Joe Lombardo
Governor

Timothy D. Galluzi
Executive Director / State CIO

Darla J. Dodge
Senior Deputy Director / COO

Adam Miller
Deputy Director / OISCD

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

Prepared for: Nevada Commission on Homeland Security
Prepared by: Governor's Technology Office (GTO)
Date: 2/6/2026

Purpose

Provide a concise, public-facing summary of the 2025 statewide cyber incident, how Nevada responded, and what is changing as a result. This document supports leadership awareness, consistent messaging, and near-term decisions tied to recovery and modernization.

Background

Nevada's technology environment is federated. Agencies operate distinct systems and missions, while also relying on shared platforms and common services. That structure supports agency autonomy, but it also increases complexity during a cyber event: dependencies are broad, restoration must be sequenced carefully, and communications must stay aligned across many organizations.

Incident Overview (High Level)

On August 24, 2025, GTO identified a major system outage affecting multiple virtual machines. Initial triage confirmed ransomware activity. GTO activated its incident response process, escalated to the State CIO and the Governor's Office, and immediately isolated affected systems to limit spread.

- Initial access occurred months earlier through a user-initiated download from a spoofed or manipulated online source (commonly described as search-result poisoning).
- The threat actor sought to expand access using compromised credentials and remote access methods typical of modern ransomware campaigns.
- The attacker attempted to disrupt recovery by deleting or degrading backups before ransomware deployment.

Scope and Impact

The incident affected services used across state government and created real-world disruption for agencies and the public. The operational goal was to restore services safely and verifiably—not quickly at all costs.

- More than 60 state agencies experienced service impacts to varying degrees.
- State offices were temporarily closed early in the event to prioritize safe stabilization and prevent additional compromise.
- Restoration was completed in approximately 28 days, with validation steps embedded throughout to confirm integrity before re-enablement.

Response and Coordination

Nevada's response centered on speed with discipline: containment first, then stabilization, validation, and phased restoration. The State activated pre-established partnerships to bring specialized capabilities to the table while keeping decision authority clear.

- **Leadership coordination:** rapid escalation and clear decision lanes between GTO, the Governor's Office, agency leadership, and emergency management communications partners.
- **Vendor surge:** specialized cyber and infrastructure partners were activated quickly using pre-negotiated vehicles and cyber insurance, allowing response work to begin within hours rather than weeks.
- **Federal engagement:** federal partners remained involved through the event, supporting investigation and recovery coordination in a sustained way.

Communications Approach

Communications were treated as an operational workstream. The State prioritized transparency about status and what people needed to do, while limiting details that could increase attacker leverage. Messaging emphasized validated milestones and consistent terminology.

- **Single source of truth**: a public recovery hub and aligned agency messaging to reduce confusion and version drift.
- **Cadence:** frequent internal situational updates early, then scheduled public updates tied to confirmed restoration milestones.
- Public release gate (four-question check):
    (1) does it help the public take the right action.
    (2) could it increase attacker leverage;
    (3) do law-enforcement/partners request holding specifics;
    (4) have protective controls already been executed.
- **Public records alignment**: communications balanced public information needs with investigative integrity and security posture, consistent with NRS 242.105 and NRS 241.020(4)(b).

Ransom Payment and Fiscal Stewardship

Nevada maintains a firm position against paying ransom demands. Instead, the State relies on preparedness, resilience investments, and rapid access to expert response support. This approach protects public funds from going to criminal actors and focuses spending on recovery and long-term risk reduction.

- Cyber insurance and pre-negotiated response vehicles functioned as a speed lever—allowing rapid activation of external expertise when time was the enemy.
- External vendor costs during incident response were obligated to restore services and harden systems; these activations were aligned to existing plans for major cyber events.

Recovery, 'Build Better', and What's Changing

Recovery work did not stop at restoration. The State is using lessons learned to strengthen security and governance statewide—improving how Nevada prevents, detects, and recovers from future events.

- **Drive toward Zero Trust:** reduce lateral movement by strengthening identity controls (multifactor authentication, least privilege, higher-assurance authentication where warranted).
- **Inventory and visibility:** improve asset and dependency awareness so restoration is faster and more confident during outages or cyber events.
- **Operational readiness**: expand exercises and rehearsal to build muscle memory across agencies and partners, not just within a single team.
- **Governance and policy improvements:** clarify decision rights, strengthen standards, and align agency processes to a consistent statewide security posture.

Key Takeaways for Leaders

- Federated environments raise the coordination bar; relationships and pre-planning are as important as tools.
- **Practice beats paper:** plans work when teams rehearse together and build routine under stress.
- **Combined force matters**: rapid vendor and federal partner activation improves outcomes when scope is large and time is tight.
- **Communications must be disciplined:** transparency on status, restraint on exploitable detail.
- Identity is central to modern defense; Zero Trust is not a buzzword—it is how you limit blast radius.