ITAB Board Packet

Agenda Item 5: Advice & Recommendations GTO is Requesting for 2026

Timothy D. Galluzi, State of Nevada CIO

Meeting date: January 13, 2026

Governor's Technology Office (GTO)

STATE OF NEVADA
GOVERNOR'S TECHNOLOGY OFFICE

What this packet is for

Item 5 discussion + possible action

Desired outcome from ITAB

- A short, prioritized list of 2026 focus areas for statewide technology outcomes
- Guidance on tradeoffs (what should move down the list when resources are finite)
- Agreement on 3–5 measures to report quarterly (progress, not vanity numbers)

What's included

- 2026 priority themes and questions for Board advice
- Budget snapshot (known FY26–27 enhancements)
- Funding model / rate structure decision points
- SOC governance & participation framing
- Potential external funding “accelerants” (grants)

Recommended “possible action”

Adopt a short set of ITAB 2026 recommendations today (or direct staff to return next meeting with final language reflecting today's discussion).

Executive Summary: A New Framework for Accountability

The Mechanism

- The Board Packet will serve as the operational dashboard for tracking the execution of AB1 (Security Operations Center).

The Methodology

- Reporting will utilize the 'GTO Performance Measures Methodology' to shift focus from tracking activity (workload) to tracking efficacy (outcome).

The Balance

Designed to maximize fiscal transparency ($6.4M FY26 appropriation) while adhering to strict statutory confidentiality regarding specific cyber threats.

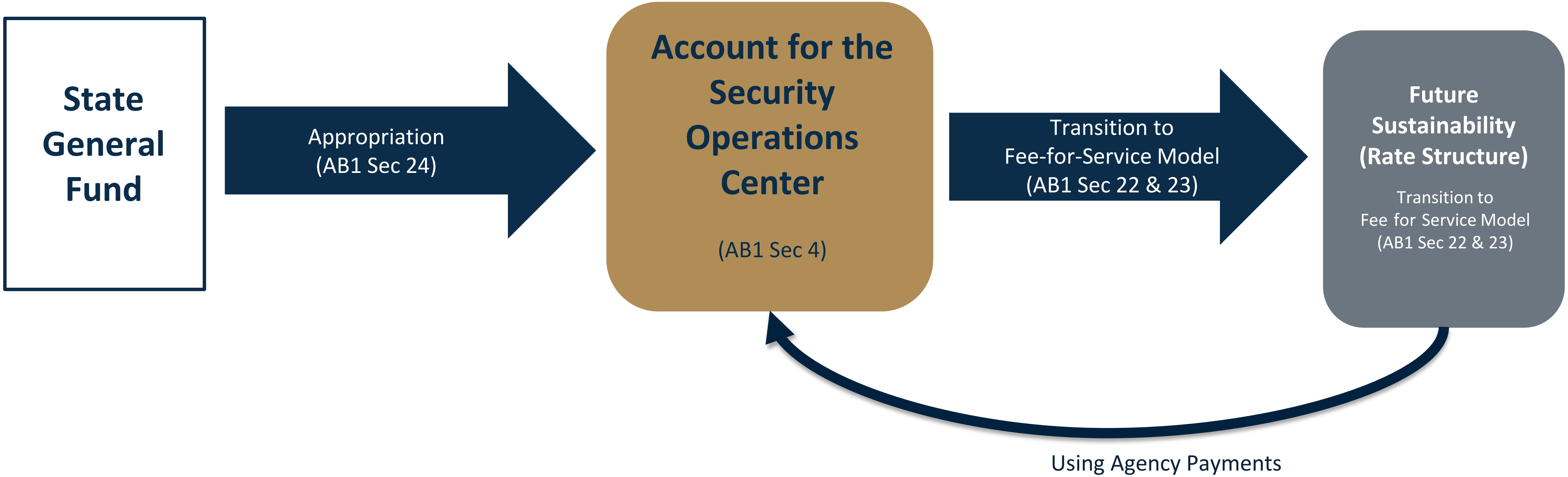
Legislative Outcomes: The 'New GTO' Mandate

AB 1: The Authority

- Mandate: Formally establishes the Security Operations Center (SOC) within the Office of Information Security and Cyber Defense (Section 13).
- Policy: Requires development of policies to combat threats, protect sensitive data, and ensure rapid incident response (Section 2).
- Control: Grants CIO emergency authority to direct executive branch IT resources during critical incidents.
- Fiscal: Creation of the Account for the Security Operations Center (Section 4).
- Funding: Appropriated from the State General Fund to the Office of Finance in the Office of the Governor for the Governor's Technology Office within the Office of the Governor for investments related to cybersecurity the following sums: (Section 24)
- For the Fiscal Year 2025-2026 .... $6,458,457
- For the Fiscal Year 2026-2027 .... $3,420,682

Financial Framework: The SOC Account & Appropriations

Note: FY26/27 appropriations support cybersecurity investments to stand up and mature capability (people, tools, and processes).



What GTO is asking ITAB to recommend

Three decisions that make 2026 actionable

STATE OF NEVADA
GOVERNOR'S TECHNOLOGY OFFICE

1 Priorities

Pick the top 3 statewide technology priorities for 2026 (and what problem each solves).

- Security + SOC direction
- Funding model / rate structure principles
- Reliability + citizen-facing services

2 Tradeoffs

Name what should move down the list if staffing and dollars are limited.

- Stop/slow low-value work
- Standardize where it reduces cost/risk
- Avoid one-time funding cliffs

3 Measures

Agree on 3–5 metrics to report quarterly so the Board can see progress.

- Risk reduction (not counts)
- Service reliability
- Time-to-detect/contain incidents

Budget snapshot (known FY26–27 items)

For context; figures shown are from current enhancement justifications

Selected FY26–27 enhancements

Item	FY 2026	FY 2027
SOC Analysts 2.0 FTE	$160,455.17	$285,244.00

Note (for discussion): SOC expansion and participation costs are still being refined. ITAB input on funding principles and governance will help shape final estimates and participation planning.

If the Board would like additional budget detail (run-rate, committed contracts, and planned enhancements), staff can provide a one-page addendum as part of the pre-read packet for the next meeting.

SOC governance & participation model (discussion)

A framework ITAB can refine

Governance: clarify decision rights

- Who sets minimum participation standards (logging, MFA, patch timelines)?
- Who approves changes to SOC services and tooling?
- How escalations work (what triggers an “all hands” response)?
- Clear service boundaries: what SOC does vs what agencies/local partners do.
- Data handling: retention, access controls, and audit expectations.

Shared responsibility (plain language)

SOC monitors and supports response, but agencies/partners still own their systems, business decisions, and day-to-day remediation.

Participation tiers (illustrative)

Baseline

Central monitoring + alert triage; basic incident coordination; required minimum logs.

Enhanced

Adds threat hunting, deeper analysis, and structured response support (playbooks).

Advisory

Assessments, tabletop exercises, and improvement planning (lighter operational touch).

Ask to ITAB:
What tiering + governance approach makes sense if participation expands beyond the Executive Branch (cities, counties, higher ed, etc.)—and what principles should drive any cost recovery / interlocal agreement model?

External funding “accelerants” (grants)

Question for Board members

Are you aware of any grant programs or external funding sources that could help accelerate statewide cybersecurity capability-building (especially shared services or regional participation) without creating long-term sustainability problems?

Examples (not exhaustive)

- State and Local Cybersecurity Grant Program (SLCGP) – DHS/FEMA + CISA
- Homeland Security Grant Program (HSGP) – cyber-eligible investments (case-specific)
- Targeted federal or sector grants tied to critical infrastructure resilience
- Foundation or university partnerships (training, exercises, workforce pipeline)

Practical guardrails (to avoid “free puppy” grants)

- Prefer funding that supports shared services or multi-entity outcomes
- Plan for sustainment before accepting (tools, staff, renewals)
- Align grant deliverables to Board-approved priorities and metrics
- Avoid duplicative tooling that increases long-term operating costs

Proposed quarterly measures (pick 3–5)

Candidate measures

Mean time to detect / contain

SOC operational performance over time (trend matters).

Critical vulnerabilities remediated

Percent fixed within an agreed timeframe (e.g., 15/30 days).

MFA coverage

Percent of privileged users protected by multi-factor authentication.

Participation / adoption

Percent of agencies meeting minimum security participation expectations.

Service reliability

Uptime + restoration time for key enterprise services.

Customer experience

Ticket resolution time + satisfaction (sampled) for enterprise support.

SOC operational performance (build in 2026)

- Mean time to detect/contain (trend)
- Incident response milestone timeliness (playbooks)
- Threat-hunting outputs (as defined by governance)

Vulnerability timelines (build in 2026)

- % critical vulnerabilities remediated within agreed timelines
- Exceptions/waivers count + aging

Participation & readiness (build in 2026)

- # agencies/partners onboarded to baseline logging
- % meeting minimum controls (MFA, logging, patch participation)
- Adoption by tier (Baseline/Enhanced/Advisory)

Ask to ITAB: which 3–5 measures should be the standard quarterly dashboard for 2026?

Appendix: Methodology and ownership (examples)

Example calculations (plain language)

- Endpoints scanned: endpoints scanned ÷ target endpoints
- SilverNet uptime: (total hours − downtime) ÷ total hours
- First-contact resolution: tickets resolved on first inquiry ÷ total inquiries
- DB currency: current/patchable databases ÷ total hosted databases

Data sources + owners

- Vulnerability scanning + incident tracking: OISCD security tools / database
- Network availability: enterprise monitoring (e.g., SolarWinds)
- Service Desk measures: ServiceNow + survey sampling
- DB currency: DBA monthly hosting/billing report

Appendix: Decision support artifacts

How GTO tracks priorities and partner experience (high level)

TIE COMPASS (portfolio + compliance analytics)

- Tracks Technology Investment Evaluation (TIE) reviews
- Shows cycle time, backlog aging, and throughput
- Helps identify bottlenecks and capacity needs
- Aligns to NRS 242.171(2) and SAM 1618.0

Agency Experience Intelligence Report (AEIR)

- Collects near-real-time partner feedback
- Trends satisfaction + sentiment over time
- Flags “special cause” drops that need investigation
- Turns comments into themes for improvement planning