From Periodic Compliance to Continuous Defense:

Kansas' Real-Time Cybersecurity Operating Model

NASCIO 2026
State IT Recognition Award
Category: **Cybersecurity**

Primary Contact
John Godfrey
Chief Information Security Officer State of Kansas
john.godfrey@ks.gov

Project Dates November 2024 – April 2026
State Kansas
Agency Kansas Office of Information Technology Services (OITS) / Kansas Information Security Office (KISO)

22,700+ Endpoints Monitored	**70+** Agencies Protected	**3.2M** Findings Reduced in 60 Days	**90%+** Patch Compliance in Hours	**$915K+** Cost Avoidance	**< 60 Days** Time to Enterprise Impact

EXECUTIVE SUMMARY

Kansas transformed cybersecurity from periodic, agency-by-agency reporting into a continuous statewide defense model that identifies risk, enforces baselines, remediates vulnerabilities, validates compliance, and reports progress in near real time. Led by the Kansas Information Security Office (KISO), the KISO Continuous Defense Model established a common operating discipline across more than 70 agencies and 22,700 endpoints, replacing fragmented visibility and manual remediation with measurable, governed, repeatable cybersecurity execution.

The results were immediate and measurable. In the first 60 days, Kansas reduced active endpoint vulnerability findings from 7.1 million to 3.9 million. By April 2026, active findings had fallen to 1.8 million, a 75% reduction from baseline. Patch compliance exceeded 90% within hours for targeted patch events, mean time to patch improved by 60%, and automated Windows 11 modernization, remediation, and validation produced more than $915,000 in documented cost avoidance.

This initiative was not simply a technology deployment. It changed how Kansas manages cyber risk. The state now has an operating model that allows leadership and participating agencies to see exposure, prioritize action, validate remediation, and demonstrate progress across the enterprise. Most importantly, it reduces risk to the systems Kansans rely on every day for benefits, licensing, public safety, tax administration, health services, and the continuity of government operations.

IDEA

The Challenge

Like many states, Kansas operated in an enterprise environment with decentralized cybersecurity execution. Agencies shared statewide risk, but cybersecurity visibility, tooling maturity, remediation practices, and reporting varied widely. This made it difficult to see risk across the enterprise, prioritize remediation consistently, validate progress quickly, and provide timely accountability to executive, agency, and legislative leadership.

- Fragmented security visibility across agencies and endpoint environments
- Periodic, snapshot-based assessments that did not reflect current operational risk
- Manual, labor-intensive vulnerability remediation and patch validation
- Inconsistent enforcement of security baselines across participating agencies
- Delayed reporting that limited enterprise accountability and slowed risk reduction

These conditions created three critical risks: known vulnerabilities remained exposed longer than necessary, agencies experienced uneven levels of protection despite shared enterprise risk, and leadership lacked a continuous, measurable view of statewide cybersecurity posture.

Kansas needed more than another cybersecurity tool. It needed a repeatable statewide operating model that could continuously identify risk, prioritize action, execute remediation, validate results, and report progress.

Why This Matters

Cybersecurity is foundational to modern government services. Kansans depend every day on digital systems that support benefits administration, public safety, licensing, tax services, health and human services, and continuity of government operations. As ransomware, exploitation of known vulnerabilities, supply chain compromise, and attacks against public-sector infrastructure continue to accelerate, periodic compliance reviews are no longer sufficient. When those systems are exposed, delayed, disrupted, or unavailable, the impact is not limited to IT; it affects public trust, service reliability, operational resilience, and stewardship of taxpayer resources.

The Kansas Cybersecurity Act and Senate Bill 291 reinforced the expectation that cybersecurity must be governed, measurable, and accountable at the enterprise level. The prior model could not consistently meet that expectation because visibility, remediation, enforcement, and reporting were not unified into one continuous discipline.

The Idea

Kansas created the KISO Continuous Defense Model: a statewide cybersecurity operating model that moves the state from periodic compliance activity to continuous defense execution. The model integrates five functions that were previously treated as separate activities:

1. Enterprise visibility into endpoint risk and security posture
2. Standardized security baselines aligned to recognized frameworks
3. Risk-based automation for patching, remediation, and configuration enforcement
4. Continuous validation of compliance and remediation outcomes
5. Executive reporting that connects operational progress to enterprise accountability

The core idea is simple but powerful: cybersecurity risk should be managed continuously, not periodically.

What Makes It Different

The model is different because it does not treat visibility, patching, vulnerability remediation, compliance enforcement, modernization, and executive reporting as separate workstreams. Kansas integrated them into one measurable operating model. This is not a tool deployment; it is a transformation in how cybersecurity is executed across state government.

Kansas did not automate everything. It automated the right things at the right level of risk, within a governed operating model designed to protect service continuity.

What Makes It Universal

The challenge Kansas addressed is not unique to Kansas. Every state faces some version of the same problem: distributed agencies, uneven maturity, limited cybersecurity staffing, expanding attack surfaces, increasing legislative oversight, and growing expectations for measurable cyber risk reduction. The model is replicable because it is built around operating principles rather than a Kansas-specific organizational structure: establish visibility, standardize baselines, prioritize measurable exposure, apply controlled automation, validate continuously, and report progress in terms executives and policymakers can act on.

IMPLEMENTATION

Kansas implemented the model through a deliberate, phased approach designed to scale safely across participating agencies while maintaining continuity of government operations. The initiative was managed as an enterprise cybersecurity transformation, not a single technology deployment. Planning and foundational deployment began in November 2024, with enterprise measurement and statewide risk reduction accelerating in August 2025.

Phase 1	**Enterprise Visibility**	Unified real-time monitoring across managed endpoints and established a single authoritative source of truth for enterprise cyber risk.
Phase 2	**Policy Standardization**	Aligned baseline expectations to NIST CSF and CIS benchmarks while accounting for diverse agency environments.
Phase 3	**Risk-Based Automation**	Applied controlled automation for patching, vulnerability remediation, and configuration enforcement using a "do no harm" approach.

Phase 4	**Governance & Reporting**	Connected operational dashboards to executive, agency, and legislative visibility into measurable progress.
Phase 5	**Statewide Adoption**	Scaled through standardized onboarding, agency communications, phased rollout, centralized support, and shared governance.

How Kansas Did It

KISO treated implementation as an enterprise change-management effort. Agencies were onboarded through an agile delivery-based approach using standardized communications, phased enforcement windows, dashboard-based validation, centralized support, and escalation paths for exceptions. Automation was introduced only after visibility and baselines were established, with human oversight maintained for higher-risk changes and agency-impacting decisions.

Governance and Stakeholder Engagement

Implementation required coordinated engagement across KISO, OITS, agency CIOs and ISOs, endpoint administrators, technical operations teams, service owners, and executive leadership. KISO served as the central coordinating body for the operating model. KISO also supported enterprise technology enablement and operational integration. Agency CIOs, ISOs, and technical teams provided local operational knowledge, participated in rollout activities, reviewed impacts, and supported adoption within their environments.

Operating Principles	Successful Implementation Looked Like
Visibility before automation. Standardization before enforcement. Automation with governance. Validation as part of execution. Reporting tied to accountability.	Enterprise visibility established, baselines enforced safely, remediation validated quickly, dashboards used by technical and executive stakeholders, and agencies supported without needing to build separate models.

Operating Cycle

The model now operates as a repeatable statewide cycle: identify risk, prioritize exposure, apply standardized remediation, validate patching and configuration outcomes, report progress through operational and executive dashboards, and refine baselines based on new risks and agency feedback.

Rollout Timeline and Phasing

PHASE 1	PHASE 2	PHASE 3	PHASE 4	PHASE 5	PHASE 6
Month 1	**Months 1–4**	**Months 5–11**	**Month 12**	**Months 13–16**	**Month 17+**
Deploy endpoint agents statewide	Operationalize the largest agencies	Operationalize smaller agencies via phased onboarding waves	Assess statewide maturity	Curated optimization workshops with agencies	Expand capabilities including threat response

The implementation succeeded because Kansas combined technology, governance, process, and agency partnership into one operating model.

IMPACT

Kansas' Continuous Defense Model produced immediate, measurable, and sustained cybersecurity outcomes across participating state agencies. The initiative changed the state's ability to identify exposure, prioritize action, remediate vulnerabilities, validate compliance, and report progress from a centralized operational view.

7.1M to 3.9M active findings reduced in first 60 days	**1.8M** active findings remaining by April 2026	**75%** reduction from baseline
22,700+ endpoints under continuous monitoring	**70+** agencies in shared model	**5.3M** active findings reduced

Measurable Enterprise Risk Reduction

In August 2025, Kansas identified approximately 7.1 million active endpoint vulnerability findings across participating agencies. Within the first 60 days, that number was reduced to 3.9 million, a reduction of 3.2 million findings. By April 2026, active findings had fallen to 1.8 million, representing a 75% reduction from baseline.

Figure 1: Enterprise vulnerability overview, 7.1M to 1.8M / 75% reduction

This was not a one-time cleanup effort. It demonstrated that Kansas had created a repeatable operating model capable of continuously reducing exposure across a large and diverse state environment.

Metric	Before	After
Enterprise Visibility	Periodic, agency-by-agency reports	Real-time, enterprise-wide dashboards
Vulnerability Remediation	Weeks to months	Hours to days
Patch Compliance Validation	Days or weeks to confirm status	90%+ compliance confirmed within hours for targeted patch events
Mean Time to Patch	38.9 days	15.5 days and shrinking
Executive Reporting	Manual, inconsistent, delayed	Automated dashboards aligned to enterprise risk, NIST CSF, SB 291, and other regulatory requirements
Cybersecurity Model	Fragmented and audit-driven	Continuous statewide operating model

Faster Remediation and Validation

For targeted patch events, Kansas achieved 90%+ patch compliance within hours, compared to days or weeks under prior manual processes. Mean time to patch improved from 38.9 days to 15.5 days and shrinking, a 60% improvement between August 2025 and April 2026. Every hour saved between vulnerability discovery, remediation, and validation reduces the window of opportunity for exploitation.

Figure 2: Mean time to patch improved from 38.9 days to 15.5 days

Security Baseline Enforcement

Automated CIS compliance enforcement for Windows 11 increased benchmark recommendation compliance from 9% to 68% within 48 hours. This is distinct from patch compliance and demonstrates the model's ability to improve configuration posture at enterprise scale. Cybersecurity policy became operationally enforceable, measurable, and reportable.

Figure 3: Windows 11 CIS recommendation compliance increased from 9% to 68% within 48 hours

Cost Avoidance and Workforce Efficiency

Kansas achieved more than $915,000 in documented cost avoidance: $708,000 in avoided Windows 11 licensing and manual upgrade-related costs, plus $207,000 in avoided staff time through automated remediation, reduced manual outreach, and centralized validation. The initiative also created workforce capacity by enabling cybersecurity and agency technical teams to spend less time reconciling reports and more time addressing risk.

Agency Operating Impact	Statewide Governance Impact
Agencies now share a consistent way to understand exposure, prioritize remediation, validate results, and communicate progress without building separate cybersecurity operating models.	Leadership can see measurable progress through dashboards aligned to enterprise risk, NIST CSF expectations, and Kansas Cybersecurity Act accountability.

The model did not simply save money. It turned limited cybersecurity capacity into a statewide force multiplier.

IMPACT ON KANSANS AND SUSTAINED VALUE

Kansans may never see the dashboards, automated remediation workflows, compliance baselines, or vulnerability reduction metrics behind this initiative. But they depend on the services those capabilities protect: benefits administration, public safety operations, licensing services, tax administration, health and human services, and the everyday digital operations of state government.

By shortening the time between discovery, action, and validation, Kansas reduced the window in which known vulnerabilities could be exploited against systems supporting essential public services. The public value is direct: more reliable government services, reduced exposure of state systems, stronger protection of public-sector operations, better stewardship of taxpayer resources, faster response to known cyber risks, and greater accountability for statewide cybersecurity performance.

Agency Testimonial

"This initiative gave our agency faster visibility into risk, clearer remediation priorities, and a more consistent way to demonstrate progress to leadership. What previously required manual coordination across multiple reports can now be validated through a shared operational view, allowing our teams to focus on remediation and service continuity instead of reconciliation."

— Shawn Brown, CIO, Kansas Department of Transportation

Sustainment and Replicability

Kansas has proven that statewide cybersecurity risk can be measured, reduced, validated, and reported continuously. The KISO Continuous Defense Model is a replicable blueprint for any state ready to operationalize cybersecurity as a continuous government function rather than a periodic compliance exercise.

Area	Continued Impact
Continued Onboarding	Expand participation and strengthen statewide coverage.
Baseline Refinement	Update security baselines as threats, technologies, and agency needs evolve.
Expanded Automation	Add safe, risk-based remediation and validation use cases.
Executive Reporting	Continue improving dashboards for agency, executive, regulatory, and legislative accountability.
Sustained Compliance	Maintain alignment with NIST CSF, CIS benchmarks, SB 291, and other requirements.

Every vulnerability reduced is a disruption prevented and a service protected.

One Team. One Mission. Defending Kansas.