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

Audit Department

April 2026

togetherforbetter

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 follow CIS Controls or NIST for electronic information security.
- 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.

Background *(Continued)*

- CIS Control 1 requires active management of all enterprise assets, including end-user devices, mobile and portable devices, network equipment, IoT devices, and servers, and includes identifying unauthorized or unmanaged assets.
- Clark County must also comply with additional data-security requirements, including HIPAA Privacy and Security Rules, PCI standards, and CJIS standards.

Objectives

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.

Conclusion

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

2 Total Audit Findings

High Risk

1. IT Does Not Maintain a Detailed Enterprise Asset Inventory
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

Finding 1 – No Detailed Enterprise Asset Inventory
(High Risk)

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; however, 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 to update the enterprise asset inventory.

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

Finding 1 – No Detailed Enterprise Asset Inventory
(High Risk) *Continued*

Recommendations:

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

Finding 1 – No Detailed Enterprise Asset Inventory
(High Risk) *Continued*

Management Response:

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 (High Risk)

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.

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 (High Risk) *Continued*

Recommendations:

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

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 (High Risk) *Continued*

Management Response:

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 administer 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.

togetherforbetter