togetherforbetter

AUDIT REPORT

Clark County's Implementation of CIS Critical Security Control 1: Inventory and Control of Enterprise Assets, Needs Improvement

April 2026

ANGELA DARRAGH, CPA, CISA, CFE
AUDIT DIRECTOR
CLARK COUNTY AUDIT DEPARTMENT

Clark County's Implementation of CIS Critical Security Control 1: Inventory and Control of Enterprise Assets, Needs Improvement

Audit Executive Summary

April 2026

Background

On June 5, 2019, Senate Bill 302 was approved in Nevada (*with an effective date of January 1, 2021.*) This bill amended NRS 603A.210 to require government agencies, acting as data collectors, to comply with Center for Internet Security (CIS) Controls or National Institute of Standards and Technology (NIST) for the purpose of electronic information security framework.

Clark County selected CIS as its security framework. CIS Controls are a set of cybersecurity best practices designed to help organizations defend against common cyber threats. They provide safeguards that organizations can implement to protect their systems, networks, and data.

CIS Control 1, *Inventory and Control of Enterprise Assets*, focuses on actively managing all enterprise assets – including end-user devices, mobile and portable devices, network equipment, Internet-of-Things devices, and servers connected physically, virtually, or remotely. It also includes controls to identify unauthorized or unmanaged assets.

Clark County must also meet additional requirements for securing data including the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rule, Payment Card Industry (PCI) standards, and Criminal Justice Information System (CJIS) standards.

What We Found

- Clark County uses an active and passive asset discovery tool to identify assets on the network. However, there isn't a single, complete and detailed enterprise asset inventory list.
- Not all devices that are connected to the County network are following Clark County Information Technology Security Policy.
- No formal process has been established to address unauthorized assets.

Recommendations

- Create, maintain and regularly update a detailed list of enterprise assets connected to the county network.
- Implement a process to address unauthorized assets.
- Disallow access to the county secured network on non-compliant devices.

togetherforbetter

Why We Did This Audit

The objective of this audit was to review Clark County's implementation of CIS 1*, Inventory and Control of Enterprise Assets*, and determine whether Clark County:

- Maintains a detailed enterprise asset inventory.
- Uses a passive and active asset discovery tool.
- Uses system logs to update the enterprise's asset inventory.
- Addresses unauthorized assets.

For more information about this or other audit reports go to clarkcountynv.gov/audit or call (702) 455-3269.

Audit Team

Angela Darragh, Director
Cynthia Birney, Audit Manager
Felix Luna, Principal Auditor
Christopher Hui, Information Systems Auditor
Joshua Cheney, Information Systems Auditor

Audit Committee

Commissioner Michael Naft
Commissioner April Becker
Commissioner William McCurdy II

About the Audit Department

The Audit Department is an independent department of Clark County reporting directly to the County Manager. The Audit Department promotes economical, efficient, and effective operations and combats fraud, waste, and abuse by providing management with independent and objective evaluations of operations. The Department also helps keep the public informed about the quality of Clark County Management through audit reports.

You can obtain copies of this report by contacting:

Clark County Audit Department
PO Box 551120
Las Vegas, NV 89155-1120
(702) 455-3269

CountyAuditor@ClarkCountyNV.gov

Or download and view an electronic copy by visiting our website at:

https://www.clarkcountynv.gov/audit/Pages/AuditReports.aspx

Table of Contents

Background

On June 5, 2019, Senate Bill 302 was approved in Nevada and the effective date is January 1, 2021. This bill amended NRS 603A.210 to require government agencies, acting as data collectors, to comply with Center for Internet Security (CIS) Controls[1] or National Institute of Standards and Technology (NIST) for the purpose of electronic information security framework.

Clark County selected CIS as its security framework. CIS controls are a set of cybersecurity best practices designed to help organizations defend against common cyber threats. They provide safeguards that organizations can implement to protect their systems, networks, and data.

CIS Control 1, *Inventory and Control of Enterprise Assets*, focuses on actively managing all enterprise assets – including end-user devices, mobile and portable devices, network equipment, Internet-of-Things devices, and servers connected physically, virtually, or remotely. It also includes controls to identify unauthorized or unmanaged assets.

NRS 603A.210 Security Measures

2. "If a data collector is a governmental agency and maintains records which contain personal information of a resident of this State, the data collector shall, to the extent practicable, with respect to the collection, dissemination and maintenance of those records, comply with the current version of the CIS Controls as published by the Center for Internet Security, Inc. or its successor organization, or corresponding standards adopted by the National Institute of Standards and Technology of the United States Department of Commerce."

The Federal Bureau of Investigation's Internet Crime Complaint Center Annual Report for 2024 estimates $16 billion in losses due to cybercrime[2].

Clark County must also meet additional requirements for securing data including the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rule, Payment Card Industry (PCI) standards, and Criminal Justice Information System (CJIS) standards.

[1] The current version of the CIS Critical Security Controls is Version 8.1, released in June 2024.
[2] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Objective

The objective of this audit was to review Clark County's implementation of CIS 1*, Inventory and Control of Enterprise Assets*, and determine whether Clark County:

- Maintains a detailed enterprise asset inventory.
- Uses a passive and active asset discovery tool.
- Uses system logs to update the enterprise's asset inventory.
- Addresses unauthorized assets.

Conclusions

We found that the Information Technology Department (IT) has implemented most of CIS 1 and uses several tools, such as passive and active discovery, to stay aware of all enterprise assets connected to the County network. However, they do not maintain this information in a single, actively managed inventory. Asset management practices could also be strengthened to ensure a consolidated and consistently updated inventory.

Findings are rated based on a risk assessment that takes into consideration the circumstances of the current condition including compensating controls and the potential impact on reputation and customer confidence, safety and health, finances, productivity, and the possibility of fines or legal penalties. It also considers the impact on confidentiality, integrity, and availability of data.

2 Total Audit Findings

2 High Risk Findings

High risk findings indicate an immediate and significant threat to one or more of the impact areas.

0 Medium Risk Findings

Medium risk findings indicate the conditions present a less significant threat to one or more of the impact areas. They also include issues that would be considered high if one control is not working as designed.

0 Low Risk Findings

Low risk findings are typically departures from best business practices or areas where effectiveness, efficiency, or internal controls can be enhanced. They also include issues that would be considered high or medium risk if alternate controls were not in place.

Findings, Recommendations, and Responses

Finding #1 – IT Does Not Maintain a Detailed Enterprise Asset Inventory

The Clark County Information Technology Department (IT) performs an annual review of the Comptroller's inventory list as part of the County's annual inventory process[3]. The Comptroller's inventory list does include most devices such as desktop computers, laptops and servers that are connected to the county; it does not include all devices that are connected to the county network.

While IT is aware of all other devices that are connected through the county network from other tools, it is not part of an all-encompassed list that is being actively maintained. This creates the risk that inactive or rogue devices may remain connected to the network for long periods.

Also, due to not having an enterprise asset list, currently there is no process in place to use logs[4] to update the enterprise asset inventory.

This is part of the requirements identified within CIS Control 1 as well as other standards.

CIS Control 1: Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

> Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate.
>
> This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review

[3] NRS 354.625 requires all local governments to establish and maintain adequate property and equipment records along with adequate inventory controls. The statute also requires that such property, equipment and inventory records clearly indicate specific ownership. The Clark County Comptroller's Office has been designated to supervise the establishment and maintenance of property records and inventory control. An annual physical inventory is conducted to determine compliance.

[4] Logging refers to the process of recording specific events, such as a user logging in or accessing a file, while monitoring involves reviewing those logs in real time or at regular intervals to detect patterns, trends, or irregularities

and update the inventory of all enterprise assets bi-annually, or more frequently.

CIS Control 1: Safeguard 1.4: Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory

Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.

See Appendix B for relevant information technology frameworks and standards related to asset inventory.

Recommendations

1. Create, maintain and regularly update a detailed list of enterprise assets connected to the county network.

2. Utilize DHCP logging on DHCP servers or Internet Protocol (IP) address management tool to update enterprise asset inventory in accordance with CIS Control 1.4

Management Action Plan

While most end-point end user devices are managed through existing processes and protocols, Clark County IT is developing a centralized, up-to-date enterprise asset inventory repository that includes all devices connected to the County network. IT will integrate existing discovery tools, implement weekly updated using privileged access management logs, document ownership and approval status for each device, and establish recurring review processes. This effort will reduce the risk of unauthorized or inactive devices remaining on the network and ensure alignment with CIS Control 1. The tentative completion date for this extensive effort is June 2028. IT will provide annual updates on this effort as part of its annual report to the IT Executive Steering Committee in the County Manager's Office by June 30th until the completion of the effort.

Finding #2 – Not All Devices Connected to the Network Comply with the County's IT Security Policy, and No Formal Process Exists to Address Unauthorized Assets

We found that Clark County Information Technology has controls that block unauthorized devices from accessing internal county network, but there are some improvements that could be made for wireless connections.

We also found that there are software and non-formal procedures that address unauthorized network assets; however, a formal procedure is not in place. Therefore, it is possible for non-compliant devices to remain on Clark County's network.

Several information technology standards, that the County is required to follow, provide guidance on managing unauthorized assets.

UNAUTHORIZED ASSET

An unauthorized asset is any hardware device connected to or used within an organization's network without official approval, documentation, or security vetting. These assets pose a security risk.

CIS Control 1 - Inventory and Control of Enterprise Assets safeguard 1.2: Address Unauthorized Assets:

Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

Clark County Information Technology Security Policy 1 (TD 1)

5. Remote Network Access.
County-owned, employee-owned, and third-party vendor desktop and laptop computers can be used to remotely access County Computing Systems and Networks as follows:

a. Access. Access to County Computing Systems and Networks via the Internet or unsecured wireless networks requires the use of VPN – LAN-to-LAN and client-based VPN with Managed PKI Services.

b. Approval. Approval to remotely access County Computing Systems and Networks requires the approval of the responsible Elected or Appointed Clark County Department Head and the Clark County CIO.

c. Configurations. Personal computers that are used for remote access to County Computing Systems and Networks shall be configured as follows:

1) Remote PC user sessions must authenticate with strong authentication (one time passwords or digital certificates).

2) Remote PCs must have installed and be operationally configured with antivirus, anti-malware, and personal firewalls.

3) Patches for the operating systems and applications and updates for Web Browsers, email clients, instant

messaging clients, antivirus software, anti-malware, and personal firewalls shall be current.

4) Email clients must be configured to favor security over functionality. Email clients should be configured to: Prevent automatic loading or remote email images; limit mobile code execution; have the default message reading and sending format set to plain text; disable automatic previewing and opening of email messages; and enable spam filtering.

5) Web browsers must be configured to favor security over functionality. Web browsers should be configured to restrict web browser cookies, block pop up windows, enable phishing filters, and run with the least privileges as possible. In addition, unneeded browser plug-ins should be removed and website passwords should not allow passwords to be recalled automatically.

6) Remote PC user sessions to County Computing Systems and Networks must be protected from unauthorized physical access during the period of connection through the use of the client operating systems screen saver utility with a low wait set and on resume password enabled.

Non-compliant devices connected to the county network allow for potentially compromised devices to have direct access to Clark County's network.

Because of the security sensitivities involved with these findings, we have communicated them separately, in greater detail to the department.

Recommendations

1. Implement a process to address unauthorized assets.
2. Implement weekly reviews for unauthorized assets and document the review.
3. Disallow access to the county secured network on non-compliant devices.
4. Ensure all devices connected to the county secured network meet TD1 requirements.

Management Action Plan

While Clark County has existing processes to authorize access to the County network, Clark County IT will create a formal process to identify and remediate unauthorized or non-compliant devices on the network by implementing certificate-based authentication on authorized devices that will be administered by multiple endpoint

management technologies. This formal process and regular review cycles will ensure all connected devices meet TD1 requirements and apply these controls consistently across both wired and wireless accounts and devices. IT will complete this effort by January 31st, 2027.

Appendix A: Audit Scope, Methodology, and GAGAS Compliance

Scope

The audit covered the period from July 2, 2025, through March 1, 2026. We considered processes in place as of January 1, 2026. The last day of field work was March 1, 2026.

Methodology

To accomplish our objectives, we conducted a preliminary survey where we gathered background information; interviewed management, reviewed written policies and procedures and identified risks relevant to our audit objectives.

Based on the risks identified during our preliminary survey, we developed an audit program and then performed the following procedures:

- Completed a walkthrough of operations pertaining to management of enterprise assets to determine compliance with CIS1.
- Interviewed and held meetings with staff to determine the comprehensiveness of enterprise asset management and usage of asset discovery tools.
- Obtained documentation regarding the tools used for dynamic Host Configuration Protocol (DHCP) and Internet Protocol (IP) address management.
- Used professional judgement to select a sample of 525 decommissioned devices and cross referenced with current active devices to ensure they are no longer active on the network.
- Verified the existence of an active asset discovery tool and confirmed usage.

While some samples selected were not statistically relevant, we believe they are sufficient to provide findings for the population as a whole.

Our review included an assessment of internal controls in the audited areas. Any significant findings related to internal control are included in the detailed results.

Standards Statement

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence

obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Our department is independent per the GAGAS requirements for internal auditors.

Appendix B: Relevant Frameworks and Standards to Information Technology Asset Inventory

There are established standards and frameworks related to maintaining an accurate information technology asset inventory. These include those provided by the Center for Internet Security's (CIS) Critical Security Controls Version 8.1, the Criminal Justice Information Services (CJIS) Security Policy Version 5.9.5 and 6, the Health Insurance Portability and Accountability Act (HIPAA) and the Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals (HPH CPGs).

The Center for Internet Security, Control 1: Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

> Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate.
>
> This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

Criminal Justice Information Services (CJIS) Security Policy Version 5.9.5 (07/09/2024)[5] Criminal Justice Information Services (CJIS) Security Policy Version 6 (12/27/2024)

> CM-8 SYSTEM COMPONENT INVENTORY
> a. Develop and document an inventory of system components that:
> 1. Accurately reflects the system;
> 2. Includes all components within the system;
>
> (1) SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATION AND REMOVAL
> Update the inventory of system components as part of component installations, removals, and system updates.
>
> Discussion: Organizations can improve the accuracy, completeness, and consistency of system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and documented. System updates include hardware, software, and firmware components.

[5] The Federal Bureau of Investigation (FBI) released CJIS Security Policy 6.0 in December 2024. Both the current version and prior version include verbiage related maintaining an accurate information technology asset inventory.

Health Insurance Portability and Accountability Act (HIPAA), Regulation Text, 2013

§ 164.310 Physical safeguards.

(d)(2)(iii) Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible, therefore.

Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals (HPH CPGs)

ID 11 - Goals: Asset Inventory

Identify known, unknown (shadow), and unmanaged assets to more rapidly detect and respond to potential risks and vulnerabilities