electronic keys, but also conduct regular audits of electronic access granted to personnel. These inventories and audits

highlight the need to better track employees who no longer need access.

Procedures to Collect or Deactivate Keys Need Improvement

Key inventories and audits found that personnel had key or electronic access despite having been transferred or terminated. This is alarming. Key management guidelines recommend that policies establish procedures to collect or deactivate keys when employees no longer need access.[36] The majority of controls for the collection of keys and deactivation of electronic access are not comprehensive. Additionally, despite policies forbidding it, key management personnel at four institutions reported being aware that departments or supervisors were keeping keys when employees leave and no longer needed access, which can lead to unauthorized access.

Keys need to be collected or deactivated when personnel no longer need them.

The Majority of Current Key Collection Processes Are Not Comprehensive. Most institutions' key shops primarily rely on a report of employment changes from their human resources department to know when keys need to be returned or deactivated. These employment changes include terminations, retirements, and transfers. However, the majority of these lists are not comprehensive and may include only employment changes for salaried or benefited employees (not part-time or student employees). Additionally, some lists may not include job changes such as department transfers, may have only started this procedure, may have old information, or may not be used by lock shop personnel. We recommend institutions establish clear procedures and controls in policy for following up with people who need to turn keys in.

Controls to collect keys may not be fully comprehensive and need improvement.

Additionally, we recommend that institutions employ controls in electronic access software that automatically deactivates access. For instance, one institution reports setting up students' electronic access to automatically deactivate at the end of each semester. Such controls will better prevent unauthorized access.

[36] *NFPA 730 Guide for Premise Security*, ASSA ABLOY's *Key Control Design Guide*, and the ISC's *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard Appendix B: Countermeasures*.

Recommendations

1. We recommend that institutions of higher education review their controls over the issuance of master keys and restrict master keys issued when access can otherwise be accommodated.

2. We recommend that institutions of higher education implement security training for those who can authorize keys.

3. We recommend that institutions of higher education establish a methodical process to determine whether to rekey after keys are lost.

4. We recommend that institutions of higher education conduct regular inventories of all keys and audits of all key access.

5. We recommend that institutions of higher education use software that will easily allow them to audit or inventory access.

6. We recommend that institutions of higher education establish clear controls for collecting or deactivating keys when personnel no longer need access.

7. We recommend that institutions of higher education create safeguards in electronic access controls to eliminate access for those who no longer need it.

Chapter V
Institutions Generally Lack IT Inventory Controls, But Closely Monitor Data Security

Inventory controls over information technology (IT) assets at institutions of higher education need improvement.[37] Inadequate inventory controls are concerning because IT assets are some of the items most likely to be lost or stolen. Six of the eight institutions do not perform an annual physical inventory, though four institutions use a digital inventory, which compensates for not tagging items but is an inadequate inventory control. Although they do not inventory physical assets, institutions are closely monitoring data security to protect the data the assets can access. This is done through both day-to-day operations and biennial security tests performed by information security officers at the institutions.

Most Institutions Do Not Adequately Inventory IT Assets

Five of the eight institutions do not perform an annual IT asset inventory. These items are some of the most frequently pilfered assets; about half of the 115 loss claims recently submitted by institutions are for IT assets. It is concerning that these items are not more closely tracked. Some institutions compensate for the lack of a physical inventory by conducting a digital asset inventory.

Most Institutions Do Not Annually Perform a Physical Inventory of IT Assets

Only three institutions perform an annual IT inventory.

Five of eight institutions do not perform an annual IT inventory or are unaware whether departments are performing inventories.[38] This deficiency is alarming, as IT assets are some of the most pilfered items. As discussed in Chapter II, most institutions delegate the inventorying and tracking of noncapital assets to departments but do not ascertain

[37] This report will define IT assets as those assets that are capable of accessing institutions' data networks.

[38] One of these five institutions, Utah Valley University (UVU), is in the process of creating an annual IT inventory process, but has not yet implemented it.

whether the departments actually conduct inventories. While three institutions maintain departmental responsibility for IT assets, four have delegated the responsibility to a central IT authority, and one does neither. Figure 5.1 explains who is responsible for IT assets at each institution and whether they perform an annual physical inventory.

Figure 5.1 Only Two Institutions Annually Inventory IT Assets As of 2018. UVU is in the process of creating an annual inventory process.

Institution	Entity Responsible for IT Assets	Annual Physical Inventory Performed
DSU	Central IT	No
SLCC	Central IT	Yes
Snow	Not Tracked	No
SUU	Department	No[1]
U of U	Department	No[2]
USU	Department	No[2]
UVU	Central IT	No[3]
Weber	Central IT	Yes

Source: Auditor analysis of institutional data
[1] Central IT at SUU is not required to track IT assets, but they decided to do it for their own benefit. While they maintain a record of computers at each department, they do not conduct an annual physical inventory. They also note that it is possible for departments to have bought computers they do not know about.
[2] Physical audits may occur in some departments, but not in all. The Universities cannot tell us which departments conduct audits.
[3] UVU central IT is in the process of forming a standardized annual inventory. They did a pilot in 2017.

Half of burglary claims institutions of higher education submitted to Risk Management involved computer assets.

Figure 5.1 is concerning because of the risk of lost items and the easily pilferable nature of IT assets. As discussed in Chapter II, institutions submitted 115 claims of burglary and theft to the Utah Division of Risk Management, almost half of which included computer assets. [39] Even more alarming is Snow College, which does not track IT assets and therefore cannot inventory them. Institutions increase the risk of missing assets by neglecting physical inventory controls.

Standards Require Tracking IT Devices. Two main data security standards (the Center for Internet Security's "CIS Critical Security Controls for Effective Cyber Defense" and the National Institute of Standards and Technology's Special Publication 800-53) both prioritize the inventory of devices. One of these standards, the CIS Critical Security Controls for Effective Cyber Defense, used by

[39] Claims were submitted during calendar years 2013 to 2017.

institutions, lists an "inventory of authorized and unauthorized devices" as its first control. It advises entities to

> Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Standards require tracking of IT assets to prevent unauthorized data access.

This standard points out the importance of tracking IT assets, not only to prevent loss but also to prevent unauthorized devices from accessing the network.

A group organized by the Utah System of Higher Education (USHE) performs biennial security tests at each of its institutions.[40] This group conducts a penetration test and reviews the requirements set forth by CIS at the institution's request. In the last two cycles of reviews, only three of the eight institutions elected to review the inventory requirement. The review found that one institution had nearly optimized this standard, while another was in the beginning stages. While choosing not to test device inventory does not necessarily mean the standard is not being met, it does raise questions about institutions' knowledge of where IT assets are located and which ones can access their network.

Some Institutions Digitally Tag IT Assets

Some institutions digitally track employee computer access.

Some institutions use some form of digital inventory to track computers. For example, USU requires all employees to annually confirm that they are still using the computer that is registered to them. Employees are sent an email asking them to log on to their computers and click a link renewing their registration if they still use that computer. If they do not go through this process, they cannot get on the network. USU does not then locate missing computers, although it has their addresses on file and could digitally track them. This system is a limited version of inventory that does little to address missing assets. Digital inventories compensate for the tagging of physical assets but are inadequate on their own as a physical

[40] These tests will be discussed in more detail later in the chapter.

inventory control. At least three other institutions use some form of this digital inventory.

Institutions Closely Monitor Data Security

Institutions have been continually vigilant in their efforts to secure sensitive data. Because institutions generally do not physically inventory IT equipment, securing the data that equipment accesses is doubly important. Utah institutions are making efforts to secure their data using national standards and have created a group to do security and penetration tests to detect weaknesses.

Data Access Is Closely Controlled

Institutions have made strong efforts to protect accessible data.

Although institutions may not all have adequate physical controls over IT assets, they have made strong efforts to protect the data that those resources may be able to access. This has been the case for some time; an audit report released by our office in 2011[41] noted that "higher education proactively monitors IT security." Our current review found that institutions continue to monitor IT security and try to adhere to best practices in data security.

This Report Does Not Detail Institutions' Security Plans. We note that this audit report has taken some of the same precautions as did the 2011 report. Namely,

To avoid risking data security, this report is intentionally generalized in its security discussion.

> Given the critical nature of and need to protect IT security plans, some information and conditions at universities…will not be discussed in this report. Instead, this report focuses on presenting some best practices that entities can rely on to protect their information assets and processing resources. The entities we worked with during this audit were rightfully protective of the security information they shared with us during the audit. Disclosure of security control details in this report could enable a potential attacker to more easily breach an entities IT security. Therefore, we have not disclosed the sensitive

[41] Report 2011-10 *A Performance Audit of IT Security at Universities and Quasi-Government Agencies*

details of entities' systems. Where needed, we discussed issues with agency management as items were identified.

This remains true of the current audit.

Institutions Use Many of the Best Practices Detailed by Data Security Experts. As briefly discussed previously, there are multiple sources of data security best practices. Institutions follow one set of data security requirements and the Utah State Department of Technology Services (DTS) another, but both have similar requirements.[42] Some of the overarching best practices include

Data security efforts include software inventory, secure configuration, and vulnerability assessments.

- Device physical inventory[43]
- Software inventory
- Secure configuration of devices
- Continuous vulnerability assessment and remediation
- Controlled use of administrative privileges
- Email and web browser protections
- Malware defenses
- Control of network ports

The institutions are very aware of these standards and are working towards meeting them at varying levels of development. Figure 5.2 shows some methods currently in use to meet these standards, and how widely they are implemented.[44]

[42] When reviewing institutions for appropriate data security, higher education uses the Center for Internet Security's (CIS) Critical Security Controls for Effective Cyber Defense. DTS uses the National Institute of Standards and Technology (NIST) Special Publication 800-53.

[43] This best practice, as discussed in more detail earlier, was found to be lacking at most institutions.

[44] We note that this statement is not meant to imply that these methods are optimized or that there is no room for improvement in these areas.

Figure 5.2 Institutions Report Using Various Methods to Protect Data in Fiscal Year 2018. Many of these methods are used in practice and required in policy.

	Two Factor ID	Regular ID Finder	Privilege Controlled	Restricted Data Center	All Devices Encrypted	Sensitive Devices Encrypted
DSU	Yes	Partial	Yes	Yes	In Process[1]	Yes
SLCC	Yes	Yes	Yes	Yes	No	No[2]
Snow	No	Partial	Yes	Yes	No	Yes
SUU	Yes	No	Yes	Yes	No	Partial
U of U	Yes	Yes	Yes	Yes	No	Yes
USU	Yes	Yes	Yes	Yes	No	Yes
UVU	Yes	Yes	Yes	Yes	Yes	Yes
Weber	Yes	Yes	Yes	Yes	No	Yes

Source: Auditor compilation of institutions' data

[1] Dixie encrypts all new laptops and is working back through older machines. Some desktops are encrypted based on the sensitivity of the data.

[2] SLCC reports that encryption is not required because no machines should have sensitive information on them.

The practices listed in Figure 5.2 are all ways to try to meet the standards discussed previously. We note that the institutions listed in Figure 5.1 that do not track IT inventory would not know whether these methods are used on all machines. The methods in Figure 5.2 include:

- Two-factor identification – a log on verification program. Users log in to their accounts and are then required to verify their identities on a phone or other device.
- Identity Finder – a system to locate sensitive information on devices. When sensitive information is located, users are encouraged to remove it from their devices. USHE purchased this system for use by all institutions.
- Privilege controlled – IT staff have only the least privileges and credentials required to do their jobs and cannot access administrative areas they do not need.
- Data center – where all the data is housed and restricted to as few staff as possible.
- Device encryption – locks devices using a secret code. Without the password, accessed data looks like gibberish.

There Are Low-Cost and Group Solutions for Data Security. Both two-factor identification and device encryption are interesting discussions. First, the two-factor system used by institutions was first purchased and then required by USHE. In September 2016, USHE sent a memo to all institutions requiring Multi-Factor Authentication for all faculty and staff. Data security officers report that this is considered one of the best proactive practices and most cost-effective solutions for preventing unauthorized theft and use of computer accounts. This is an interesting case of USHE recognizing a need and exercising its oversight responsibilities to ensure it was addressed. While multiple institutions were already implementing this control before required, institutions have told us this is a very useful tool in their security arsenal. Snow College, the only institution to report not using two-factor identification, reports that it is in the testing phase and will soon be implemented.

USHE purchased and required two-factor identification of all institutions.

The second area, encryption, is also interesting because two institutions reported that encrypting institution devices is a low-cost undertaking. Microsoft and Apple machines automatically come with the ability to encrypt the machine by simply checking a box in the settings. Implementing encryption on an institution-wide basis would be slightly more complicated, but still considered low cost. While most institutions require machines that hold sensitive data to be encrypted, institution information security officers told us that it would be very useful to them if policy required all machines to be encrypted. In fact, a U of U internal audit report recommended that "…policies requiring encryption of certain devices be strengthened. Ideally, encryption should be required for all mobile devices except those containing only public data." Encryption appears to be a low-cost step to increase data security and we recommend that the Utah State Board of Regents (Regents) determine whether to require encryption on all machines.

Device encryption is a low-cost security measure.

USHE Group Analyzes Institution Security

Institutions have found a low-cost way to meet the penetration test standard put forth by both NIST and CIS. Since 2013, information security officers from most USHE institutions have conducted a biennial security review of all institutions. This review includes digital penetration testing as well as testing the physical security of institutions, with emphasis on breaking into data centers.

Security reviews have been an effective, low cost way to test data access at institutions.

Institutions report that this security review is quite beneficial to their security, both the review itself and the knowledge their staff gains while conducting reviews of other institutions. They also report that these reviews have been quite cost effective, with some smaller institutions reporting that they would not have the resources to either conduct a similar test or pay for one.

Because of the extremely sensitive nature of these reports, we will not be discussing the detail of the findings or methods of the reviews. We will note two main general findings.

Institutions have generally improved over time.

First, the reports generally note improvement over time at the institutions. Most reports noted that many conditions from previous reviews had improved, indicating that institutions take these reports and data security seriously. Most institutions reported that, after the reviews were conducted, they were reported to a small number of administrators and then an action plan was developed to fix problems. Information security officers further report that, in general, they were given the resources needed to mitigate the weaknesses found.

Decentralized IT systems make data security more difficult.

The second finding, which seems to be repeated over multiple years, is that those institutions with a decentralized IT system have a much more difficult time enforcing data security requirements. Decentralized systems occur when an institution's central IT department does not control the purchase or security of all IT assets, but it instead delegates one or both to individual department IT staff. Much of the work done during the security review is done with the central IT, leaving departmental IT out of the review overall. Because this weakness is continually pointed out both by the security reviews and the IT standards used by the state and higher education, institutions should determine whether more closely centralizing IT would be beneficial to their operations. It would be valuable for the Regents to study this issue and determine whether the benefits of increased data security would outweigh the costs of centralizing IT at institutions. As part of this review, the Regents could review security at individual departments within institutions.

Recommendations

1. We recommend that all institutions of higher education follow policies enacted by the Utah State Board of Regents to inventory and regularly track physical IT assets.

2. We recommend that institutions of higher education continue to review data security measures at other institutions to determine which best practices would improve their own data security.

3. We recommend that the Utah State Board of Regents determine whether it would be useful and cost effective to require encryption of all institution of higher education devices with access to sensitive information.

Agency Response

UTAH SYSTEM OF HIGHER EDUCATION
Building a Stronger State of Minds℠

State Board of Regents
Board of Regents Building, The Gateway
60 South 400 West
Salt Lake City, Utah 84101-1284

Phone 801.321.7101
Fax 801.321.7199
TDD 801.321.7130
www.utahsbr.edu

July 11, 2018

Mr. John Schaff
Legislative Auditor General
W315 Utah State Capitol Complex
Salt Lake City, Utah 84114-5315

Dear Mr. Schaff,

Thank you for the opportunity to respond to the audit report entitled "A Performance Audit of Inventory and Security Controls at Institutions of Higher Education" on behalf of the Utah System of Higher Education (USHE). The Board of Regents and the USHE institutions have made concerted efforts to be prudent stewards for higher education assets and I appreciate your recommendations on how we may further secure system assets. We have already begun implementing many of the recommendations made in the audit report and will fully implement all 19 recommendations.

Chapters 1 & 2

We appreciate the auditors' recognition that "capital assets were, in general, tightly controlled by institutional policy,"[1] since capital assets make up the majority of tangible institution assets. Although accounting standards do not require entities to track noncapital assets and state Division of Finance policy allows state agencies to "choose *not* to track [noncapital] assets,"[2] five of the eight USHE institutions currently have policies that require tracking them.[3]

We agree with the auditors that tracking certain noncapital assets would benefit USHE institutions. I appreciate the auditors' recommendations that allow the Board of Regents to create a noncapital asset tracking policy that would benefit the system and its institutions. I will advance such a policy to the Board of Regents for their consideration and action as soon as possible.

Chapter 3

The auditors' work to identify potential building security risks during non-business hours is helpful. Institutional staff are actively working to correct exterior door deficiencies and to provide the recommended training to ensure interior and exterior doors are secured.

Chapter 4

We appreciate the auditors' review of key distribution and accounting procedures and institutional staff are in the process of implementing all seven recommendations. Although institutions do not necessarily

[1] "A Performance Audit of Inventory and Security Controls at Institutions of Higher Education," page 5.
[2] FIACCT 09-12.00 (emphasis added).
[3] "A Performance Audit of Inventory and Security Controls at Institutions of Higher Education," page 9.

employ a consistent practice for addressing lost keys, as noted in the audit report, staff at all eight institutions consider the risks that a lost key might create. Considerations for rekeying a building include the likelihood of the key being found by an individual with nefarious intentions, identified as a key to a specific lock, and used to gain unauthorized access of secured assets.

Chapter 5

We appreciate the auditors' recognition that USHE "institutions have been continually vigilant in their efforts to secure sensitive data."[4] In September 2016, the Board of Regents required institutions to "implement multi-factor authentication for all administrative and functional access to IT resources that store, process or transmit Personally Identifiable Information."[5] Multi-factor authentication significantly reduces the likelihood that an unauthorized individual could access sensitive information on any institution computer. We will implement all three recommendations to further secure IT assets.

Thank you again for the opportunity to respond to this audit report and we look forward to continuing to increase the effectiveness of our asset management.

Sincerely,

David L. Buhler, Ph.D.
Commissioner of Higher Education

[4] "A Performance Audit of Inventory and Security Controls at Institutions of Higher Education," page 54.
[5] Board of Regents Policy R345-4.1.3