

CHICAGO PARK DISTRICT  
OFFICE OF INSPECTOR GENERAL

---

# Audit of the Chicago Park District's Information Technology Asset Management

March 27, 2025



PETER NEUMER | INSPECTOR GENERAL  
DANIEL N. LOPEZ | DIRECTOR OF AUDIT

## Table of Contents

<b>I. Executive Summary</b> .....	<b>2</b>
<b>II. Background</b> .....	<b>4</b>
A. The IT Asset Lifecycle.....	4
B. IT Asset Databases.....	6
C. The IT Department and SDI .....	7
<b>III. Objectives, Scope, and Methodology</b> .....	<b>8</b>
<b>IV. Findings and Recommendations</b> .....	<b>10</b>
<b>Finding 1: The Chicago Park District risks loss or misplacement of IT assets due to the lack of formal, periodic inventorying</b> .....	<b>10</b>
A. The Chicago Park District does not have policies and procedures requiring a formal, regular inventory of its IT assets .....	10
B. The IT Department uses several, disparate databases to track the District's IT asset inventory instead of one centralized database.....	13
C. The IT Department stated it is not informed of District operations which impact inventory of IT assets .....	14
D. The Chicago Park District risks noncompliance with inventory requirements for IT assets purchased with federal funds.....	15
<b>Finding 1 Recommendations</b> .....	<b>16</b>
<b>Finding 2: The Chicago Park District risks loss or theft of an estimated half a million dollars of stored IT assets due to insufficient security measures...</b>	<b>17</b>
A. The Chicago Park District does not have policies and procedures requiring the secure storage of its IT assets.....	17
B. The Park fieldhouse does not have sufficient security measures to ensure protection against the loss or theft of its IT assets.....	18
C. The Chicago Park District risks noncompliance with safeguarding regulations for IT assets purchased with federal funds.....	20
<b>Finding 2 Recommendations</b> .....	<b>20</b>
<b>Appendix A: The Department of Information Technology's Management Response</b> .....	<b>22</b>

---

## Acronyms

CPS	Chicago Public Schools
IT	Information Technology
OIG	Office of Inspector General
SDI	SDI Presence LLC
SLFRF	Coronavirus State and Local Fiscal Recovery Fund

## I. Executive Summary

The Office of Inspector General (OIG) conducted an audit of the Chicago Park District's (District) Information Technology (IT) asset management to determine whether the District effectively inventories and stores its IT assets, which include, but are not limited to, laptops, monitors, routers, and switches. The District's Department of Information Technology (IT Department or Department) is responsible for the District's IT assets during the assets' lifecycle, including the inventorying and storage of these assets.

The OIG found the following:

1. The District risks loss or misplacement of IT assets due to the lack of formal, periodic inventorying.
2. The District risks loss or theft of an estimated half a million dollars of stored IT assets due to insufficient security measures.

Specifically, regarding inventory, the District does not conduct formal, regular (e.g., annual) inventories of its IT assets, risking the loss or misplacement of these assets. The IT Department stated that the last full inventory was completed in either 2018 and 2019. The District does not conduct these formal, regular inventories, in part, because the District does not require such inventories nor does it have policies outlining specific processes for inventorying IT assets. The District may be additionally hindered by the use of several siloed databases to record the IT assets, which limits the District's ability to effectively and efficiently access information regarding its IT assets, including their quantity, location, and status. Further, the IT Department stated the Department is not informed of District operations which impact its IT inventory, such as a department independently purchasing IT assets or personnel moving from one facility to another. Finally, as it relates to inventorying, the District procured a subset of its IT assets using federal funding and risks noncompliance with federal funding requirements, which explicitly require regular inventories.

Regarding the storage of IT assets, there is material evidence that the District does not adequately secure these assets prior to deployment. The IT Department requires a second working location, separate from the District's Headquarters building, for assembling and storing IT assets due to limited space within the Headquarters building. However, this second, off-site location within the basement of a park fieldhouse lacks adequate security measures to reduce the risk of loss or theft of these assets. Specifically, the fieldhouse is accessible to the public, does not have 24-hour security, and the one padlock used outside of the IT Department's basement area is often left unlocked during work hours. In addition, the IT Department does not have policies governing the security of its physical assets, including IT assets. Finally, the same federal funding discussed above also has safeguarding

requirements and, as such, the District risks similar noncompliance with these requirements as it does with the inventorying requirements.

To address the inventorying issues, the OIG recommends the following:

1. The IT Department should conduct formal, regular (e.g., annual) inventories of its IT assets, including developing written policies and procedures outlining the steps and designating the entities responsible for the inventory. The District should allocate the resources necessary to perform these inventories. The IT Department should further collaborate with the relevant District entities to develop written policies and procedures for ensuring coordination with the Department when IT assets are procured, lost, stolen, or transferred.
2. The IT Department should consider consolidating its separate, disparate IT asset inventory systems into one main system. To the extent that this is not practical or feasible, the IT Department should create an inventory of its databases to establish which systems include which type of IT assets. The IT Department should also work with staff, contractors, and vendors of these databases to resolve all errors to ensure valid and accurate data.
3. The IT Department should consult with the District's Department of Law to determine whether it is currently in full compliance with the inventory requirements of the American Rescue Plan Act's State and Local Fiscal Recovery Funds.

To address the security issues, the OIG recommends the following:

4. The IT Department should work with the District to securely store its IT assets by ensuring any storage location has the appropriate security measures in place for secure storage, including restricted access by unauthorized personnel.
5. The IT Department should develop and implement a formal policy outlining the protocols for safeguarding IT assets.
6. The IT Department should consult with the District's Department of Law to determine whether it is currently in full compliance with the safeguarding requirements of the American Rescue Plan Act's State and Local Fiscal Recovery Funds.

The IT Department agreed with the OIG's findings, stating it would work with the relevant entities to conduct annual inventories and to safeguard the District's IT assets, develop written policies for these processes, and consult with the Department of Law to determine the compliance requirements under the American Rescue Plan Act.

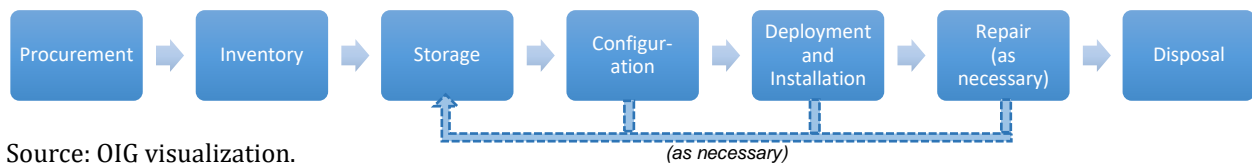
## II. Background

An asset is a resource with economic value owned or controlled by an entity, including information technology (IT) assets such as laptops, desktops, servers, monitors, chargers, and network equipment like routers and switches. The Chicago Park District (District) acquires various IT assets to assist in the performance of its mission and its operations. The District's Department of Information Technology (IT Department or Department) is responsible for these assets.

### A. The IT Asset Lifecycle

Each IT asset has a lifecycle, the stages of which include procurement, inventory, storage, configuration, deployment and installation, repair as necessary, and disposal (see *Figure 1*).

**FIGURE 1: THE IT ASSET LIFECYCLE**



Source: OIG visualization.

#### 1. Procurement

The procurement of IT assets typically begins when the IT Department's IT Manager or Senior Project Manager initiates a purchase with a vendor. If District employees require equipment, they are to submit a request through the IT Help Desk. This process helps ensure that the IT Department is informed of all equipment needs; however, there are circumstances where District personnel can procure IT assets independent of the IT Department (see Finding 1 for more information).

#### 2. Inventory

When a vendor delivers IT assets to the District, the vendor provides a receipt which serves as proof of delivery. For IT assets valued over \$100, the Department reviews the packing slip and enters the relevant data into the ServiceNow database, which creates an inventory entry for the asset. Some assets are also stored in other databases, depending on the type of asset and its intended use. As of September 4, 2024, the ServiceNow database contained a total of 5,046 IT assets (see Finding 1 for more information about the District's inventory processes and databases).

#### 3. Storage

The District stores its IT assets at one of two locations: (1) its District Headquarters and (2) the IT Department's working space in the basement of a park fieldhouse.<sup>1</sup> At Headquarters, a subset of IT assets is stored in a secured storage room, including spare laptops, monitors,

<sup>1</sup> In the interest of security, the OIG has deidentified the location of the park fieldhouse.

printers, and equipment designated as electronic waste (e-waste) for recycling and disposal. Access to this room requires a key card, which must be granted by authorized personnel. A second, separate location within Headquarters, known as the Data Center, contains the District servers and also requires key card access. The District's Department of Facility Management has access to the Data Center due to shared infrastructure, including the air conditioning and fire system. This room also stores e-waste. Additionally, lockable filing cabinets around the IT Department desks hold smaller items such as routers, switches, and antennas. The IT Department maintains a lockbox containing the keys to these cabinets.

At the park fieldhouse, the IT Department performs several of their duties in a room in the fieldhouse basement, including assembling and configuring IT assets. The Department also stores IT assets in this same room. Within this designated space, there is an additional storage room equipped with an electronic keypad for added protection. Both the primary room and the storage room feature shelving units for organizing equipment, as well as floor space for larger items (see Finding 2 for more information on IT asset storage).

#### 4. Configuration

The configuration of IT assets is typically carried out by a contractor, SDI Presence LLC (SDI; for additional information regarding SDI, *see infra* Section C of the Background section). This process involves setting up laptops and employee accounts, assembling touch screens and stands to create kiosks, and configuring network equipment to securely integrate with the existing infrastructure.

#### 5. Deployment and Installation

When District personnel require the use of an IT asset, a member of the IT Department will deploy, i.e., deliver, the asset to the personnel or personnel's workstation. According to the IT Department, when an asset is deployed, the ServiceNow database must be updated to indicate the new location and the new user of the asset.

#### 6. Repair

When assets, such as laptops or network equipment, become damaged or broken due to wear and tear, accidents, or hardware malfunctions, the IT Department coordinates with the asset owner to resolve the issue.<sup>2</sup>

#### 7. Disposal

When an IT asset reaches the end of useful life or is damaged beyond repair, it is classified as e-waste. Depending on the sensitivity and condition of the equipment, it may either be disposed of through an e-waste service or donated to organizations in Chicago that can utilize the equipment. As mentioned above, e-waste is securely stored at District Headquarters until the appropriate organization can collect it. Upon disposal, the organization brings their own pallets for transport and requires the presence of an IT Department member with access to the Data Center to oversee the collection and ensure that

---

<sup>2</sup> Additionally, the IT Department performs maintenance in the form of system updates and software patches by sending out updates to the District's computers through the use of IT asset management software.

only specified items are removed. All disposed assets must be updated in the ServiceNow database, designated as e-waste, and reclassified as disposed.

## **B. IT Asset Databases**

The IT Department uses several databases to record information about its IT assets. These databases include:

- *ServiceNow*  
ServiceNow tracks IT assets that meet a value threshold of \$100, including, but not limited to docking stations, monitors, kiosks, laptops, and printers. The database includes data fields for each IT asset including, but not limited to: serial number, location, manufacturer, asset tag, and assigned District personnel. It does not currently include any financial information relating to the cost of assets, but notes can be added to individual assets in order to record additional details such as physical damage, technical faults, repairs, and warranty facts. ServiceNow is not linked to other databases and requires manual updates to add or modify the status of assets. All changes made within ServiceNow are tracked and recorded via an automatic activity log.
- *Ivanti*  
Ivanti tracks desktop and laptop inventory by monitoring when these assets access the District network. Ivanti is completely independent from ServiceNow.
- *Ruckus*  
Ruckus is a required database under the City of Chicago's Digital Equity Plan, a public wi-fi initiative; this database tracks antennas and switches needed to provide wi-fi and is required because the wi-fi is open to members of the public, not just to District personnel.
- *A custom-built Android-based application*  
This app tracks the IT assets relevant to the City of Chicago's Digital Equity Plan; the app is also completely independent from ServiceNow.
- *Altaworx*  
Altaworx is a web-based platform that allows the IT Department to manage mobile devices and monitor their usage.
- *Cradlepoint*  
Cradlepoint is a web-based application for managing the District's routers. This application allows for the tracking of these assets in real-time as well as seeing each router's current status.

- *Verizon Portal*  
This portal enables the viewing of active phone numbers associated with the District's Verizon account, along with their monthly usage. Mobile phones are not recorded in ServiceNow.

### **C. The IT Department and SDI**

The contractor SDI provides the District with certain services, including assisting the IT Department with ongoing infrastructure projects, visiting District sites to assess IT assets, and updating asset information in the ServiceNow database.<sup>3</sup> SDI also administers ServiceNow as part of the contractor's service delivery.

---

<sup>3</sup> The District piggybacks off the contract that SDI has with the City of Chicago, but the contract has amendments to meet the specific needs of the District. The District has a five-year contract with SDI, which is set to expire at the end of September 2025 and can be renewed.

### **III. Objectives, Scope, and Methodology**

#### **A. Objective**

The objective of this audit was to determine whether the Chicago Park District effectively inventories and stores its IT assets.

#### **B. Scope**

The scope of this audit includes all policies and procedures for the Chicago Park District, broadly, and the IT Department, specifically, pertaining to the inventorying and secure storage of the District's IT assets. Additionally, this audit includes the primary storage locations of the District Headquarters and the park fieldhouse location, but does not include how individual facilities, e.g., fieldhouses, utilize, and secure actively used IT assets.

#### **C. Methodology**

The OIG performed the following methodology to conduct this audit:

- Reviewed policies and procedures from the Department of Information Technology and the Office of the Comptroller.
- Reviewed comparative policies and procedures from the City of Chicago, the Chicago Police Department, the Chicago Public Schools, the New York State Comptroller, and Los Angeles County, as well as the Los Angeles County Board of Supervisors.
- Conducted interviews with representatives from the Department of Information Technology, including SDI Presence LLC, as well as the Office of the Comptroller.
- Conducted one site visit to the Chicago Park District Headquarters building and two site visits to the park fieldhouse.
- Reviewed point-in-time data from the ServiceNow database dated September 4, 2024 and January 15, 2025.
- Reviewed the City of Chicago Digital Equity Plan, the Department of the Treasury's "Compliance and Reporting Guidance – State and Local Fiscal Recovery Funds," dated December 19, 2024, and the Code of Federal Regulations.

#### **D. Standards**

The OIG conducts performance audits with guidance from the United States Government Accountability Office's Generally Accepted Government Auditing Standards (GAGAS or "Yellow Book," 2024 revision). Pursuant to the Yellow Book:

Performance audits provide objective analysis, findings, and conclusions to assist management and those charged with governance and oversight with, among other things, improving program performance and operations, reducing costs, facilitating decision making by parties

responsible for overseeing or initiating corrective action, and contributing to public accountability.<sup>4</sup>

For other categories of work-product, such as advisories, explainers, notifications, and program descriptions, the Department follows the guidance set forth by the Association of Inspectors General in *Principles and Standards for Offices of Inspector General* ("Green Book," 2024 revision).<sup>5</sup>

### **E. Authority**

The authority to perform this audit is established in Chapter II(D)(4) of the Chicago Park District Code, which states that the OIG has the power and duty to promote economy, efficiency, effectiveness and integrity in the administrations of programs and operations of the District by reviewing programs, identifying any inefficiencies, waste and potential for misconduct therein, and recommending policies and methods for the elimination of inefficiencies and waste, and for the prevention of misconduct.

---

<sup>4</sup> United States Government Accountability Office, "Government Auditing Standards 2024 Revisions," February 2024, accessed February 24, 2025, <https://www.gao.gov/assets/d24106786.pdf>.

<sup>5</sup> Association of Inspectors General, "Principles and Standards for Offices of Inspector General," July 1, 2024, accessed February 24, 2025, <https://inspectorsgeneral.org/blog/newly-revised-aig-green-book-principles-and-standards-for-offices-of-inspector-general-is-now-available-for-download/>.

## IV. Findings and Recommendations

1

### The Chicago Park District risks loss or misplacement of IT assets due to the lack of formal, periodic inventorying

The Chicago Park District does not conduct formal, regular (e.g., annual) inventories of its IT assets, thus risking the loss or misplacement of these assets. The IT Department stated the last full inventory of District IT assets was completed in either 2018 and 2019. The District does not conduct these formal, regular inventories, in part, because the District does not require such inventories nor does it have policies outlining specific processes for inventorying IT assets. The District may be additionally hindered by the use of several siloed databases to record its IT assets, which limit the District's ability to effectively and efficiently access information regarding its IT assets, including their quantity, location, and status. Further, the IT Department stated the Department is not informed of District operations which impact its IT inventory, such as a department independently purchasing IT assets or personnel moving from one facility to another. Finally, as a subset of its IT assets were procured using federal funding, the District risks noncompliance with federal inventorying requirements.

#### A. The Chicago Park District does not have policies and procedures requiring a formal, regular inventory of its IT assets

Unlike other Chicago governmental entities, the District does not have policies and procedures requiring a formal, regular inventory of its IT assets. The following provides excerpts from these comparative inventory-related policies juxtaposed with the District's policy to illustrate the differences.

##### 1. Comparative Policies from Other Chicago Governmental Entities

The City of Chicago, the Chicago Police Department, and the Chicago Public Schools (CPS) each have policies requiring formal, annual inventorying of IT assets. The City of Chicago's "Information Security and Technology Policy" states:

An inventory of information assets, including systems, software, and service providers, is to be kept current at all times... Technical Operations and Enterprise Network Architecture [a unit under the purview of the City's Chief Information Officer] should compile and maintain a data repository catalog of physical assets owned by the City. This catalog should be reviewed and updated annually. The catalog should contain descriptive asset information. Business unit managers should assist Technical Operations and Enterprise

Network Architecture in maintaining this catalog and should communicate changes or additions in a timely manner.<sup>6</sup>

Similarly, the Chicago Police Department has its own inventory policy, separate from the City's policy, which states:

On an annual basis, the Office of Public Safety Administration [an administrative City department which supports the City's public safety departments, including the Chicago Police Department] will conduct a Department-wide equipment and technology audit to: 1. maintain an accurate and current inventory record of equipment and technology held by the Department [and] 2. determine what equipment is outdated, broken, or otherwise in need of repair or replacement.<sup>7</sup>

Additionally, CPS's "Asset and Inventory Management" policy provides the following instructions for CPS's physical inventory:

Each organizational unit accountable official or designee will conduct/oversee a physical inventory of all assets assigned to the organizational unit at least annually. The accountable official or designee will reconcile the results of the physical inventory to CPS's centralized electronic inventory and asset management system, identify and document any differences and investigate the reason for the differences within 30 days of the completion of the physical inventory. The organizational unit accountable official will be responsible for the compliance and accuracy of their annual inventory. The reporting unit will, on an annual basis, certify the unit's inventory and receive notice of compliance from the Office of the Controller.<sup>8</sup>

Each of these policies include similar guidance for conducting an inventory, specifically:

- The frequency of the inventory, e.g., all three policies require a minimum of an annual inventory;
- The entity or entities responsible for conducting the inventories and, where necessary, the ultimate authority of the annual inventory, e.g., in the CPS policy, while

---

<sup>6</sup> City of Chicago, "Information Security and Technology Policy," May 7, 2024, accessed February 24, 2025, <https://www.chicago.gov/content/dam/city/depts/dgs/InformationTechnology/ISTP.pdf>.

<sup>7</sup> Chicago Police Department, "Uniform and Property U05-02: Department Equipment and Property Control System," November 6, 2024, accessed February 24, 2025, <https://directives.chicagopolice.org/#directive/public/6253>.

<sup>8</sup> Chicago Public Schools, "Asset and Inventory Management," March 21, 2024, accessed February 24, 2025, <https://www.cps.edu/sites/cps-policy-rules/policies/400/401/401-9/#:~:text=All%20assets%20are%20to%20be,of%20receipt%20by%20CPS%20staff.>

individual organizational units are responsible for the physical inventory, the Office of the Controller determines that the inventory is in compliance.

- Updated procedures and clarifications, as necessary. For example, the City of Chicago's policy was originally effective October 20, 2014, with the most recent revision date of May 7, 2024; the Chicago Police Department's policy was effective May 21, 2002, with the most recent revision of November 6, 2024; and CPS's current policy, dated March 21, 2024, rescinds other policies which date back to at least 1988.

## 2. The Chicago Park District Policies

The District's "Asset Management and Inventory Control Policy," effective December 2013, does not establish a formal inventory process for any of the District's assets, including its IT assets. The policy notes that an October 2009 version of the policy required "documenting certain information on a standard form regarding non capitalized assets; [however, m]ost of this information was required to be captured and maintained on paper records which are cumbersome and not easily updated." In an effort to address the "cumbersome" paper records, the policy states:

Assets with a cost greater than or equal to \$5,000 with a useful life greater than one year will be capitalized and recorded by the Comptroller as part of the year-end financial reporting process... Departments will be required to update records for existing capital assets with a cost greater than \$500 but below \$5,000 on a standard excel spreadsheet... Certain equipment such as computers and printers have already been tagged and inventoried and therefore can be excluded from this policy. Once records are updated, spreadsheets should be maintained in electronic format by the Departments as well as at the location. It will be the responsibility of the Departments to ensure spreadsheets are updated and available for audit.<sup>9</sup>

The policy, last updated over a decade ago, does not specifically provide guidance for the inventorying of "[c]ertain equipment such as computers and printers" and neither the District, broadly, nor the IT Department, specifically, have inventory policies for such assets. Further, this policy does not require a regular, e.g., annual, inventory and does not designate an entity or entities responsible for such an inventory.<sup>10</sup>

The IT Department does attempt to record assets as they are procured, as discussed in Section A of the Background. Additionally, the Department partially relies on what it refers

---

<sup>9</sup> The December 2013 policy states this specific section was to be effective February 1, 2014.

<sup>10</sup> The "Chicago Park District IT Security Policy," dated December 4, 2007, does state, "[t]he Department of Information Technology maintains a central inventory of computer equipment and software via an asset inventory," but does not elaborate on this statement. The "Department of Information Technology IT Security Policy," dated October 2012 and marked as "Draft," contains the same statement.

to as an “automatic inventory” by documenting IT assets if they log onto the District’s network; however, the IT Department acknowledges if District personnel do not log in to the network, the Department cannot differentiate between an asset that is missing versus one that is simply unused.

### **B. The IT Department uses several, disparate databases to track the District’s IT asset inventory instead of one centralized database**

As discussed in Section B of the Background, the IT Department uses several databases to record information about its IT assets, including:

- ServiceNow
- Ivanti
- Ruckus
- Cradlepoint
- Altaworx
- A custom Android-based application
- A Verizon portal to record the District’s phone assets.

Many of these databases record only specific types of IT assets, (e.g., Ivanti for desktops and laptops, Ruckus for switches and routers) and the systems are siloed from one another (e.g., Ivanti is independent of ServiceNow, which, in turn, is independent of the custom app). This makes it difficult for either the District, broadly, or the IT Department, specifically, to fully understand the complete inventory of the District’s IT assets, including, quantity, location, and status of the assets.

Additionally, ServiceNow, the database that records over 5,000 assets such as laptops, monitors, and printers, presents unique challenges for assessing the District’s IT asset inventory. ServiceNow data from September 2024 showed 223 (4.4%) of IT assets did not have a known or listed location. The IT Department reviewed these assets and stated some of the issues were due to data entry errors while others appeared to be “test entries” among actual data. In the same data set, another 43 assets had a location that simply stated, “Chicago.”<sup>11</sup> The same dataset included 20 assets that did not have some or all of the following information: serial number (20 assets), location (15), manufacturer (19), model ID (19, with 11 of these specifically stating “unknown”), model number (17), and vendor (20).

Further, ServiceNow lacks standard classification of IT assets. For example, the database includes the classifications of “computer” and “personal computer,” which the IT Department stated should be a single category. The “computer” assets were created by five Department members, whereas all of the “personal computer” assets were created by one of the five members. Another example is an asset named “Cisco 2811” where one Department member

---

<sup>11</sup> The OIG inquired about the missing locations in December 2024; the IT Department reviewed the data and provided an updated data pull in January 2025 which had 30 assets that did not have a location and 50 assets that had a location of “Chicago.”

classified the assets as "Network Gear" and another member classified the assets as "IP Router." The same holds true for the assets named "Cisco AP 1815" and "R350 Series," where different individuals created the asset records and did not classify the assets in a consistent manner.

### **C. The IT Department stated it is not informed of District operations which impact inventory of IT assets**

The IT Department stated it is not informed of District operations which impact the IT asset inventory, including procurement of assets by other District entities, when assets are lost or stolen, and when personnel move within or separate from the District. Unlike other governmental entities, the IT Department does not have a policy for coordination with other District entities when operational changes or actions impact the IT asset inventory. For example, the Chicago Police Department states in regards to the procurement of new assets:

The unit commanding officer will immediately notify the Equipment and Supply Section, General Support Division, Office of Public Safety Administration upon receipt of any new or additional property that should be included on the Inventory Control Record.<sup>12</sup>

Regarding "lost, stolen, damaged, or unaccounted" assets, the same policy states:

Unit commanding officers will... prepare a To-From-Subject Report for all lost, stolen, damaged, or unaccounted inventoried property, stating pertinent facts relating to the investigation including documentation and action taken with reference to the circumstances surrounding the loss, theft, or damage of the property, and submit the To-From-Subject Report through their chain of command to the First Deputy Superintendent [and] notify the Equipment and Supply Section, General Support Division, Office of Public Safety Administration, providing a copy of the submitted To-From-Subject Report.<sup>13</sup>

Finally, for assets which are either removed, transferred, or exchanged:

Inventoried property will not be moved or transported from one unit to another without prior notice to the Equipment and Supply Section, General Support Division, Office of Public Safety Administration. Whenever property is removed, transferred, or exchanged, a Transfer Record/Inventoried Property form will be prepared by the unit or agency removing, transferring, or exchanging the property and one copy will be forwarded to Inventory Control, General Support Division, Office of Public Safety Administration. Each

---

<sup>12</sup> Chicago Police Department, "Uniform and Property U05-02: Department Equipment and Property Control System," November 6, 2024, accessed February 24, 2025, <https://directives.chicagopolice.org/#directive/public/6253>.

<sup>13</sup> Chicago Police Department, "Uniform and Property U05-02: Department Equipment and Property Control System," November 6, 2024, accessed February 24, 2025, <https://directives.chicagopolice.org/#directive/public/6253>.

unit will attach a copy of the Transfer Record/Inventoried Property form to their latest Inventory Control Record.<sup>14</sup>

Additionally, the City of Chicago states, “[b]usiness leaders are to assist in maintaining this catalog [i.e., asset inventory] and should communicate any changes or additions.”<sup>15</sup> The New York State Comptroller’s “IT Asset Management” report for school districts states, “officials should establish a separate, well-defined policy that includes guidance for school district officials to maintain detailed, up-to-date inventory records for all IT assets including [a]dding new equipment to the inventory [and n]otifying the IT Department when equipment is reassigned, lost, or stolen.”<sup>16</sup> Los Angeles County tasks its “Inventory Staff” to “[c]ollaborate with offices to maintain an accurate Department-wide inventory listing with supporting documentation throughout the year” for lost, stolen, recovered, disposed, and transferred assets.<sup>17</sup>

#### **D. The Chicago Park District risks noncompliance with inventory requirements for IT assets purchased with federal funds**

In June 2022, the City of Chicago committed an initial \$6 million from the Coronavirus State and Local Fiscal Recovery Funds (SLFRF), authorized under the America Rescue Plan Act, to install free wireless internet in the District’s fieldhouses and parks. The U.S. Department of the Treasury requires assets procured with SLFRF to be in compliance with the Uniform Guidance, 2 CFR Part 200, Subpart D, which states:

Regardless of whether equipment is acquired in part or its entirety under the Federal award, the recipient or subrecipient must manage equipment (including replacement equipment) utilizing procedures that meet the following requirements... A physical inventory of the property must be conducted, and the results must be reconciled with the property records at least once every two years.<sup>18</sup>

The IT Department confirmed a subset of its IT assets, i.e., those for the City of Chicago’s Digital Equity Plan, were procured using SLFRF. As discussed above, the IT Department does

---

<sup>14</sup> Chicago Police Department, “Uniform and Property U05-02: Department Equipment and Property Control System,” November 6, 2024, accessed February 24, 2025, <https://directives.chicagopolice.org/#directive/public/6253>.

<sup>15</sup> City of Chicago, “Information Security and Technology Policy,” May 7, 2024, accessed February 24, 2025, <https://www.chicago.gov/content/dam/city/depts/dgs/InformationTechnology/ISTP.pdf>.

<sup>16</sup> New York State Comptroller, “IT Asset Management 2022-MS-2,” March 2023, accessed February 24, 2025, <https://www.osc.ny.gov/files/local-government/audits/2023/pdf/it-asset-management-2022-ms-2.pdf>.

<sup>17</sup> Los Angeles County, “Capital/Non-Capital Assets,” November 24, 2021, accessed February 24, 2025, [https://pubftp.dcfslacounty.gov/Policy/Management%20Directives/007926\\_21-01\\_Capital\\_Non-Capital\\_Assets\\_v2.pdf](https://pubftp.dcfslacounty.gov/Policy/Management%20Directives/007926_21-01_Capital_Non-Capital_Assets_v2.pdf).

<sup>18</sup> Uniform Guidance, “2 CFR 200.313 Equipment,” accessed February 24, 2025, <https://www.ecfr.gov/current/title-2/section-200.313>.

not conduct formal, regular inventories of its IT assets and thus risks noncompliance with these federal inventory requirements.<sup>19</sup>

## Recommendations

1. The IT Department should conduct formal, regular (e.g., annual) inventories of its IT assets, including developing written policies and procedures outlining the steps and designating the entities responsible for the inventory. The Chicago Park District should allocate the resources necessary to perform these inventories. The IT Department should further collaborate with the relevant Chicago Park District entities to develop written policies and procedures for ensuring coordination with the Department when IT assets are procured, lost, stolen, or transferred.
2. The IT Department should consider consolidating its separate, disparate IT asset inventory systems into one main system. To the extent that this is not practical or feasible, the IT Department should create an inventory of its databases to establish which systems include which type of IT assets. The IT Department should also work with staff, contractors, and vendors of these databases to resolve all errors to ensure valid and accurate data.
3. The IT Department should consult with the District's Department of Law to determine whether it is currently in full compliance with the inventory requirements of the American Rescue Plan Act's State and Local Fiscal Recovery Funds.

## Management Response

The IT Department agreed with Recommendation 1, stating between September 2025 and December 2026, the Department will present a plan for an annual districtwide inventory, continue to develop and share written policies and procedures, and work with relevant District entities to “ensure adequate, appropriate, and competent resources are allocated” for the inventory. The Department also noted it will review the City of Chicago's Asset Management as a guideline for planning and executing annual inventories.

The Department agreed in part with Recommendation 2, noting ServiceNow is the “System of Record” for IT assets but also “acknowledge[d] the need to create a project to finalize the consolidation and integration of other asset tracking applications to ServiceNow” between October 2025 and September 2026.

Finally, regarding Recommendation 3, the Department stated that it will consult with the Department of Law by June 2025 to determine compliance with any inventory requirements under the American Rescue Plan Act.

For the IT Department's full response, *see infra* Appendix A.

---

<sup>19</sup> Cursory OIG research did not indicate what consequences, if any, would result from non-compliance with such requirements.

## 2

### **The Chicago Park District risks loss or theft of an estimated half a million dollars of stored IT assets due to insufficient security measures**

The Chicago Park District does not sufficiently secure its IT assets when not in use by District personnel. The District stores its IT assets in two primary locations: in its Headquarters building and in the basement of a park fieldhouse. At the latter location, the IT Department estimates the value of IT assets stored is approximately \$450,000 to \$500,000; however, this value may be greatly higher or lower on any given day due to the number of assets either being delivered as a shipment or deployed to an end user or location. The IT Department requires a second location for assembling and storing IT assets due to limited space within the District's Headquarters building. According to the Department, the District selected the fieldhouse basement, a former woodworking shop, because the Department's Director had an existing "good relationship" with the Park's Area Manager. However, the fieldhouse basement was not designed nor intended for storing IT assets. For example, the fieldhouse does not have a loading dock so the IT Department stated it has to wait for a delivery truck to pull up outside, whereupon the pallets containing the IT assets are broken down in view of the public and the assets are then carried down to the basement. As discussed below, this second location does not have sufficient security measures in place, including policies and physical security, to reduce the risk of loss or theft of these assets.

#### **A. The Chicago Park District does not have policies and procedures requiring the secure storage of its IT assets**

Several governmental agencies have policies requiring that assets, including IT assets, are physically secured. For example:

- The City of Chicago's "Information Security and Technology Policy" notes, "[r]obust physical and environmental controls exist to protect information assets and systems from unauthorized access and safeguard against environmental threats."<sup>20</sup> The policy then requires the following:
  - Establish a security perimeter for all non-public buildings;
  - Establish a process for restricting and monitoring physical access to the applicable facilities;
  - Monitor and review access to the applicable facilities.
- CPS requires that "[e]ach organizational unit accountable official or designee will implement adequate safeguards to prevent loss, damage, or theft of assets. Upon discovery of potential loss, damage, or theft of an asset, the accountable official must

---

<sup>20</sup> City of Chicago, "Information Security and Technology Policy," May 7, 2024, accessed February 24, 2025, <https://www.chicago.gov/content/dam/city/depts/dgs/InformationTechnology/ISTP.pdf>.

document, research and report the potential loss, damage or theft to the asset management team.”<sup>21</sup>

- The New York State Comptroller states, “[t]o safeguard IT assets from loss, theft, or misuse, IT assets should be in a locked and secured area with environmental controls such as smoke detectors, fire alarms and extinguishers, and protection from water damage.”<sup>22</sup>
- Los Angeles County states, “[i]f [an asset] is unassigned and kept to loan out to various employees, the individual that controls the unassigned [asset] is responsible for securing it in a locked area when it is not on loan.”<sup>23</sup> Further, the County’s Board of Supervisors requires each department “to develop a plan describing how all County Information Assets will be protected from physical tampering, damage, theft, or unauthorized physical access. County Information Assets containing Non-Public Information located in unsecured areas shall be secured to prevent physical tampering, damage, theft, or unauthorized physical access.”<sup>24</sup>

Conversely, the District does not have any policies requiring such securing of its IT assets. The District does have two policies pertaining to IT security; however, these policies concern IT security for software, not stored physical IT assets:

- The “Chicago Park District IT Security Policy (Number 1200.028),” dated December 5, 2007, “outlines and defines [the District’s] IT Security Policy” for software and files but does not provide guidance on the secure storage of IT assets.
- The “Department of Information Technology IT Security Policy,” dated October 2012 and marked as “draft,” similarly outlines procedures for software protection but does not contain such guidance for securely storing IT assets.

## **B. The Park fieldhouse does not have sufficient security measures to ensure protection against the loss or theft of its IT assets**

The IT Department risks loss or theft of its stored IT assets at the park fieldhouse due to insufficient security measures. The Department stated both park patrons and unauthorized contractors “wander down” to the fieldhouse basement. For example, on one occasion, staff overheard youth in the hallway outside the basement IT storage room. When questioned, the youth claimed they were searching for the woodworking shop which had been closed for

---

<sup>21</sup> Chicago Public Schools, “Asset and Inventory Management,” March 21, 2024, accessed February 24, 2025, <https://www.cps.edu/sites/cps-policy-rules/policies/400/401/401-9/#:~:text=All%20assets%20are%20to%20be,of%20receipt%20by%20CPS%20staff>.

<sup>22</sup> New York State Comptroller, “IT Asset Management 2022-MS-2,” March 2023, accessed February 24, 2025, <https://www.osc.ny.gov/files/local-government/audits/2023/pdf/it-asset-management-2022-ms-2.pdf>.

<sup>23</sup> Los Angeles County, “Capital/Non-Capital Assets,” November 24, 2021, accessed February 24, 2025, [https://pubftp.dcms.lacounty.gov/Policy/Management%20Directives/007926\\_21-01\\_Capital\\_Non-Capital\\_Assets\\_v2.pdf](https://pubftp.dcms.lacounty.gov/Policy/Management%20Directives/007926_21-01_Capital_Non-Capital_Assets_v2.pdf).

<sup>24</sup> Los Angeles County Board of Supervisors, “Information Security Policy,” July 13, 2004, accessed February 24, 2025, [https://library.municode.com/ca/la\\_county\\_-\\_bos/codes/board\\_policy?nodeId=CH6INTE\\_6.100INSEPO](https://library.municode.com/ca/la_county_-_bos/codes/board_policy?nodeId=CH6INTE_6.100INSEPO).

several years. On another occasion, contractors performing work at the fieldhouse unexpectedly entered the IT Department's basement area and saw laptops in the main area. When the contractors asked about the laptops, the IT Department made the decision to store the laptops in the secure room and install an electronic keypad. Although the IT Department has made attempts to improve the security, such as this electronic keypad, the fieldhouse, generally, and the IT Department space, specifically, presents several security issues:

- The basement is accessible to the public.
- The fieldhouse does not have 24-hour security.
- The hallway to the IT Department's space is locked only with a padlock and is left open during normal work hours (see Figure 2, below).

**FIGURE 2: ENTRANCE TO THE IT DEPARTMENT'S SPACE IN THE PARK FIELDHOUSE BASEMENT**



Source: OIG site visit.

Accordingly, the IT Department's space in the fieldhouse does not align with best practices. The City of Chicago states:

[S]ensitive facilities should have a staffed reception area to control access to the main entry of the facility and appropriate controls to access secondary entrances. For facilities without a staffed reception area, the perimeter should

be controlled via access controls on doors and windows, and doors and windows must be always locked.<sup>25</sup>

Additionally, as noted above, the New York State Comptroller states that IT assets should be “in a locked and secured area,” which is echoed by the Los Angeles County policy.<sup>26</sup>

### **C. The Chicago Park District risks noncompliance with safeguarding regulations for IT assets purchased with federal funds**

As discussed in Finding 1, the IT Department procured a subset of its IT assets for the City of Chicago's wireless internet initiative using SLFRF and the U.S. Department of the Treasury requires assets procured with SLFRF to be in compliance with the Uniform Guidance, 2 CFR Part 200, Subpart D, which states,

Regardless of whether equipment is acquired in part or its entirety under the Federal award, the recipient or subrecipient must manage equipment (including replacement equipment) utilizing procedures that meet the following requirements... A control system must be in place to ensure safeguards for preventing property loss, damage, or theft. Any loss, damage, or theft of equipment must be investigated. The recipient or subrecipient must notify the Federal agency or pass-through entity of any loss, damage, or theft of equipment that will have an impact on the program.<sup>27</sup>

The IT Department stores these wireless assets, such as the routers which have an approximate value of \$2,000 each, at its satellite location in the fieldhouse basement. Like the federal inventorying requirement, the District risks noncompliance with this federal safeguarding requirement for these IT assets.

## **Recommendations**

4. The IT Department should work with the District to securely store its IT assets by ensuring any storage location has the appropriate security measures in place for secure storage, including restricted access by unauthorized personnel.
5. The IT Department should develop and implement a formal policy outlining the protocols for safeguarding IT assets.

---

<sup>25</sup> City of Chicago, “Information Security and Technology Policy,” May 7, 2024, accessed February 24, 2025, <https://www.chicago.gov/content/dam/city/depts/dgs/InformationTechnology/ISTP.pdf>.

<sup>26</sup> New York State Comptroller, “IT Asset Management 2022-MS-2,” March 2023, accessed February 24, 2025, <https://www.osc.ny.gov/files/local-government/audits/2023/pdf/it-asset-management-2022-ms-2.pdf>; Los Angeles County, “Capital/Non-Capital Assets,” November 24, 2021, accessed February 24, 2025, [https://pubftp.dcms.lacounty.gov/Policy/Management%20Directives/007926\\_21-01\\_Capital\\_Non-Capital\\_Assets\\_v2.pdf](https://pubftp.dcms.lacounty.gov/Policy/Management%20Directives/007926_21-01_Capital_Non-Capital_Assets_v2.pdf).

<sup>27</sup> Uniform Guidance, “2 CFR 200.313 Equipment,” accessed February 24, 2025, <https://www.ecfr.gov/current/title-2/section-200.313>.

6. The IT Department should consult with the District's Department of Law to determine whether it is currently in full compliance with the safeguarding requirements of the American Rescue Plan Act's State and Local Fiscal Recovery Funds.

## Management Response

The IT Department agreed with Recommendation 4 stating between June 2025 and October 2026, the Department will work with the District's Department of Facilities Management to "identify and secure adequate storage facilities for IT assets," including potentially finding a different location than the park fieldhouse.

The Department further agreed with Recommendation 5, stating by December 2025, it will develop and implement a formal policy for safeguarding IT assets, but noted a policy may be contingent on the "successful execution" of other recommendations, including Recommendation 4.

Finally, the Department agreed with Recommendation 6, stating it will consult with the Department of Law by June 2025 to determine compliance with the safeguarding requirements of the American Rescue Plan Act.

For the IT Department's full response, *see infra* Appendix A.

## Appendix A: The Department of Information Technology's Management Response

Chicago Park District Office of Inspector General – Management Response Form  
 Audit of the Chicago Park District's Information Technology Asset Management 24-0280

<b>Recommendation 1</b>	
<p>The IT Department should conduct formal, regular (e.g., annual) inventories of its IT assets, including developing written policies and procedures outlining the steps and designating the entities responsible for the inventory.</p> <p>The Chicago Park District should allocate the resources necessary to perform these inventories.</p> <p>The IT Department should further collaborate with the relevant Chicago Park District entities to develop written policies and procedures for ensuring coordination with the Department when IT assets are procured, lost, stolen, or transferred.</p>	
<b>Department Response</b>	Agree <input checked="" type="checkbox"/> Agree, in part <input type="checkbox"/> Disagree <input type="checkbox"/>
<b>Notes on Department Response</b>	
<b>Department's Proposed Corrective Action (if in agreement with Recommendation)</b>	
<ul style="list-style-type: none"> <li>• Department of Information Technology (DoIT) will present a plan for IT's annual districtwide inventory which includes timeline and resources.</li> <li>• DoIT will continue to develop and share written policies and procedures detailing IT Asset Management (ITAM) and IT Asset Disposition (ITAD) environments, along with associated resources.</li> <li>• DoIT will work with relevant Chicago Park District entities to ensure adequate, appropriate, and competent resources are allocated. Furthermore, IT will review and consider the City of Chicago (CoC) Asset Management environment as a guideline for planning and execution.</li> </ul>	
<b>Implementation Time Frame</b>	September 2025 – December 2026
<b>Responsible Party(ies) for Implementation</b>	DoIT, currently our managed IT services provider is SDI Presence (SDI)
<b>Recommendation 2</b>	
<p>The IT Department should consider consolidating its separate, disparate IT asset inventory systems into one main system.</p> <p>To the extent that this is not practical or feasible, the IT Department should create an inventory of its databases to establish which systems include which type of IT assets.</p> <p>The IT Department should also work with staff, contractors, and vendors of these databases to resolve all errors to ensure valid and accurate data.</p>	
<b>Department Response</b>	Agree <input type="checkbox"/> Agree, in part <input checked="" type="checkbox"/> Disagree <input type="checkbox"/>
<b>Notes on Department Response</b>	
<p>The System of Record is ServiceNow. Other systems monitoring connectivity and performance may also include inventory of assets in production. DoIT acknowledges the need to create a project to finalize the consolidation and integration of other asset tracking applications to ServiceNow.</p>	
<b>Department's Proposed Corrective Action (if in agreement with Recommendation)</b>	

Chicago Park District Office of Inspector General – Management Response Form  
 Audit of the Chicago Park District's Information Technology Asset Management 24-0280

DoIT will continue to work with staff, contractors, and vendors to consolidate disparate IT Asset Management systems into a cohesive ITAM environment that addresses all touchpoints identified.	
<b>Implementation Time Frame</b>	October 2025 – September 2026
<b>Responsible Party(ies) for Implementation</b>	DoIT, currently our managed IT services provider is SDI Presence (SDI)

<b>Recommendation 3</b>	
The IT Department should consult with the District's Department of Law to determine whether it is currently in full compliance with the inventory requirements of the American Rescue Plan Act's State and Local Fiscal Recovery Funds.	
<b>Department Response</b>	Agree <input checked="" type="checkbox"/> Agree, in part <input type="checkbox"/> Disagree <input type="checkbox"/>
<b>Notes on Department Response</b>	
DoIT acknowledges the need to consult with the District's Department of Law to ensure full compliance with the inventory requirements.	
<b>Department's Proposed Corrective Action (if in agreement with Recommendation)</b>	
DoIT will consult with the District's Department of Law to understand the current inventory requirements of the American Rescue Plan Act's State and Local Fiscal Recovery Funds.	
<b>Implementation Time Frame</b>	June 2025
<b>Responsible Party(ies) for Implementation</b>	DoIT

<b>Recommendation 4</b>	
The IT Department should work with the District to securely store its IT assets by ensuring any storage location has the appropriate security measures in place for secure storage, including restricted access by unauthorized personnel.	
<b>Department Response</b>	Agree <input checked="" type="checkbox"/> Agree, in part <input type="checkbox"/> Disagree <input type="checkbox"/>
<b>Notes on Department Response</b>	
DoIT acknowledges the need to secure IT assets.	
<b>Department's Proposed Corrective Action (if in agreement with Recommendation)</b>	
DoIT will work with the District's Facility Management Department to identify and secure adequate storage facilities for IT assets. Potential location – McCormick Place.	
<b>Implementation Time Frame</b>	June 2025 – October 2026
<b>Responsible Party(ies) for Implementation</b>	Facility Management, DoIT

<b>Recommendation 5</b>	
The IT Department should develop and implement a formal policy outlining the protocols for safeguarding IT assets.	
<b>Department Response</b>	Agree <input checked="" type="checkbox"/> Agree, in part <input type="checkbox"/> Disagree <input type="checkbox"/>
<b>Notes on Department Response</b>	
DoIT agrees, depending on the successful implementation of recommendation 4.	
<b>Department's Proposed Corrective Action (if in agreement with Recommendation)</b>	

Chicago Park District Office of Inspector General – Management Response Form  
 Audit of the Chicago Park District's Information Technology Asset Management 24-0280

DoIT will develop and implement a formal policy outlining the protocols for safeguarding IT assets. This requirement may have a dependency on the successful execution of recommendations #1, #3, and #4.	
<b>Implementation Time Frame</b>	December 2025
<b>Responsible Party(ies) for Implementation</b>	DoIT

<b>Recommendation 6</b>	
The IT Department should consult with the District's Department of Law to determine whether it is currently in full compliance with the safeguarding requirements of the American Rescue Plan Act's State and Local Fiscal Recovery Funds.	
<b>Department Response</b>	Agree <input checked="" type="checkbox"/> Agree, in part <input type="checkbox"/> Disagree <input type="checkbox"/>
<b>Notes on Department Response</b>	
DoIT acknowledges the need to be in full compliance with the safeguarding requirements.	
<b>Department's Proposed Corrective Action (if in agreement with Recommendation)</b>	
DoIT will consult with the District's Department of Law to understand the current safeguarding requirements of the American Rescue Plan Act's State and Local Fiscal Recovery Funds.	
<b>Implementation Time Frame</b>	June 2025
<b>Responsible Party(ies) for Implementation</b>	DoIT



---

The mission of the Office of Inspector General (OIG) is to:

- Investigate allegations of fraud, waste and abuse or misconduct by Chicago Park District employees, Board members, contractors, agents, or volunteers
- Monitor the Park District's compliance with the Employment Plan's rules governing hiring and other employment actions
- Conduct audits to enhance the effectiveness and efficiency of the District, ensure compliance with legal requirements, policies, and best practices, and mitigate risks which could impair the mission of the District.

It is the duty of every employee, Board member, agent, and contractor of the District to report any fraud, mismanagement, waste of funds or resources, abuse of authority, conflicts of interest, ethical violations or other improper act by another involving District business or assets. The Park District Code prohibits retaliation for reporting to, cooperating with, or assisting the Inspector General.

---

Submit a report to the Office of Inspector General through one of the following options:

- Online: <https://chicagoparkdistrict.i-sight.com/external/case/new>
- By telephone: (312) 742-3333 (Confidential Hotline)
- By fax: (312) 742-9505
- In writing: Chicago Park District Office of Inspector General, 740 N. Sedgwick St., Suite 300, Chicago, IL 60654
- In person: 740 N. Sedgwick St., Suite 300, Chicago, IL 60654