State of Nevada
Governor's Finance Office
Division of Internal Audits

Audit Report

Governor's Technology Office

*****

Information Technology Infrastructure Oversight

****

Improving oversight of information technology infrastructure will strengthen cybersecurity, improve asset visibility and management, reduce costs, and enhance governance.

DIA Report No. 26-01
July 9, 2026

EXECUTIVE SUMMARY
Governor's Technology Office
Information Technology Infrastructure Oversight

Introduction ..... page 1

Objective: Improve information technology security, management, and oversight.

Collaborate with Federal Agencies to Proactively Test Information Technology Systems and Strengthen Cybersecurity Practices ..... page 2

The Governor's Technology Office (GTO) relies on in-house cybersecurity testing and third-party software to conduct cybersecurity scans and assessments, and agency-specific testing is largely request-driven rather than governed by a mandatory, recurring testing schedule. Collaborating with federal agencies to proactively test information technology (IT) systems and strengthen cybersecurity practices will improve awareness of any existing and potential vulnerabilities of Executive Branch IT systems. Leveraging no-cost cybersecurity services offered by the Cybersecurity and Infrastructure Security Agency (CISA), including vulnerability scanning, network penetration testing, and web application scanning, will provide independent, external validation of existing security controls and align GTO's practices with federal and other authoritative guidance.

Coordinate with the Information Technology Advisory Board to Evaluate the Information Technology Review Threshold Set in Statute and Submit a Bill Draft Request to Lower the Threshold, if Advised ..... page 8

Statute requires GTO to review applications of information systems with an estimated development cost of $50,000 or more, while other IT procurements are not required to receive technical review and can avoid review when misclassified as non-IT related or purchased through certain procurement methods. Coordinating with the Information Technology Advisory Board to evaluate the IT review threshold and submitting a Bill Draft Request to lower the threshold will improve visibility over Executive Branch agency IT procurements. Lowering the threshold will strengthen cybersecurity, reduce the risk of unreviewed technology entering the state's information systems, and improve IT infrastructure oversight.

Revise and Enforce the Software Inventory Policy, Compile and Analyze Inventory, and Coordinate with the Purchasing Division to Lower Software Acquisition Costs ..... page 12

GTO's Software Inventory and Control Standard requires Executive Branch agencies to maintain annual software inventories; however, the requirement has not been enforced, agencies do not submit software inventories to GTO, and GTO does not collect or analyze this information, limiting visibility over software deployed. As a result, GTO cannot readily identify unauthorized, unsupported, duplicative, or technically similar software solutions, nor can it effectively evaluate opportunities for coordinated purchasing and enterprise-wide licensing to reduce Executive Branch IT expenditures.

Requiring agencies to submit standardized software inventories and compiling the results into a consolidated inventory will improve cybersecurity oversight, support identification of duplicative and redundant software purchases, and enable enterprise-wide licensing and strategic sourcing opportunities to reduce software acquisition costs. GTO should create and distribute a software inventory template that includes a required field for inputting software licensing information needed by the State Controller's Office to comply with GASB Statement No. 96 reporting requirements.

Request Funding for Information Security Training Positions ..... page 18

GTO training responsibilities are largely performed as secondary duties by IT professionals and other technical staff, requiring highly skilled personnel to divert time from primary operational and security functions to deliver training. Having dedicated training staff will improve statewide cybersecurity readiness by providing consistent instruction on information security requirements, technology policies, incident response procedures, and emerging threats, while freeing up IT professionals to focus on core responsibilities. IT employment growth in Nevada is estimated to increase by 4.2% in 2026, the highest percentage increase among all states, and Executive Branch IT positions have been designated as hard to fill. Other western states have established centralized cybersecurity training programs to improve compliance, reduce risk, and strengthen implementation of statewide technology and security requirements. Funding two information security training positions will free-up IT professionals to perform primary duties and improve cybersecurity.

Appendix A ..... page 24
Scope and Methodology, Background, and Acknowledgments

Appendix B ..... page 26
Response and Implementation Plan

Appendix C ..... page 30
Timetable for Implementing Audit Recommendations

INTRODUCTION

At the direction of the Executive Branch Audit Committee, the Division of Internal Audits (DIA) conducted an audit of the Governor's Technology Office (GTO). The audit focused on information technology infrastructure oversight. DIA reviewed GTO's asset management policies, continuity of operations plan, advisory board oversight, cybersecurity testing and assessment practices, and statewide training capacity. The audit scope and methodology, background, and acknowledgments are included in Appendix A.

DIA's audit objective was to develop recommendations to:

- ✓ Improve information technology security, management, and oversight.

Governor's Technology Office Response and Implementation Plan

DIA provided draft copies of this report to GTO for review and comment. DIA considered GTO's comments in preparation of this report; GTO's response is included in Appendix B. In its response, GTO accepted the recommendations. Appendix C includes a timetable to implement the recommendations.

NRS 353A.090 requires within six months after the final report is issued to the Executive Branch Audit Committee, the DIA Administrator shall evaluate the steps GTO has taken to implement the recommendations and shall determine whether the steps are achieving the desired results. The Administrator shall report the six-month follow-up results to the committee and GTO.

The following report (DIA Report No. 26-01) contains DIA's *findings, conclusions*, and *recommendations*.

Improve Information Technology Security, Management, and Oversight

The Governor's Technology Office (GTO) can improve information technology (IT) security, management, and oversight by:

- Collaborating with federal agencies to proactively test IT systems and strengthen cybersecurity practices;
- Coordinating with the Information Technology Advisory Board to evaluate the information technology review threshold set in statute and submitting a Bill Draft Request to lower the threshold, if advised;
- Revising and enforcing the software inventory policy, compiling and analyzing inventory, and coordinating with the Purchasing Division to lower software acquisition costs; and
- Requesting funding for information security training positions.

Improving IT security, management, and oversight will: strengthen cybersecurity and reduce risk to the state from cyber attacks; improve visibility and management of Executive Branch IT assets; reduce costs; and enhance governance by eliminating duplicative and unreviewed technology investments and by consistently enforcing technology security requirements.

Approximately $40 million of current and planned IT purchases have been identified as being duplicative to IT solutions currently being provided by GTO. Government-wide software agreements negotiated by the U.S. General Services Administration have provided discounts ranging between 4% and 10% through consolidated purchasing. Using GSA-achieved savings rates as a benchmark, the state could reduce future costs by approximately $1.6 million to $4 million by consolidating $40 million of identified duplicative IT purchases.

Collaborate with Federal Agencies to Proactively Test Information Technology Systems and Strengthen Cybersecurity Practices

The Governor's Technology Office (GTO) should collaborate with federal agencies to proactively test information technology (IT) systems and strengthen cybersecurity practices. Collaborating with federal agencies to proactively test Executive Branch IT systems will improve GTO's awareness of existing and potential vulnerabilities affecting IT systems. Using IT services offered by federal agencies, including external security assessments and network penetration testing, will better align GTO's cybersecurity practices with federal cybersecurity guidance and recognized best practices.

GTO Does Not Leverage External Cybersecurity Testing Offered by Federal Agencies

GTO does not leverage external cybersecurity testing offered by federal agencies such as the U.S. Department of Homeland Security's Cybersecurity Infrastructure and Security Agency (CISA) or the National Guard. CISA offers a variety of cybersecurity testing and cyber hygiene services to states. Services offered by CISA that could benefit the state include vulnerability scanning, network penetration testing, and web application scanning.[1] The costs of these services are incurred by the federal government and not charged to states.

The National Guard, through State Guard units, can conduct comprehensive network vulnerability assessments, configuration reviews, and cyber tabletop exercises.[2] The costs of using State Guard units to conduct these assessments, reviews, and exercises would be incurred by the state. Funds were not appropriated in the 2025-2027 Legislatively Approved Budget to pay for services offered by the State Guard. This audit report does not recommend incurring the costs of using the cybersecurity services offered by the State Guard because services are offered by CISA and its federal service partners at no cost to the state.

GTO Relies on In-House Cybersecurity Testing and Third-Party Software to Secure Networks and Technology

GTO relies on in-house cybersecurity testing and third-party software to conduct scans and assessments to secure state networks and technology at the enterprise level. GTO offers in-house security services to Executive Branch agencies that include vulnerability scanning, penetration testing, incident triage and response coordination, and security oversight and guidance at the agency level. GTO's services are provided to agencies through a service-by-request model rather than a mandatory testing plan. As a result, agencies do not receive periodic independent testing unless testing is requested, testing is required before a new system or network is initiated, or testing is otherwise performed through an agency-specific effort. GTO's use of in-house resources and third-party software is an accepted and cost-effective practice, but the approach lacks periodic independent, external validation. GTO's cybersecurity approach can be improved by mandating external recurring penetration testing, vulnerability scanning, and threat assessments are conducted with a frequency and scope that is based on cost effectiveness. Leveraging CISA's no-cost network penetration testing and cyber hygiene services will improve GTO's cybersecurity practices.

---

[1] Vulnerability scanning and penetration testing serve related but distinct purposes. Vulnerability scanning is a recurring process used to identify known weaknesses, missing software patches, configuration issues, or exposed services. Penetration testing is a deeper assessment that attempts to determine whether identified weaknesses can be exploited and what impact exploitation may have on systems or data.

[2] Cyber tabletop exercises are simulations where military personnel, civilian government agencies, and critical infrastructure partners walk through hypothetical cyber attack scenarios in a low-stress, no-risk setting. The exercises test incident response plans and coordination procedures without impacting actual networks.

Executive Branch Agency Cybersecurity Testing Services Are Request-Driven

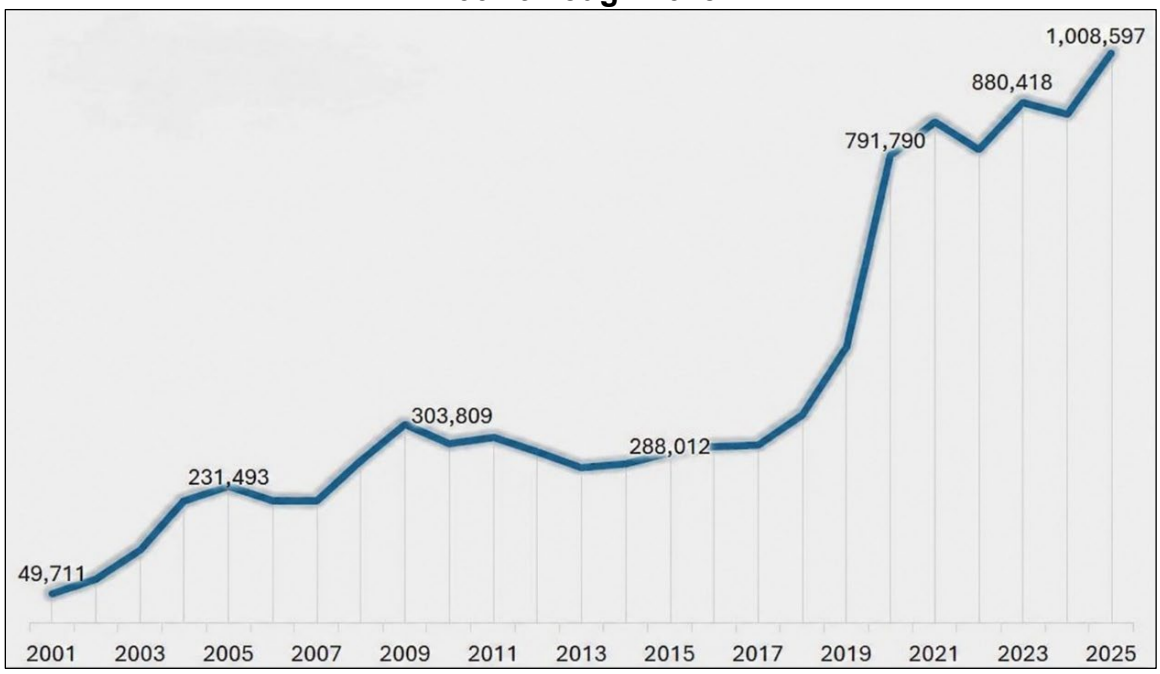
Executive Branch agency cybersecurity testing services offered by GTO are largely request-driven rather than being governed by a mandatory, recurring testing schedule. GTO conducts enterprise-level cybersecurity testing and offers vulnerability scanning and penetration testing through its security assessment services. Agency-specific testing occurs upon request through the GTO Service Desk or when conducted within the agency. State Information Security Program Policy 100 requires vulnerability scanning and penetration testing before a new IT system or network is initiated, but it does not require recurring testing after implementation. GTO's security policies, standards, and procedures do not establish a mandatory schedule for agency cybersecurity testing, and GTO does not audit agency cybersecurity testing to ensure agency systems are tested periodically.

FBI Data Demonstrates Sharp Increase in Cyber Threats Worldwide and in Nevada

Federal Bureau of Investigation (FBI) Internet Crime Complaint Center data indicates cyber threats rose significantly during the COVID-19 pandemic, followed by a sharp increase in 2025. FBI data identified 880,418 cyber threats in 2023 and 1,008,597 in 2025, an increase of approximately 15%. Exhibit I shows the increase in cyber threats reported worldwide from 2001 to 2025.

Exhibit I

Cyber Threats Reported to FBI
2001 through 2025



Source: FBI Internet Crime Report, 2025.

Nevada Among Highest in Nation for Cyber Threats Reported Over Past Three Years

Nevada is among the highest states in the nation for cyber threats reported per capita over the past three years. Cyber threats reported to FBI climbed from a rate of 310 per 100,000 residents in 2023 to 407 in 2025, an increase of approximately 31%. The increase suggests Nevada residents are increasingly the target of cyber threats. On a per capita basis, Nevada ranked third in the nation for number of cyber threats reported in 2025. Exhibit II shows cyber threats reported per capita in Nevada from 2023 to 2025.

Exhibit II

Cyber Threats Reported in Nevada 2023 through 2025

Year	Cyber Threats Reported Per 100K Residents in Nevada	Nevada's National Rank[a]
2025	407	3
2024	328	4
2023	310	3

Source: FBI Internet Crime Reports from 2023 through 2025.
Notes: [a] Rank 1 = most cyber threats reported per capita.

State Was the Target of a Cyber Attack

The state was the target of a cyber attack executed on August 24, 2025. GTO restored business-critical services within one week including payroll continuity, state accounting system functionality, and access to law enforcement information systems. GTO recovered approximately 90% of data during the recovery period, exceeding a public sector recovery rate of 58%.[3] Recovery occurred within 28 days, on par with a public sector recovery benchmark of 28 days.[4] GTO effectively recovered from the cyber attack; however, the attack demonstrated the continued importance of proactively testing and assessing IT systems for threats.

Recent Federal Actions Prioritized Supporting Statewide Testing Efforts

Recent federal actions increased emphasis on cybersecurity and support for state and local governments. In March 2026, the White House released its Cyber Strategy for America which states the federal government will galvanize the role of state, local, tribal, and territorial authorities in national cybersecurity efforts. In September 2025, CISA implemented a revised approach for supporting state and local governments that emphasizes providing direct federal assistance,

[3] Sophos, Puja Mahendru, *The State of Ransomware in State and Local Government 2022*, September 30, 2022, sophos.com.
[4] Comparitech, Rebecca Moody, *On Average*, *Government Offices Suffer a Month of Downtime After Ransomware Attacks*, updated March 18, 2025, comparitech.com.

cybersecurity expertise, no-cost cybersecurity services, and grant funding. Leveraging federal expertise can complement, rather than replace, GTO's existing cybersecurity services.

Authoritative Guidance Supports External Testing

Authoritative guidance supports external testing. National Institute of Standards and Technology (NIST) calls for an external penetration testing agent or team, and CISA guidance similarly supports regular, proactive vulnerability scanning and penetration testing to identify exploitable weaknesses before threat actors do.[5]

NIST Guidance Establishes Expectations for Proactive External Testing

NIST guidance establishes expectations for proactive external testing as part of a broader cybersecurity assessment program. NIST recommends penetration testing be conducted at an organization-defined frequency by an external agent or team free from perceived or actual conflicts of interest with the systems being tested. NIST guidance states that regularly scheduled vulnerability scanning, combined with periodic penetration testing, can help prevent attacks and reduce the impact of successful attacks.[6]

CISA Cybersecurity Performance Goals Support Testing

CISA guidance supports penetration testing as part of a proactive cybersecurity program. CISA Cross-Sector Cybersecurity Performance Goals designate a voluntary baseline of high-priority security practices. CISA's vulnerability management guidance states that scanning and penetration testing are proactive activities that should be scheduled, which supports establishing an independent testing schedule for state systems.[7]

GTO Standards Require Security Testing and Periodic Evaluation

GTO's security framework requires some cybersecurity testing and evaluation activities for Executive Branch IT systems. State Information Security Program Policy 100 requires state systems and networks to have vulnerability scans and penetration tests before a new system or network is initiated.

GTO's Security Evaluations Standard S.2.05.01 requires agencies to conduct a security evaluation upon installation and periodic security evaluations to confirm continued protection and compliance as technologies, security threats, and state

[5] NIST 800-53 Revision 5, control CA-8 and CISA Cross-Sector Cybersecurity Performance Goals 2.0.
[6] NIST SP 800-115.
[7] CISA, *Cyber Resilience Review Resource Guide, Volume 4: Vulnerability Management*.

policies and standards change. Together, these requirements support a testing plan that includes initial testing and recurring evaluation, but do not require external testing.

Independent Testing Reduces Risk

Independent testing reduces risk by proactively identifying exploitable weaknesses and providing objective assurance over the effectiveness of existing security controls. GTO completes scanning of Executive Branch agency systems using tools and services that include Microsoft Defender, Accenture, Tenable, Microsoft Sentinel, and other tools, services, and methods not disclosed in this audit report. Collaborating with federal agencies such as CISA to proactively test and assess Executive Branch IT systems will provide the external analysis needed to further strengthen cybersecurity.

Conclusion

GTO should collaborate with federal partners such as CISA to strengthen cybersecurity by conducting recurring independent vulnerability assessments, penetration testing, and cyber hygiene reviews of Executive Branch information technology systems. Leveraging no-cost federal cybersecurity services will provide objective validation of existing security controls, improve identification of vulnerabilities before they can be exploited, align state practices with federal guidance and industry best practices, and enhance GTO's ability to manage increasing cyber threats.

Recommendation

1. Collaborate with federal agencies to proactively test information technology systems and strengthen cybersecurity practices.

Coordinate with the Information Technology Advisory Board to Evaluate the Information Technology Review Threshold Set in Statute and Submit a Bill Draft Request to Lower the Threshold, if Advised

The Governor's Technology Office (GTO) should coordinate with the Information Technology Advisory Board to evaluate the information technology (IT) review threshold set in statute and submit a Bill Draft Request (BDR) to lower the threshold, if advised. Coordinating with the Information Technology Advisory Board to evaluate the IT review threshold and lowering the threshold, if advised, will improve GTO's visibility over agency IT assets, reduce the risk of IT procurements not being reviewed by being misclassified or structured below the review threshold, strengthen cybersecurity, and enhance IT infrastructure oversight.

IT Review Threshold Set in Statute Limits GTO's Oversight

The IT review threshold set in statute limits GTO's oversight of Executive Branch agency IT procurements. NRS 242.171(2) requires GTO to review applications of information systems with an estimated developmental cost of $50,000 or more.[8] Most other IT procurements valued under $50,000 are not required to be reviewed, which limits GTO's visibility of some Executive Branch IT assets. Visibility is necessary to support GTO oversight. NRS 242.115 and NRS 242.171(2) assign GTO IT governance responsibilities, including developing policies and standards for information services and reviewing applications of information systems that meet the statutory review threshold. These duties require sufficient visibility into agency IT procurements prior to acquisition.

Cyber Attack Demonstrated Limits on GTO's Visibility of Executive Branch IT Assets

The August 2025 cyber attack demonstrated limits on GTO's visibility of Executive Branch IT assets. Certain IT assets were not known to GTO until after the attack occurred and were identified through response and recovery activities. According to GTO's After Action Report, the attack disrupted some state systems for up to 28 days and required coordination across more than 60 state agencies, underscoring the importance of GTO's visibility over agency IT assets. The lack of awareness of certain IT assets before the attack occurred increased the difficulty of coordinating the response, recovery, and risk management efforts. The cyber attack underscores the importance of GTO receiving information about agency technology procurements, including those under $50,000 and IT assets already procured and in service, before those assets can affect statewide operations and cybersecurity or have an impact on future recovery efforts.

[8] State Administrative Manual Section 1618(D) requires cloud-based technology procurements of any value to be reviewed by GTO.

Agency IT Procurements Avoid Review through Contract Misclassification

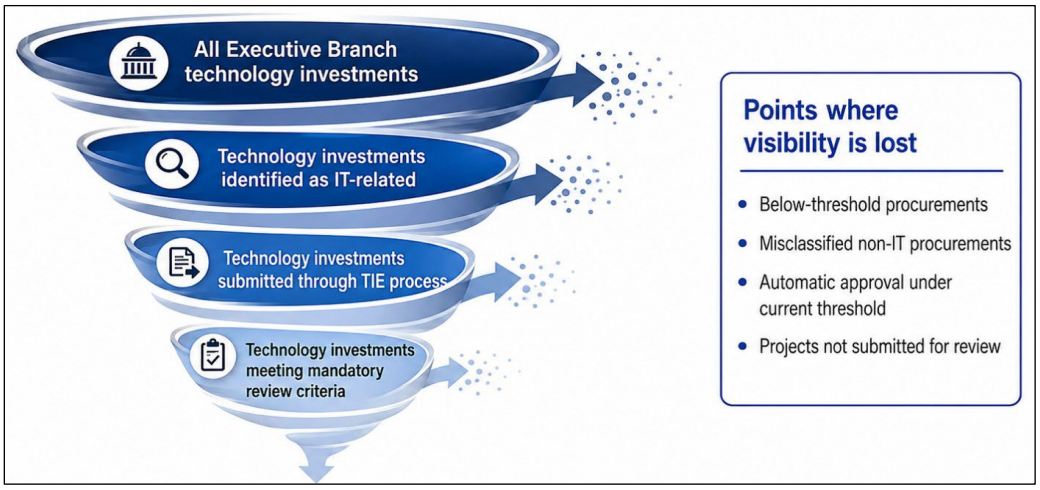
Agency IT procurements avoid GTO review when misclassified as non-IT-related in the Contract Entry and Tracking System or when the value is structured below the statutory review threshold. Agencies can avoid GTO review by not checking the "IT related" checkbox on contract summaries and not submitting a Technology Investment Evaluation (TIE) memorandum. If these errors are not detected, GTO review is circumvented.

Executive Branch agency IT purchases of $50,000 or more receive GTO technical review. Procurements below the current statutory review threshold are approved without technical review or bypass GTO review entirely, depending on the procurement method. Agency IT purchases made using a Procurement Card can bypass GTO review. Likewise, IT purchases made using a purchase order outside of the state's electronic procurement system (Nevada ePro) can bypass GTO review. IT purchases below the $50,000 threshold made using Nevada ePro require IT approval, but, in practice, the approval is applied without conducting technical review.

Agencies are required to submit a TIE memorandum to GTO for an IT procurement of $50,000 or more. The GTO-approved TIE memorandum is required to be attached to the contract. The intent of the TIE review process is to proactively identify assets that will be introduced into the Executive Branch's technology portfolio, identify potential risks, identify opportunities to consolidate purchases, and avoid redundant solutions. GTO's visibility over agency IT procurements that fall under the mandatory review threshold is limited, reducing GTO's ability to identify redundant solutions and determine whether proposed technology could negatively impact cybersecurity. Exhibit III shows how some IT procurements can avoid GTO review.

Exhibit III

IT Procurements Can Avoid GTO Review



Source: DIA analysis of TIE and IT procurement processes.

Statute Requires ITAB to Advise GTO Concerning Issues Relating to IT

Pursuant to statute, the Information Technology Advisory Board (ITAB) is required to advise GTO concerning issues relating to IT, including development, acquisition, consolidation, and integration, in addition to IT policies, planning, and standards.[9] Statute also requires ITAB to review GTO's strategic plans periodically and proposed budgets before submission.[10] Regular ITAB meetings are necessary to support effective oversight. NRS 242.123 requires ITAB to meet at least once every three months to provide a formal and recurring forum to carry out its statutory advisory duties and evaluate technology governance issues in a timely manner. ITAB is the appropriate advisory board to evaluate the statutory IT review threshold because statute assigns ITAB an advisory role over statewide IT issues.

ITAB evaluation of the $50,000 threshold should take into consideration cybersecurity exposure that can result from no-cost or low-cost hardware and software that does not currently trigger GTO review under a cost-based threshold. No-cost and low-cost hardware and software can allow unintended access to state data, connect to state systems, create unsupported software risk, or introduce vulnerabilities that warrant GTO review before being deployed. Exhibit IV shows ITAB members as of June 2026 and the statutory basis for each member's service.

Exhibit IV

ITAB Members
As of June 2026

ITAB Members	Statutory Basis to Serve on ITAB
David Tyburski (Chair)	One of two members representing the IT industry[a]
Loren Young	One of two members representing the IT industry[a]
Raymond Medeiros	One of three members engaged in IT or IT security representing a city or county in Nevada[a]
Christopher Turner	One of three members engaged in IT or IT security representing a city or county in Nevada[a]
Unfilled	One of three members engaged in IT or IT security representing a city or county in Nevada[a]
Timothy Galluzi	GTO Chief
Hillery Pichon	Attorney General's designee
Senator Rochelle Nguyen	Member of the Senate Standing Committee on Finance[b]
Assemblymember Natha Anderson	Member of the Assembly Standing Committee on Ways and Means[c]

Source: GTO website and NRS 242.122.
Notes: [a] Appointed by the Governor.
[b] Appointed by the Majority Floor Leader of the Senate.
[c] Appointed by the Speaker of the Assembly.

[9] NRS 242.124 Information Technology Advisory Board: Duties; powers.
[10] Ibid. Statute also authorizes ITAB to review agency IT plans and certain IT issues upon request.

DIA review of ITAB meeting materials and the ITAB webpage on GTO's website indicate ITAB did not meet at least once every three months as required by statute between October 2024 and September 2025.[11] ITAB is the advisory forum for IT governance matters, including the adequacy of the IT review threshold. GTO should request the ITAB chair schedule a meeting and agendize an evaluation of the IT review threshold set in statute at the next meeting to allow GTO time to submit a BDR to lower the threshold, if advised.

NIST and CISA Guidance Reinforce the Need for Technology Visibility

National Institute for Standards and Technology (NIST) supply chain guidance states that agencies are exposed to cybersecurity risks through software and services acquired, deployed, used, and managed including third-party and open-source software. NIST cybersecurity framework recommends visibility over technology that exists or is being introduced into the environment.

Cybersecurity Infrastructure and Security Agency (CISA) asset inventory guidance recommends organizations create and maintain asset inventories because organizations cannot adequately secure assets that have not been identified and documented. CISA describes visibility over asset inventories as foundational to risk reduction and cybersecurity defense. Visibility over agency IT procurements is necessary to maintain awareness of Executive Branch IT infrastructure. GTO should be informed of proposed technology procurements before technology is acquired, connected to IT systems, or granted access to Executive Branch data. Oversight is important for technology acquisitions, including no-cost and low-cost applications of information systems, because cybersecurity risks stem from factors such as access permissions, software vulnerabilities, and supply chain risks, not the cost of the technology.

Conclusion

GTO should coordinate with ITAB to evaluate whether the current statutory IT review threshold provides adequate oversight of Executive Branch technology procurements and, if advised, submit a Bill Draft Request to lower the threshold. Strengthening IT oversight in the agency procurement process would improve visibility over agency IT assets, strengthen cybersecurity awareness, reduce the risk of unreviewed technology entering the state environment, and support more cost effective procurement of Executive Branch information technology assets.

Recommendation

2. Coordinate with the Information Technology Advisory Board to evaluate the information technology review threshold set in statute and submit a Bill Draft Request to lower the threshold, if advised.

[11] NRS 242.123 Information Technology Advisory Board: Meetings; compensation.

Revise and Enforce the Software Inventory Policy, Compile and Analyze Inventory, and Coordinate with the Purchasing Division to Lower Software Acquisition Costs

The Governor's Technology Office (GTO) should revise and enforce the software inventory policy to ensure Executive Branch agencies submit annual software inventories using a standardized template that includes information useful to GTO, the Department of Administration Purchasing Division, and the State Controller's Office. GTO should compile and analyze the software inventory to identify duplicative purchases and opportunities to coordinate with the Purchasing Division to lower software acquisition and licensing costs. Enforcing a standardized annual software inventory process will improve GTO's awareness of existing Executive Branch agency software, identify opportunities to leverage the state's purchasing power to achieve economies of scale for software acquisition, and provide the State Controller's Office with subscription-based software information necessary for financial reporting purposes.

GTO Lacks Visibility of Software Purchased and Used by Agencies

GTO lacks visibility of software being purchased by Executive Branch agencies and software currently deployed on state information systems. GTO's Software Inventory and Control Standard S.6.02.01 requires Executive Branch agencies to establish and maintain annually a software inventory to track and control applicable software installations. The standard also requires agencies to conduct an annual software audit and inventory of libraries and computer systems to determine whether the agency is complying with applicable software license agreements and with federal, state, and agency standards and procedures. The Software Inventory and Control Standard does not require agencies to submit a copy of the inventory to GTO. Accordingly, agencies do not submit software inventories to GTO for review and GTO cannot compile the inventory results into a consolidated inventory.

Some Agencies May Be Unaware of Annual Software Inventory Requirements

Some agencies may be unaware of annual software inventory requirements mandated by Software Inventory and Control Standard S.6.02.01. The requirement to maintain a software inventory is not communicated to agency heads through an All Agency Memorandum or by agency Information Security Officers (ISOs), and the requirement has not been enforced by GTO. The Software Inventory and Control Standard was last revised on December 31, 2020. Discussions with an ISO supporting multiple agencies disclosed the ISO was unaware of the software inventory requirement, but was aware of agency physical asset (personal property) inventory requirements.

Statute and SAM Require Annual Reconciliation and Reporting of Agency Physical Personal Property Inventory

Statute, State Administrative Manual (SAM) Section 0326, and All Agency Memorandums issued annually by the Purchasing Division require Executive Branch agencies to conduct an annual physical inventory of agency personal property and to reconcile the results with inventory records maintained in the state's accounting system. SAM 0326(B)(1) requires agencies to maintain an inventory of computer equipment, including laptops, desktops, and servers, regardless of acquisition value. NRS 333.220 requires the Chief of the Purchasing Division to maintain inventory records of physical property in the possession of agencies.

Physical information technology (IT) assets, such as laptops and servers, are subject to annual inventory requirements. Agency submission of physical inventory records, and the compilation of physical inventory records by the Purchasing Division, are enforced annual requirements. GTO's annual software inventory requirement has not been enforced, and the Software Inventory and Control Standard does not mandate agency reporting of software inventories or GTO compilation of the inventories. Limited software visibility increases cybersecurity risk because GTO cannot readily determine whether software used by agencies is authorized, supported, or compliant with GTO requirements. Lack of visibility over software being used by agencies limits the Executive Branch's ability to identify opportunities to consolidate purchases to reduce costs or eliminate duplicative or technically similar software purchases.

Some Agencies Purchased Software Already Provided by GTO and Some Agencies Purchased Technically Similar Software Solutions

Some agencies purchased software already provided by GTO. For example, the Nevada Department of Transportation (NDOT) purchased approximately 2,000 Microsoft Office licenses. GTO does not purchase or manage Microsoft Office licenses on behalf of NDOT; instead, NDOT purchases and maintains its own licenses. The staff resources required to support and administer the Microsoft Office platform separately from GTO are duplicative. GTO estimates the cost of this duplicative spend to be $220,000 per fiscal year.

Some agencies purchased technically similar software solutions from different software creators. For example, GTO procured Microsoft Defender to provide, among other things, integrated endpoint threat analysis and protection to Executive Branch agencies. Some Executive Branch agencies, such as the Aging and Disability Services Division, the Department of Conservation and Natural Resources, the Department of Motor Vehicles, the Department of Veterans Services, and the Division of Public and Behavioral Health purchased software that provides technically similar endpoint threat analysis and protection from other companies such as Carbon Black, PDQ Connect, Forcepoint ONE, and HP Wolf

Security. GTO lacks visibility over software necessary to identify when the same or technically similar software is being purchased and when the software is being purchased from different vendors.

Agencies Can Purchase the Same Software from Different Vendors

Executive Branch agencies can purchase the same software and software licenses from different vendors. For example, Adobe software products and licenses can be purchased directly from Adobe using a Procurement Card, through CDW Government LLC using a purchase order, through SHI International Corporation using a statewide contract, or from other vendors not on a statewide contract. The Purchasing Division mandates agencies purchase software using a statewide contract when available, such as the current statewide contract with SHI International Corporation for Adobe licenses, but agencies can circumvent the requirement.

The Purchasing Division can see agency purchases made through the state's electronic procurement system (Nevada ePro), but agencies can use a Procurement Card or an agency purchase order to circumvent Nevada ePro. Additionally, Nevada ePro does not have a record of all agency software purchases made prior to the time of agency roll-out in Nevada ePro.[12] GTO and the Purchasing Division lack complete visibility over agency software purchases and existing software used. An annual software inventory can close the gap in software visibility.

Individual Software Licenses from the Same Vendor Can Be Consolidated and Purchased in Bulk to Reduce Costs

Executive Branch agencies are procuring individual, or small quantities of, software licenses from the same vendor that could otherwise be consolidated and purchased in bulk on an enterprise-level contract. For example, licenses for the identity verification platform ID.me have been purchased by the Department of Employment, Training, and Rehabilitation (DETR) on a contract extended through June 30, 2025. The current contract renewal has been expanded into an enterprise-level agreement that will serve multiple Executive Branch agencies, resulting in immediate savings of approximately $40,000 for DETR, plus a fixed cost shared by the remaining contract participants. Visibility of all software purchased by Executive Branch agencies will promote opportunities to consolidate future purchases using statewide, enterprise-level contracts.

[12] Agencies were not rolled out concurrently, and Nevada ePro did not exist prior to 2018, meaning procurements made prior to the existence of Nevada ePro or the individual agency's roll-out date (beginning in February 2019) are not captured.

GTO is Responsible for Promoting Secure, Economical, and Non-Duplicative Use of Technology Resources

GTO is responsible for promoting the secure and economical use of information systems and reducing unnecessary proliferation of technology pursuant to NRS 242.071. The Chief Information Officer must establish policies, standards, and practices governing state information systems pursuant to NRS 242.111. Statutory responsibilities support GTO's authority to maintain and enforce a comprehensive software inventory and to use inventory information to identify cybersecurity risks, reduce duplicative software acquisitions, and pursue more cost-effective statewide purchasing, licensing, and administration of software resources.

NASPO, GAO, and NIST Support Enterprise-Wide Analysis of Software Purchasing and Licensing

The National Association of State Procurement Officials (NASPO) Procurement Guide for Executive and Legislative Leadership advises that strategic sourcing relies on the analysis of purchasing and expenditure data to achieve cost savings, improve efficiency, manage supply risks, and increase the value derived from procurement activities.

The U.S. Government Accountability Office (GAO) reported that decentralized procurement practices can limit an organization's ability to leverage its collective purchasing power. According to GAO, strategic sourcing helps organizations achieve cost savings and operational efficiencies by shifting procurement activities from numerous independent purchases to coordinated, enterprise-wide purchasing strategies that aggregate demand and increase negotiating leverage.[13]

The National Institute of Standards and Technology's (NIST) Cybersecurity Framework 2.0 recommends that organizations maintain inventories of software, services, systems, and other technology assets and manage those assets throughout their life cycles. NIST further recommends that organizations identify, validate, and document vulnerabilities associated with those assets.

To support effective IT asset management, NIST advises organizations to regularly review and update inventories, record changes resulting from installations, removals, and system updates, and detect unauthorized hardware, software, and firmware components. NIST also recommends maintaining a centralized inventory repository, noting that centralized asset information improves accountability, increases operational efficiency, and enables organizations to more quickly identify compromised components and responsible personnel.[14]

[13] GAO-12-919 *Strategic Sourcing: Improve and Expanded Use Could Save Billions in Annual Procurement Costs*, September 20, 2012.
[14] NIST SP 800-53 Revision 5.

Maintaining and analyzing consolidated software inventory information can provide the visibility necessary to identify opportunities for enterprise-wide licensing, coordinated procurement, and the reduction of duplicative software purchases.

Software Inventory Will Support
GASB Statement No. 96 Compliance

A software inventory will support compliance with Governmental Accounting Standards Board (GASB) Statement No. 96. GASB establishes accounting and financial reporting requirements for subscription-based information technology arrangements (SBITAs), including the recognition and reporting of certain subscription assets and liabilities. Compliance with these requirements is contingent upon agencies identifying qualifying software subscriptions and maintaining accurate information regarding subscription terms and costs.

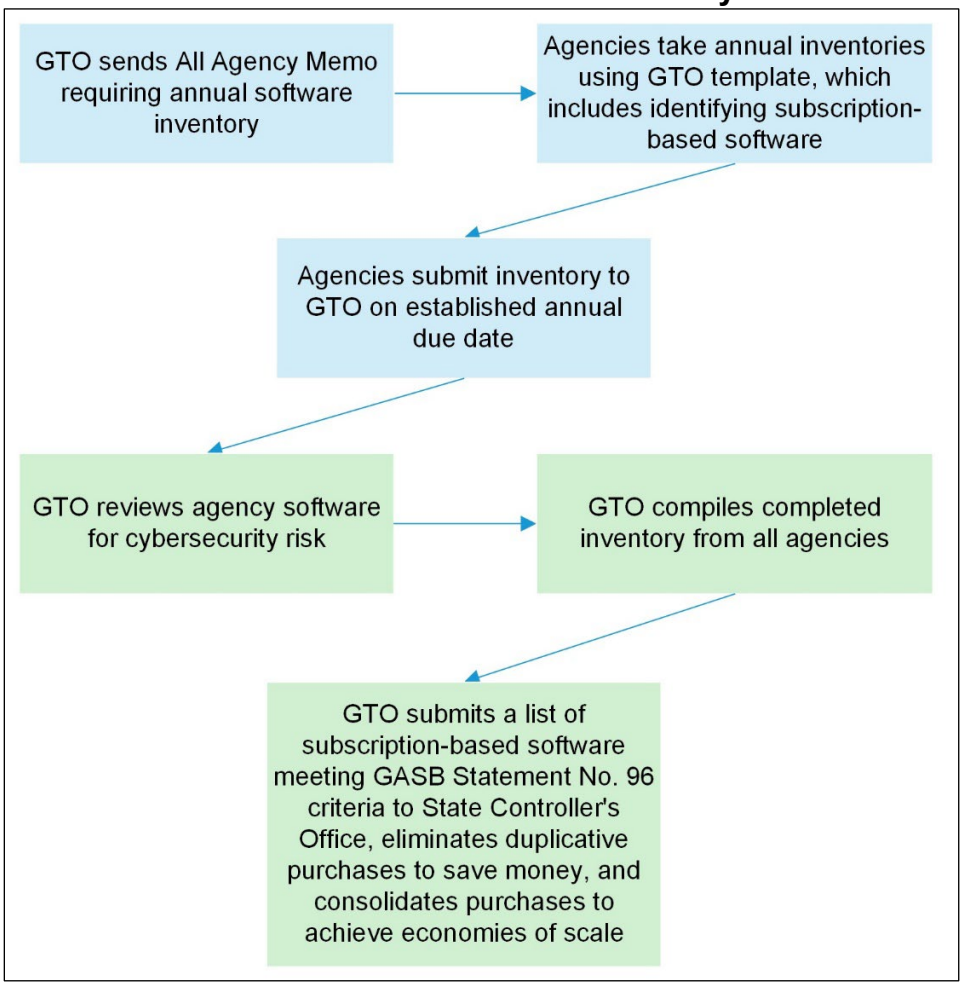
Revising the software inventory standard and reporting process to include information required for compliance with GASB Statement No. 96 will help the State Controller's Office identify reportable SBITAs and efficiently compile the information necessary for annual financial reporting. Executive Branch agencies would complete an annual inventory by:

- Using a standardized inventory reporting template provided by GTO;
- Identifying software that is subscription-based;
- Submitting the inventory by a GTO-mandated due date; and
- Maintaining the inventory when new software is added or when existing software is updated or removed from agency information systems.

Exhibit V shows the recommended annual software inventory process.

Exhibit V

Recommended Annual Software Inventory Process



Source: DIA proposed annual software inventory process.

Conclusion

GTO should revise and enforce its software inventory requirements to ensure Executive Branch agencies annually report software assets using a standardized inventory process and template. Compiling and analyzing software inventory information will improve visibility over software deployed, strengthen cybersecurity by identifying unauthorized or unsupported software, identify opportunities to reduce costs through coordinated purchasing and enterprise licensing agreements, reduce duplicative software acquisitions, and provide information necessary to support statewide financial reporting requirements.

Recommendation

3. Revise and enforce the software inventory policy, compile and analyze inventory, and coordinate with the Purchasing Division to lower software acquisition costs.

Request Funding for Information Security Training Positions

The Governor's Technology Office (GTO) should request funding for two information security training positions. If funding is approved, the positions should be responsible for developing a centralized training program to coordinate, deliver, and track standardized training for Information Security Officers (ISOs), agency information technology (IT) staff, GTO staff, and Executive Branch agency staff with access to state information systems. The information security training positions should focus primary training efforts on information security, compliance, and IT implementation requirements. Dedicated information security trainers would improve information security awareness, support policy implementation efforts, and improve statewide readiness in the event of a cyber attack.

Other Western States Prioritize Information Security Training

Other western states prioritize information security training. In Nevada, training is not required at the enterprise or agency level on state information systems, virtual machine environments, or state-specific IT applications. Common software application training, such as Microsoft Office applications, is not made available to employees through GTO. GTO uses an online training platform, KnowBe4, to provide employees with self-paced, instructorless information security training. GTO requires Executive Branch employees to annually complete approximately one hour of training that covers the following topics:

- Security awareness;
- Handling and sharing sensitive information;
- Reporting security incidents;
- Artificial intelligence; and
- Multi-factor authentication.

A DIA survey of ten western states found some states offer more robust IT and cybersecurity training, which generally includes centralized aspects of role-based instruction, curriculum development, scheduling, agency outreach, compliance reinforcement, and program measurement, in addition to recurring security awareness training. Some states require statewide technology and security policy training for agency personnel using state information systems or who are responsible for implementing and enforcing IT policies. For example, Washington requires both basic and role-based security training. Some states, such as Colorado and Utah, mandate statewide training as part of their central security service model.

Exhibit VI shows states included in the survey and a description of IT training functions.

Exhibit VI

IT Training Functions in Western States

State	IT Training Functions
Arizona	Strategic Enterprise Technology Office provides courses covering cybersecurity best practices and requires awareness training before access.
California	California Department of Technology's Office of Professional Development provides a training framework, academies, a training guide for building programs, and an annual survey of IT training needs from Department Training Officers and Coordinators. California Department of Technology hosts a cybersecurity boot camp for Information Security Officer and security office roles.
Colorado	Governor's Office of Information Technology provides awareness and training programs for securing state assets, such as incident response planning and training through tabletop cyber exercises.
Idaho	Office of Information Technology Services facilitates cybersecurity training enterprise-wide.
Montana	State Information Services Division has a Training Coordinator position dedicated to employee development and end-user training, improving performance, creating in-house training, supporting orientation, and developing employee skills.
New Mexico	Office of Cybersecurity coordinates cybersecurity awareness and training programs.
Oregon	Enterprise Information Services has a Training Coordinator position responsible for building, maintaining, and measuring the statewide program. Provides annual training; monthly training; phishing simulations; metrics; outreach; compliance support; long-range planning; tailored course development; and vendor coordination.
Utah	Division of Technology Services provides agencies with security awareness training alongside compliance, risk, vulnerability, incident-management, and forensic services.
Washington	Washington Technology Solutions requires basic training for users and training aligned to user roles, provides enhanced awareness modules and newsletters, and offers technical training to agency IT staff.
Wyoming	Enterprise Technology Services employs Cyber Risk Culture Strategists who emphasize comprehensive employee training to identify and mitigate risks.

Source: DIA survey of IT training functions in western states.

GTO Staff Training Responsibilities Are Performed as Secondary Duties

GTO staff training responsibilities are performed as secondary duties. GTO does not have dedicated training staff responsible for IT and information security training. In the absence of dedicated training staff, development of common training materials, onboarding for new ISOs and agency IT staff, recurring refresher training, communication of policy changes, and follow-up instruction are performed as secondary duties that compete with primary operational duties and priorities. The absence of centralized, dedicated training staff increases the risk that Executive Branch agencies will receive inconsistent, incomplete, untimely, or insufficient training on IT and cybersecurity requirements. As a result, agencies may be less aware of applicable policies, standards, procedures, and emerging cybersecurity risks, increasing the likelihood of noncompliance, inconsistent implementation of IT or information security requirements, and avoidable security weaknesses.

Auxiliary training is generally provided by GTO on an ad hoc basis by the GTO process owner, such as the IT Professional responsible for administering the specific process. For example, GTO staff developed Technology Investment Evaluation (TIE) process guidelines and made staff available to provide agencies with instruction and training on the TIE process. Agencies that fail to engage knowledgeable GTO staff administering the TIE process may encounter issues that delay the TIE approval process.

Nevada Projected to Lead Nation in IT Employment Growth and Demand for IT Employees is Increasing

Nevada is projected to lead the nation in IT employment growth in 2026, and demand for IT employees is increasing statewide. IT employment in Nevada is projected to increase by 4.2%, the highest percentage increase among all states.[15] Las Vegas IT employment is projected to increase by 4% in 2026, resulting in 1,529 new positions.

Executive Branch IT positions have been designated as hard-to-fill. As such, efforts have been made to decrease vacancies through actions such as special one-grade pay increases authorized by the Legislature for IT roles such as: IT Manager, IT Professional, and IT Technician. IT positions are hard to fill due to a shortage of candidates and “skills mismatch” where an abundance of entry-level candidates exist but there is a shortage of enterprise-experienced candidates.

Training provided by dedicated training staff will free up critical IT staff, such as IT Professionals, to perform primary operational duties, rather than secondary training duties.

[15] Computing Technology Industry Association, *State of the Tech Workforce 2026*, March 2026.

Cyber Attack After Action Report Identifies Staff Training and Awareness as Critical Factors in Mitigating Risk

The August 2025 cyber attack After Action Report identifies cultivating staff training and awareness as critical factors in mitigating cyber risk. The cyber attack, which disrupted state systems and required a coordinated response at both the enterprise and agency levels, reinforced the operational importance of ensuring GTO and agency IT staff possess current knowledge of cybersecurity threats, incident response procedures, state technology policies and standards, and respective roles and responsibilities during cybersecurity events. Dedicated training positions will enable GTO to provide consistent onboarding, recurring training, and timely communication of evolving cybersecurity requirements and emerging threats across Executive Branch agencies.

Statutes Assign GTO Responsibility for Establishing and Administering Centralized Requirements and Implementation

Statutes assign GTO responsibility for establishing and administering centralized technology and information security requirements and supporting consistent implementation across Executive Branch agencies. NRS 242.115 requires GTO to develop Executive Branch information systems policies and standards, guidelines, and procedures for procurement of information systems.

NRS 242.111 requires GTO's Chief to adopt standards necessary to ensure the security of the information systems of agencies subject to GTO's authority. NRS 242.101 supports the staffing necessary to carry out these statewide responsibilities. Collectively, these provisions contemplate a governance structure in which GTO develops requirements and provides the coordination necessary to promote consistent implementation across Executive Branch agencies.

GTO Policy Framework Supports Centralized Approach to Training and Awareness

GTO policy framework further supports a centralized approach to training and awareness. State Information Security Program Policy 100 requires Executive Branch agencies to comply with statewide information security requirements and assigns the Office of Information Security responsibility for establishing, implementing, administering, and overseeing the State Information Security Program. The policy also requires the Office of Information Security to develop guidance, assist agencies in establishing security programs, standards, procedures, and plans, and support security awareness and training activities.

GTO standards likewise establish training, communication, and coordination responsibilities that extend across agencies. The State Security Committee Charter Standard provides a State Information Security Committee to facilitate

statewide coordination on information security policies, standards, problems, and issues.[16]

The ISO Roles and Responsibilities Standard requires agencies to appoint one or more ISOs responsible for the development, implementation, management, training, and enforcement of policies and standards regarding the security of information and information technologies.[17] The standard also requires ISOs to coordinate an Information Security Awareness Program, while GTO's Security Awareness and Training Program Standard, S.6.17.01, requires periodic briefings, continual reinforcement, timely orientation training, and annual reinforcement of security awareness training. These requirements depend on GTO's ability to develop, deliver, and coordinate consistent training and guidance across Executive Branch agencies.

Dedicated Training Resources Will Help Reduce Risk

Dedicated training resources will help reduce risk to the state by ensuring GTO staff, agency ISOs, and agency IT personnel receive consistent and timely instruction regarding statewide technology governance, information security requirements, and operational responsibilities. When training is performed as a secondary duty, delivery of training, communication of policy changes, and reinforcement of security expectations must compete with primary operational priorities, increasing the risk that information is communicated inconsistently or not delivered in a timely manner.

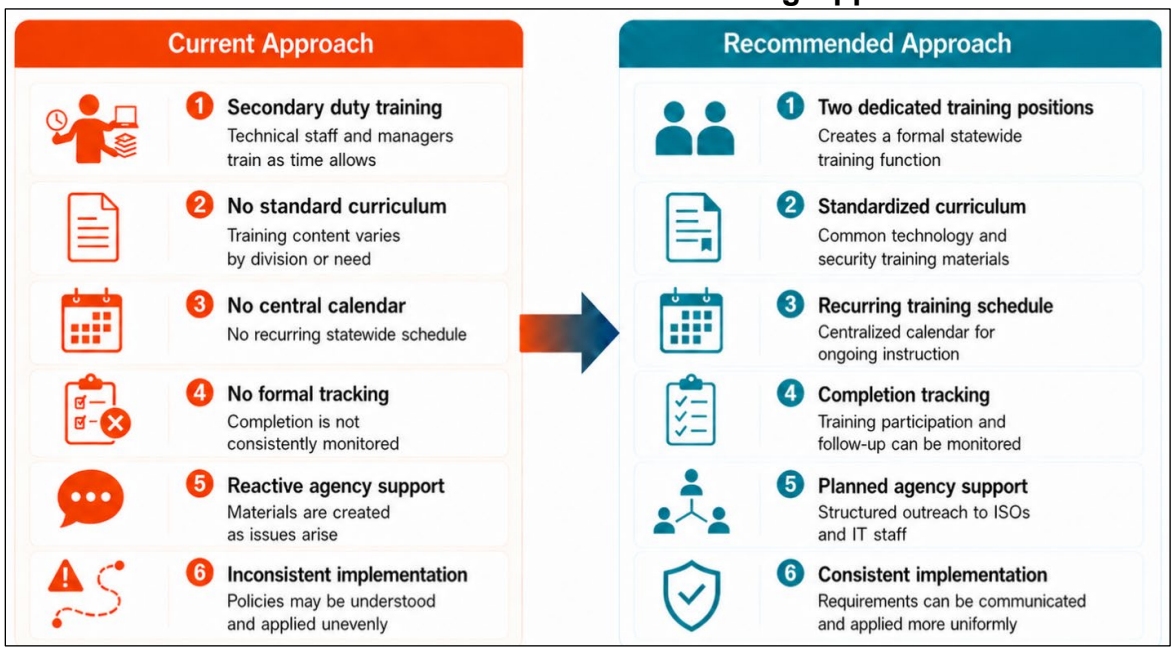
Seeking legislative approval and funding for dedicated information security training positions will help standardize training across Executive Branch agencies, improve awareness of statewide requirements, support agency compliance efforts, and strengthen preparedness for cyber attacks and other operational disruptions. Dedicated training staff will also provide capacity for onboarding, recurring awareness training, policy implementation support, and ongoing coordination with agency personnel responsible for technology and information security functions.

Exhibit VII shows the current versus the recommended training approach.

[16] GTO State Security Committee Charter Standard S.2.03.01.
[17] GTO ISO Roles & Responsibilities Standard S.3.03.01.

Exhibit VII

Current Versus Recommended Training Approach



Source: DIA analysis of current and recommended training approach.

Conclusion

GTO should request funding for dedicated information security training positions to provide centralized training, onboarding, policy implementation support, and recurring awareness programs for agency personnel. Dedicated training staff will improve statewide cybersecurity readiness, strengthen compliance with information security requirements, reduce reliance on operational staff to perform training as a secondary duty, and help ensure agencies receive consistent and timely guidance on evolving cybersecurity risks, technology governance requirements, and incident response responsibilities.

Recommendation

4. Request funding for information security training positions.

Appendix A

Scope and Methodology, Background, and Acknowledgments

Scope and Methodology

We began the audit in October 2025. In the course of our work, we interviewed management and staff of the Governor's Technology Office (GTO) to discuss policies, procedures, and internal controls related to information technology (IT) governance, cybersecurity assessment practices, IT asset and software visibility, continuity planning, advisory board oversight, and technology training capacity. We reviewed GTO records, policies, standards, procedures, meeting materials, continuity planning documents, inventory information, and other supporting documentation. We also researched legislative history, applicable Nevada Revised Statutes, Nevada Administrative Code, Nevada State Administrative Manual, state information security policies and standards, federal cybersecurity guidance, and other state and federal guidelines. We concluded fieldwork in May 2026.

We conducted our audit in conformance with the *Institute of Internal Auditors' Global Internal Audit Standards.*

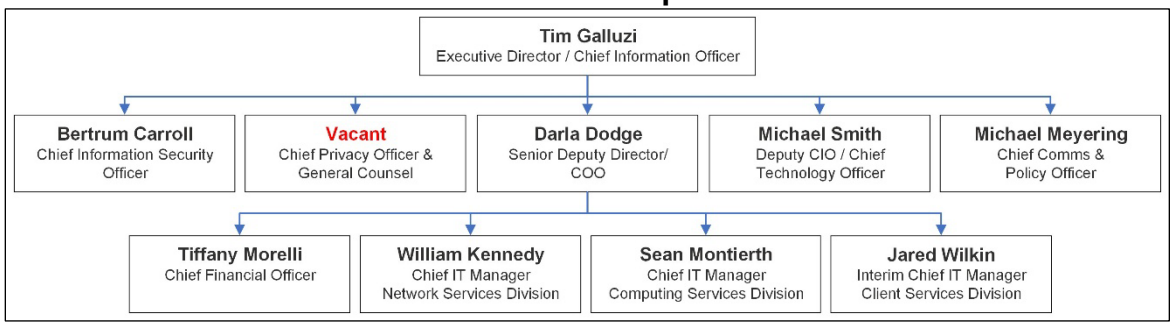
Background

The mission of the Governor's Technology Office (GTO) is to lead statewide technology by fostering secure innovative solutions and coordinating collaborative governance to deliver reliable technology services and solutions for Nevadans. GTO's values include stewardship, transparency, integrity, innovation, and collaboration. GTO has 206 full-time employees who provide centralized technology services and guidance for the Executive Branch, including service desk support, network and connectivity services, hosting and computing services, cybersecurity services, statewide information technology (IT) standards, and the Technology Investment Evaluation (TIE) process. GTO's role supports the coordinated, orderly, secure, and economical use of information systems, and prevents the unnecessary proliferation of equipment and personnel among Executive Branch agencies.

GTO includes the Office of Information Security and Cyber Defense, which leads statewide cybersecurity strategy, vulnerability management, incident response, and information security governance to protect Executive Branch systems, networks, and sensitive data. GTO's information security policies, standards, and procedures establish the baseline for Executive Branch information security programs. Exhibit VIII shows GTO's organizational chart as of May 2026.

Exhibit VIII

GTO Senior Leadership Structure



Source: Governor's Technology Office.

Acknowledgments

We express appreciation to the Governor's Technology Office management and staff, and the Governor's Finance Office, Budget Division for their cooperation and assistance throughout the audit.

Contributors to this report included:

Craig Stevenson
Administrator

Courtney Smith, J.D.
Executive Branch Auditor

Ruby Camposano, CPA
Executive Branch Auditor

Appendix B

Governor's Technology Office
Response and Implementation Plan

Joe Lombardo
Governor

Timothy D. Galluzi
Executive Director / State CIO

Darla J. Dodge
Senior Deputy Director / COO

Michael D. Smith
Deputy CIO / CTO

Bert Carroll
State CISO

STATE OF NEVADA
GOVERNOR'S TECHNOLOGY OFFICE

100 N. Stewart Street, Suite 100 | Carson City, Nevada 89701
Phone: (775) 684-5800 | www.it.nv.gov | CIO@it.nv.gov |Fax: (775) 687-9097

To: Executive Audit Committee & Administrator, Division of Internal Audits

From: Timothy D. Galluzi, State CIO & Executive Director, GTO

Subject: Audit Response for Inclusion for Audit Committee Meeting

Date: June 23, 2026

The Governor's Technology Office (GTO) would first like to express our sincere appreciation to the Division of Internal Audits, in particular, Administrator Craig Stevenson and Executive Branch auditor Courtney Smith, for their partnership and effort that went into this audit. The questions asked, research conducted and collaboration are demonstrated with the thorough audit report. Our hope is that these recommendations will help lead Nevada's Executive Branch into an era that demonstrates our shared goal of a more efficient, effective, and secure IT ecosystem that enables departments and divisions across the state to focus on their core mission of serving Nevadans.

The GTO is in full alignment and supportive of all recommendations in the audit and is already engaging in the foundational work to fully complete the recommended actions.

Recommendation 1:

Collaborate with federal agencies to proactively test information technology systems and strengthen cybersecurity practices.

The GTO concurs with and accepts this recommendation.

The GTO has previously attempted to evaluate the capacity and ability of federal partners to assist with scanning the state infrastructure. Historically, the scope that these scanning efforts made available to Nevada has been on an agency-level and by request from each agency. The Cybersecurity & Infrastructure Security Agency (CISA) has recently endured significant resource

cuts, to include the teams that have historically conducted these evaluations, with up to a third of their workforce transitioning.[1] GTO intends on continuing to build the relationship with CISA and leverage any services we can to better secure the state. We have also been investigating any additional scanning services beyond our current resources to give our Office of Information Security and Cyber Defense (OISCD) a more wholistic view of any potential vulnerabilities and areas for improvement.

- CISA at a crossroads amid workforce cuts, paused partnerships | Federal News Network

Recommendation 2:

Coordinate with the Information Technology Advisory Board (ITAB) to evaluate the information technology review threshold set in statute and submit a Bill Draft Request to lower the threshold, if advised.

The GTO concurs with and accepts this recommendation.

GTO has seen that even low-cost software can pose significant risks to the state. Low-cost or no-cost software can allow threat actors to gain access to critical state systems. During the August 2025 cybersecurity incident, it was a 'free' administrative tool software package that was downloaded that allowed access to the user's workstation. Cloud products that are low-cost may house sensitive constituent data or be used for critical services to Nevadans. Without proper vetting of these tools this will continue to become an area of risk. GTO is still expected to secure and defend the statewide ecosystem without having a role in vetting these low-cost investments that can result in a significant negative impact which we may find out exist when it is too late.

One way GTO has mitigated this risk was to bring in GovRAMP to provide 3rd party assessments on all cloud investments for the state. They provide this service to the state at no cost. The evaluation is based on the national NIST 800.53 standard. This is not just a point in time evaluation at procurement, GovRAMP also provides ongoing and regular assessments to ensure that 3rd-party cloud tools remain in compliance. GTO has already incorporated this into our statewide governance process established by NRS 242.171 for the evaluation of IT Solutions.

GTO will work with the Chair of ITAB to present this evaluation of the current threshold set in statute at the next available ITAB meeting for discussion and possible action in the form of a documented recommendation.

Recommendation 3:

Revise and enforce the software inventory policy, compile and analyze inventory, and coordinate with the Purchasing Division to lower software acquisition costs.

The GTO concurs with and accepts this recommendation.

GTO believes that siloed and uncoordinated procurement of IT software and hardware assets is inefficient and drives state IT costs higher than necessary to provide services. We have seen multiple agencies procure products and services that are duplicative to statewide offerings, examples of this include 3rd party-hosted websites when the state provides a platform for all agencies, and endpoint protection and management tools that are duplicative to the service offering that agencies are already paying for via statewide assessments.

To mitigate this early in the process, GTO has already established a duplicative spend review process in conjunction with our NRS 242.171 evaluation. While this should help with recent and future investments, we concur that collecting a full and complete inventory has a number of significant benefits.

1) GTO can use the collected inventory to identify out of support or high-risk software deployed at agencies.
2) GTO can identify opportunities to coalesce multiple procurements into a streamlined procurement vehicle that can leverage economies of scale provided by a multi-agency, enterprise-level agreement.
3) GTO can identify opportunities to create additional enterprise-wide service offerings if a similar product or service is being consumed across a number of agencies.
4) GTO can create and maintain a list of pre-approved software to enable rapid procurement and deployment across agencies.
5) GTO can use this inventory to rapidly identify affected software when notified of vendor-based vulnerabilities.
6) GTO can assist the State Controller's Office in Governmental Accounting Standards Board reporting with appropriate data sharing.

GTO has the foundational tools to begin the collection of this data quickly. Executive-level support will be required of all agencies across the state to compile a comprehensive inventory. This will not be something GTO can accomplish alone but will need the partnership of all agencies.

Recommendation 4:

Request funding for information security training positions.

The GTO concurs with and accepts this recommendation.

GTO identified knowledge, skill, and ability disparities across the Executive Branch during the response efforts in late 2025. Some agencies had very mature IT and security professionals who were able to operate very independently with minimal guidance and direction from GTO. Others required significant time and attention from GTO personnel to provide basic server administration tasks for their agency infrastructure.

GTO wants to be a resource in closing the gap and raising the technical maturity level for all agencies.

GTO believes that if we can provide training for agencies on the enterprise services that we provide for all agencies, not only will it improve outcomes for individuals and their agencies, but will increase our resilience, our cybersecurity maturity, and create efficiencies in numerous areas regarding the support of technology across the state.

These trainers would also aid in the acceptance and adoption of enterprise technologies; they could provide opportunities for increasing user adoption of new tools and capabilities aiding in organizational change management. They will be charged with creating educational pathways for career growth within the IT job specifications.

All of these goals lead to the positive outcome of a better equipped IT and cybersecurity workforce across the Executive Branch.

GTO would again like to thank the Division of Internal Audits for their work on this audit. GTO is confident that once all of the above recommendations are in place, with the support of Executive Branch leadership - our technology landscape across the state will be more efficient, more productive, more resilient and more secure.

Timothy D. Galluzi
State CIO

Appendix C

Timetable for Implementing Audit Recommendations

In consultation with the Governor's Technology Office (GTO), the Division of Internal Audits categorized the recommendations contained within this report into two separate implementation time frames (i.e., *Category 1* – less than six months; *Category 2* – more than six months). GTO should begin taking steps to implement all recommendations as soon as possible. The target completion dates are incorporated from Appendix B.

Category 1: Recommendations with an anticipated implementation period less than six months.

Recommendations	Time Frame
2. Coordinate with the Information Technology Advisory Board to evaluate the information technology review threshold set in statute and submit a Bill Draft Request to lower the threshold, if advised.	Sept 2026
4. Request funding for information security training positions.	Aug 2026

Category 2: Recommendations with an anticipated implementation period exceeding six months.

Recommendations	Time Frame
1. Collaborate with federal agencies to proactively test information technology systems and strengthen cybersecurity practices.	June 2027
3. Revise and enforce the software inventory policy, compile and analyze inventory, and coordinate with the Purchasing Division to lower software acquisition costs.	June 2027

The Division of Internal Audits shall evaluate the actions taken by GTO concerning the recommendations within six months from the issuance of this report. The Division of Internal Audits must report the results of its evaluation to the Executive Branch Audit Committee and GTO.