

# Securing the Public Sector in 2026

## *Federal and SLED Edition*

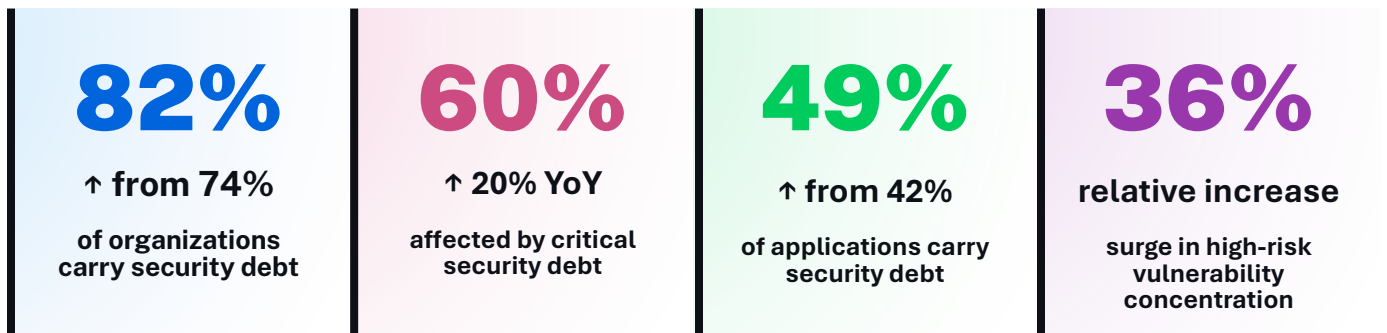
Government software applications are accumulating security debt faster than agencies and institutions can resolve it. Veracode's analysis of 1.6 million applications and 141 million security findings reveals what public sector technology leaders need to know — and do — right now.



# Executive Summary

The software powering government — from defense platforms to K-12 student information systems — is accumulating a dangerous backlog of unresolved vulnerabilities. Veracode's 2026 State of Software Security report, analyzing 1.6 million applications, reveals a stark reality for security leaders: **the pace of vulnerability discovery has structurally outrun the capacity to fix them.**

The result is 'security debt' — known vulnerabilities left unresolved for over a year, transforming from manageable technical tasks into active mission liabilities. With 60% of organizations now carrying *critical* security debt, the mandate is clear: detection is no longer enough. The next era of public sector cybersecurity must be defined by remediation.



What makes this especially urgent for the public sector is the nature of the debt that is accumulating. Critical security debt — defined as vulnerabilities that are both highly severe and highly exploitable — now affects 60% of organizations, a 20% jump in a single year <sup>[2]</sup>. These are not theoretical edge cases. They are exactly the class of flaw that nation-state actors, ransomware groups, and opportunistic attackers are more likely to seek out. For federal agencies, they are the vulnerabilities CISA's Known Exploited Vulnerabilities (KEV) catalog was designed to mandate remediation of. For SLED organizations, they represent the attack surface through which ransomware actors are breaching school districts and municipal systems at an increasing rate.

The 2026 data also reveals a dangerous new dynamic: the rise of AI-assisted code generation is likely introducing new patterns of high-risk vulnerabilities into the software supply chain, even as AI-driven remediation tools are beginning to offer a credible path out of the debt accumulation cycle. Public sector organizations need strategies that address both dimensions of this AI double-edge — hardening development pipelines against AI-introduced risk while deploying AI-powered remediation to finally close the productivity gap that security debt represents.

This report translates Veracode's 2026 SoSS findings into the specific policy, compliance, and operational context of Federal civilian agencies and the State, Local, and Education (SLED) sector. It provides public sector technology leaders with both the data to communicate urgency and the framework to act on it.

**Data source note:** All statistics and findings in this report are from Veracode's 2026 State of Software Security research unless specifically attributed to a third-party source. Third-party statistics are sourced and noted in the Appendix.

# About the Research

The 2026 State of Software Security report is Veracode's annual data-driven analysis of application security trends. The findings in this report are derived exclusively from Veracode's own platform telemetry — no competitive data is included.

## Research Dataset — 2026

Findings come from applications tested through Veracode's cloud platform using Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Software Composition Analysis (SCA). The dataset spans organizations of all sizes across commercial, government, and open-source sectors globally. <sup>[3]</sup>

**1.6m**

Unique  
Applications  
Analyzed

**141.3m**

Raw  
Security  
Findings

**115.6m**

Static  
Analysis  
Findings

**22.1m**

SCA  
Findings

**3.6m**

Dynamic  
Analysis  
Findings

## The Security Debt Crisis: By the Numbers

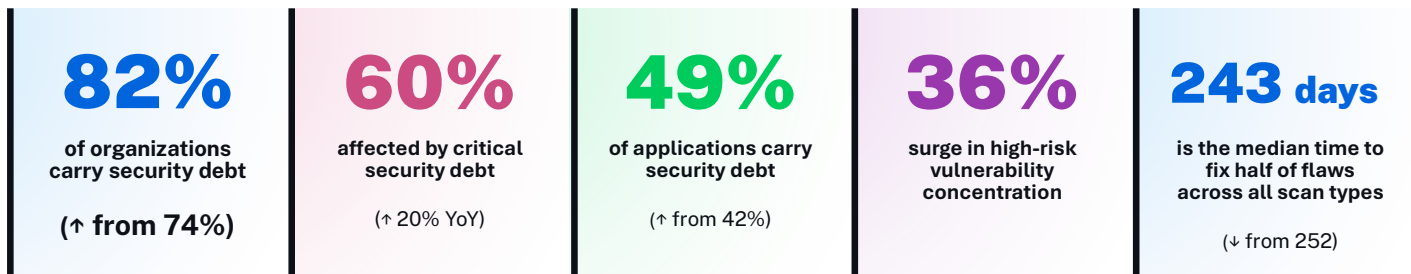
Veracode defines **security debt** as known vulnerabilities that remain unresolved for more than one year. This threshold is meaningful: a one-year-old vulnerability is one that teams have had multiple opportunities to remediate and have not. It represents a deliberate or forced deferral, not an oversight — and it is exactly the class of flaw that attackers exploit when they discover organizational assets are running outdated, vulnerable software. <sup>[4]</sup>

**Critical security debt** is the most dangerous subset: flaws that are both highly severe and highly exploitable, left unresolved for over a year. These are the vulnerabilities most likely to be weaponized, and their organizational prevalence increased 20% in a single year — from 50% to 60% of all organizations in the data. <sup>[2]</sup>

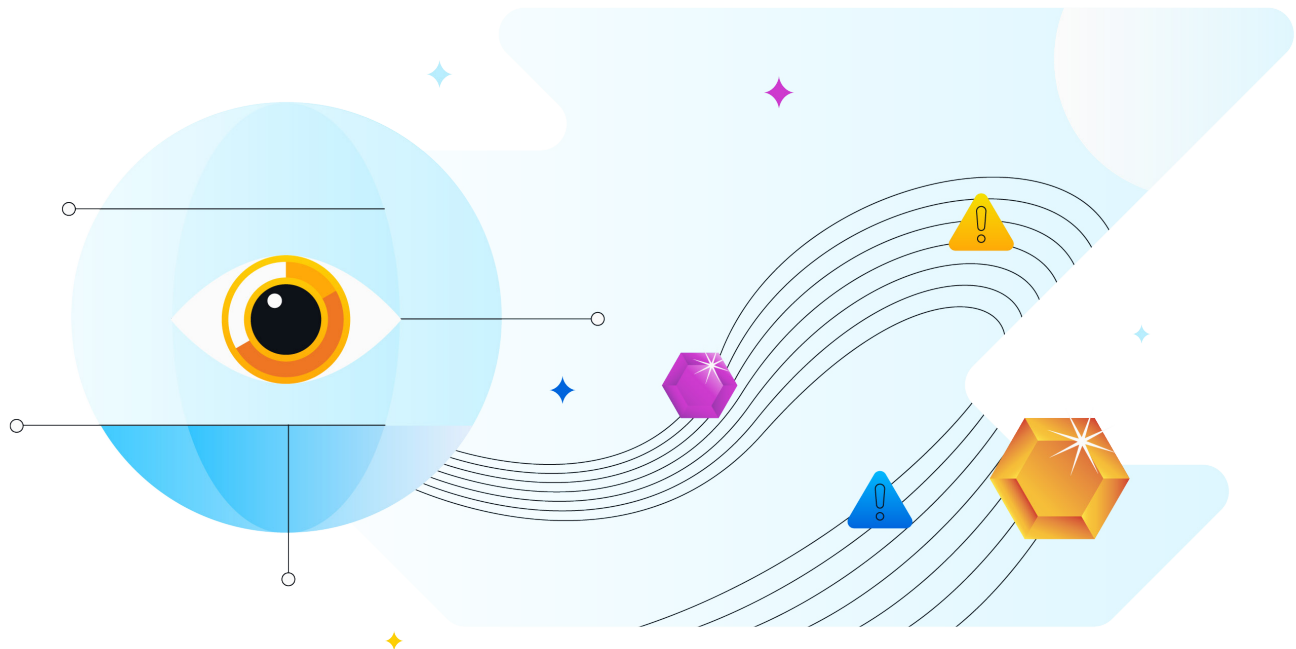
KEY FINDING

# Detection is accelerating. Remediation is not.

While overall flaw prevalence declined modestly, fix capacity for the median organization remains at approximately 10% of discovered flaws per month. At that rate, the backlog grows faster than it shrinks.



The mathematics are stark. If an organization discovers 1,000 vulnerabilities and resolves 10% per month, it eliminates 100. But if the development pipeline introduces more than 100 new vulnerabilities in that same month — through new features, dependency updates, AI-generated code — the backlog grows. The 12% year-over-year increase in the share of applications carrying security debt<sup>[7]</sup> indicates this is precisely what is happening across the sector.





## PART 1

# Federal Agencies: From Compliance to Mission Assurance

How the 2026 SoSS data maps to federal mandates — and what it means for the agencies responsible for securing government systems, citizen data, and national infrastructure.



## PART 1: FEDERAL

# The Federal Policy Landscape in 2026

Federal agencies in 2026 are operating under the most prescriptive software security regulatory environment in the history of US government IT. The mandates established under EO 14028 have matured into operational requirements, and new directives are continuing to raise the bar. Understanding how Veracode's SoSS findings map to these mandates is essential context for every federal technology leader.

| MANDATE                             | CORE REQUIREMENT                                                                                                                                                                                                               | SOSS CONNECTION                                                                                                                                                                        |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EO 14028 / SSDF<br>SP 800-218       | OMB M-22-18 (mandatory SSDF attestation) was rescinded by M-26-05 (Jan 2026). Agencies now use risk-based approaches and may optionally require attestation. NIST SP 800-218 serves as guidance. <sup>[8]</sup> <sup>[9]</sup> | SoSS data benchmarks vendor AppSec maturity — SAST, DAST, SCA, fix velocity — against SSDF practice areas, which agencies may still reference when developing risk-based requirements. |
| OMB M-26-05                         | Risk-based software attestation replaces the Common Form. Agencies may require vendors to provide current SBOMs upon request. <sup>[10]</sup>                                                                                  | SoSS supply chain data (66% of critical debt from third parties) validates the urgency of SBOM-based supply chain visibility.                                                          |
| CISA BOD 22-01                      | FCEB agencies must remediate KEV-catalog vulnerabilities within mandated timelines (15 days for critical, 30 for high-severity). <sup>[11]</sup>                                                                               | The median 243-day fix half-life <sup>[12]</sup> is an order of magnitude slower than BOD 22-01 mandates.                                                                              |
| GSA Contractor Framework (Jan 2026) | Contractors handling CUI must implement NIST SP 800-171/172. Assessments required; documentation must include supply chain risk management. <sup>[13]</sup><br><div>Third-party</div>                                          | SCA capabilities and SBOM generation satisfy the supply chain documentation and risk management requirements.                                                                          |
| CISA<br>FY2024-2026<br>Strategy     | Push technology providers to build security into products throughout their lifecycle and be radically transparent about known software weaknesses. <sup>[14]</sup>                                                             | SoSS provides the empirical evidence base for the software security transparency CISA's strategy demands.                                                                              |

**Compliance Gap Alert:** The CISA KEV catalog now contains over 1,484 entries (at the time of writing), and active exploitation of vulnerabilities surged 20% in 2025. Third-party — Cybersecurity News, Jan 2026, citing CISA data Federal agencies are required to remediate critical KEV vulnerabilities within 15 calendar days — roughly 16 times faster than what the median organization currently achieves across all vulnerability levels based on Veracode's SoSS data. This gap is a compliance risk, not just an operational one.

# Key Findings for Federal Agencies

## Finding 1: Security Debt Has Reached Mission-Critical Scale

Security debt — known vulnerabilities unresolved for over a year — now affects 82% of organizations, up from 74% the prior year, representing an 11% increase in organizational prevalence in a single year. At the application level, 49% of all applications now carry security debt, up from 42% — a 12% increase. <sup>[15]</sup> <sup>[16]</sup>

### Federal Mission Framing:

Security debt in a federal context is not merely a technical backlog — it is a compliance exposure and a mission risk. Under BOD 22-01, unresolved vulnerabilities that appear in the KEV catalog must be remediated on strict timelines. When nearly half of all applications carry year-old vulnerabilities, the probability that some of those flaws are KEV-listed — and therefore mandatory to remediate immediately — is high. Agencies using systematic application security scanning can identify exactly which security debt items fall into that category and prioritize them accordingly.

## Finding 2: Critical Security Debt Surged 20% — Weaponizable Flaws Are Accumulating

The most alarming trend in the 2026 data is not the breadth of security debt but its depth. Critical security debt — vulnerabilities that are both highly severe and highly exploitable, left unresolved for over a year — now affects 60% of organizations, up from 50%. <sup>[2]</sup> The 20% relative increase indicates that organizations are increasingly deferring not routine housekeeping but the very vulnerabilities adversaries most actively seek to exploit.

**60%**

↑ from 50%

of organizations carry  
critical security debt

**+20%**

year-over-year

relative increase in critical debt  
organizational prevalence

The driver is structural. Teams are not accepting this risk by choice but because capacity constraints make comprehensive remediation impossible for most organizations. <sup>[17]</sup> For federal agencies with complex contractor development ecosystems, staffing ceilings, and legacy architecture constraints, this capacity gap is even more pronounced than in the private sector.

## Finding 3: High-Risk Vulnerabilities Increased 36% — The Attack Surface Is Sharpening

Beyond security debt metrics, Veracode's 2026 data identified a 36% relative increase in the concentration of vulnerabilities that are simultaneously rated high in both severity and exploitability — what the report terms the "high-risk region," rising from 8.3% to 11.3% of all findings. <sup>[18]</sup> These are the vulnerabilities likely to be weaponized by sophisticated adversaries, including nation-state actors who often target federal systems.

#### Prioritization Implication:

Traditional CVSS-score-only prioritization is insufficient to address this risk profile.<sup>[19]</sup> A high CVSS score alone does not indicate that a flaw is actively exploitable in a given environment. Federal agencies need prioritization frameworks that weight exploitability alongside severity — and that correlate findings across all scan types (SAST, DAST, SCA) with runtime and business context to identify which specific flaws in which specific systems pose the greatest immediate risk to mission.

### Finding 4: The Software Supply Chain Is the Dominant Source of Critical Risk

Third-party and open-source components represent the most dangerous, most persistent dimension of security debt in the 2026 dataset. Third-party code accounts for 66% of the most dangerous, long-lived vulnerabilities in the average application portfolio — down from 70% the prior year, reflecting growing adoption of dependency hygiene and SBOM practices, but still representing the dominant source of critical risk.<sup>[20] [21]</sup>

**66%**

↓ from 70%

of critical security debt originates  
in third-party components

**358**

days average

to fix third-party flaws — 115 days  
longer than other scan types

The half-life of third-party flaws identified through Software Composition Analysis (SCA) is 358 days — nearly a full year, and 115 days longer than the average across all scan types.<sup>[22]</sup> The complexity of modern dependency chains — with both direct and transitive dependencies creating layered risk<sup>[23]</sup> — creates a fundamental challenge: resolving a third-party vulnerability often requires coordination across teams, compatibility testing, and waiting for upstream maintainers. For agencies operating under EO 14028's supply chain security mandates, this data underscores the urgency of proactive SCA tooling and SBOM management.

#### EO 14028 / M-26-05 Alignment:

The SoSS supply chain findings directly justify M-26-05's preserved option for agencies to require current SBOMs from vendors. When third-party components represent two-thirds of critical security debt, and third-party flaws take an average of 358 days to remediate, point-in-time attestation is insufficient. Continuous SCA monitoring — scanning all third-party and open-source components in real time against current vulnerability databases — is the operational standard agencies should require of their software vendors.<sup>[24]</sup>

# AI: Risk and Opportunity for Federal Programs

Artificial intelligence is reshaping federal software development in ways that simultaneously introduce new vulnerabilities and offer new remediation capabilities. The 2026 SoSS data captures both dimensions of this dynamic. <sup>[25]</sup>

## AI RISK

### AI-generated code is introducing new high-severity vulnerability patterns

The 36% surge in high-risk region vulnerabilities is believed to be at least partially attributable to the proliferation of AI-assisted code generation tools in development pipelines. A finding from the 2025 GenAI Code Security Report — another report by Veracode cited in the SoSS research — found that in 86% of tests, AI-generated code failed security tests for cross-site scripting (XSS), a class of vulnerability that can enable severe data breaches in web-facing applications. <sup>[26]</sup>

For federal agencies, particularly those overseeing software development contractor organizations that have rapidly adopted AI coding tools, this creates a new category of procurement oversight risk. AI-generated code that passes functional review may contain security vulnerabilities that would only surface through dedicated security scanning — making continuous SAST, SCA, and DAST coverage more critical, not less, as AI adoption expands.

## AI OPPORTUNITY

### AI-assisted remediation is the most credible path to closing the velocity gap

The same AI capabilities creating new vulnerability patterns are also enabling a step-change in remediation velocity. AI-driven tools can provide actionable insights and automated fix suggestions tailored to an application's specific environment and criticality, significantly reducing the manual workload for overstretched development and security teams. <sup>[27]</sup> Deploying AI remediation tools for the substantial portion of security debt that consists of simple, repetitive vulnerability patterns — and allocating a dedicated portion of sprint capacity to AI-assisted debt reduction — offers a realistic path to doubling fix capacity without proportional cost increases. <sup>[28] [29]</sup>

*"The themes analyzed here — debt intensification, high-risk vulnerability surge, detection-remediation gap, persistent supply chain challenges, and AI's double-edged impact — form a tale of transformation imperative. Organizations have spent the last decade learning to find vulnerabilities. The next decade must be about learning to fix them."*

**Veracode, 2026 State of Software Security Report <sup>[30]</sup>**





# The AI Implication for Federal SSDF Compliance

The updated SSDF (due in final form in 2026) will include practices regarding the secure development and delivery of software as well as security of the software itself. <sup>[9]</sup> As these updates are finalized, they are expected to address the new risk categories that AI-assisted development introduces — making security scanning coverage of AI-generated code a likely SSDF conformance requirement in the near term. Agencies should get ahead of this requirement by establishing expectations in their current contractor oversight frameworks.

## Recommendations for Federal Leaders

Drawing on the 2026 SoSS data and the current federal regulatory environment, the following actions represent the highest-priority steps for federal agency technology leaders in 2026.

### 1 Implement Exploitability-Weighted Prioritization

CVSS-score-only prioritization fails to capture which vulnerabilities are actively exploitable in your specific environment. Move to an exploitability-weighted framework that correlates findings across SAST, DAST, and SCA with runtime and business context. This shift is essential for meaningful BOD 22-01 compliance and achievable critical debt reduction.

### 4 Update Contractor Oversight to Address AI-Generated Code Risk

Contractor development teams adopting AI code generation tools without security guardrails are likely introducing new high-severity vulnerability patterns into agency systems. Update contractor SSDF attestation requirements to specifically require security scanning coverage of AI-assisted development pipelines, and add AI code vulnerability patterns to security training requirements. <sup>[33]</sup>

### 2 Establish Continuous SBOM Visibility Across the Software Portfolio

With third-party components representing 66% of critical security debt <sup>[20]</sup> and a 358-day average remediation timeline <sup>[32]</sup>, point-in-time attestation is insufficient. M-26-05 preserves the right to require current SBOMs from vendors upon request <sup>[10]</sup> — agencies should exercise this right systematically for high-criticality systems and require continuous SCA monitoring rather than annual assessments.

### 5 Implement "Fix Before Merge" Policies for New Code

The most cost-effective approach to security debt is preventing it from accumulating in the first place. Integrating automated security scanning and fix suggestions directly into developer workflows — before code reaches production — eliminates a class of vulnerabilities before they become debt. <sup>[34]</sup> Target: Keep net-new security debt below 20% of applications.

### 3 Deploy AI-Assisted Remediation to Close the Velocity Gap

The 243-day median fix half-life is incompatible with BOD 22-01's 15–30-day remediation mandates. AI-assisted remediation — supplying automated fix suggestions with human review — is the only scalable path to achieving compliance-grade velocity without proportional expansion of security staffing. <sup>[27]</sup> Allocate dedicated sprint capacity for AI-assisted security debt reduction as a standard development process requirement.

### 6 Elevate Security Debt as a Program-Level Mission Risk Metric

Security debt should be tracked and reported at the program executive level alongside mission assurance metrics, not buried in technical vulnerability backlogs. When security debt becomes a KPI at agency leadership level — tied to OKRs and contractor performance metrics — the urgency and budget for systematic remediation programs follow. <sup>[35]</sup> Target: Organizational security debt decreasing quarterly; top-quartile performance within 18 months.

## PART 2

# State, Local & Education: Resilience Under Constraint

For school districts, municipalities, and state agencies navigating limited budgets, rising threats, and new compliance mandates — the SoSS data provides both a diagnosis and a path forward.



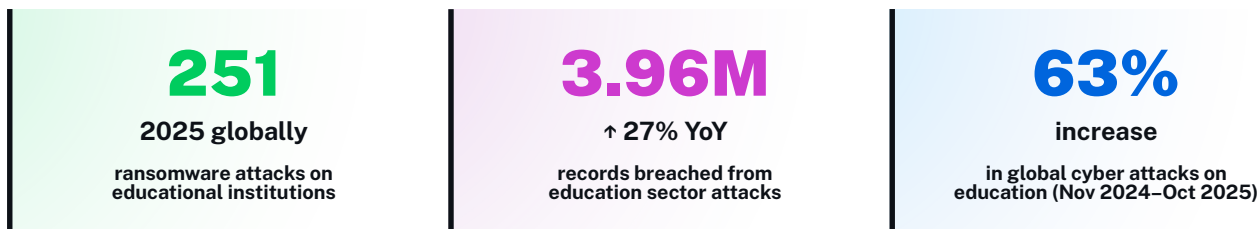
## PART 2: SLED

# The SLED Threat & Policy Landscape in 2026

State, local, and education organizations are navigating a cybersecurity environment in 2026 that is simultaneously more threatening, more regulated, and more resource-constrained than at any prior point. The convergence of rising ransomware activity, expanding state-level cybersecurity mandates, tightening cyber insurance requirements, and shifting federal grant dynamics has created a uniquely difficult operating environment — even as the imperative to act has never been greater.

## The Threat Reality

Ransomware attacks on educational institutions globally reached 251 in 2025, resulting in the breach of more than 3.96 million records — a 27% increase in breached data from the prior year. The US accounted for more than half of all attacks. <sup>[36]</sup>



**Third-party sources :** Ransomware statistics: Comparitech (January 2026). Education sector attack increase: National Law Review / Quorum Cyber 2026 Global Cyber Risk Outlook for Higher Education.

For state and local government, ransomware attacks on government entities rose 27% globally in 2025. <sup>[37]</sup> The attackers targeting these organizations are not, in most cases, deploying novel zero-day exploits. They are finding and exploiting the class of known, unresolved, highly exploitable vulnerabilities that Veracode's 2026 data shows accumulating in every organization's application portfolio.

## The Resource Reality

Despite this escalating threat, 61% of K-12 school districts rely on general funds rather than dedicated cybersecurity budgets to protect their networks and data. <sup>[38]</sup> Nearly 40% of schools feel under-supported against ransomware, and three-quarters lack a dedicated cybersecurity specialist — even as budgets and awareness are slowly improving. <sup>[39]</sup>

**The Core SLED Challenge:** SLED organizations manage enterprise-scale software portfolios — student information systems, benefits administration platforms, public safety systems, permitting applications — with technology teams a fraction of the size of their private-sector counterparts. Many commercial security products are designed for large enterprises, making them expensive, overly complex, or incompatible with government and education legacy infrastructure. <sup>[40]</sup>

## The Regulatory Reality

State legislatures are responding to the escalating threat environment with new mandates. In 2026, new state cybersecurity laws are requiring K-12 districts to implement multi-factor authentication, network segmentation, and zero-trust principles — whether or not federal funding is available to support compliance. <sup>[41]</sup>

Simultaneously, cyber insurance carriers have raised the bar for coverage. Insurers now require documented, demonstrable security controls before issuing or renewing policies — including application security scanning evidence and vulnerability management documentation. <sup>[42]</sup> Organizations that cannot demonstrate systematic security programs face both coverage gaps and premium increases.

State and Local Cybersecurity Grant Program funds are increasingly being directed toward automation in security operations, governance frameworks for AI deployments, and continuous training — a grant planning posture that application security automation programs align with directly. <sup>[43]</sup>

# Key Findings for SLED Organizations

## Finding 1: Nearly Half of All Applications Carry Year-Old Vulnerabilities, With Limited Resources to Fix Them

Veracode's 2026 data shows that **49% of applications now carry security debt** — known vulnerabilities older than one year. <sup>[44]</sup> For SLED organizations, this finding arrives in a uniquely difficult context. State agencies, municipalities, and school districts operate enterprise-level software portfolios with technology teams that are often severely understaffed relative to the scope of what they manage.

The mechanism is straightforward: fix capacity for the median organization is only about **10% of discovered flaws per month**. <sup>[6]</sup> When an IT team is simultaneously managing help desk requests, deploying new instructional technology, and maintaining aging infrastructure, vulnerability remediation competes with immediate operational demands — and often loses. Security debt is an almost inevitable consequence of the staffing and budget equation in most SLED environments, not a failure of awareness or intent.

### THE SLED FRAMING

The conversation with SLED stakeholders should not be about blame for accumulated debt — it should be about leverage. SLED organizations face the same vulnerability exposure as the largest commercial enterprises but have a fraction of the remediation bandwidth. The right solution is tooling that converts limited security bandwidth into outsized impact: AI-assisted remediation that automates fix suggestions, enabling IT staff to address security debt in the normal flow of their work rather than as a separate, competing project.

## Finding 2: Critical Security Debt Surged: The Vulnerabilities Ransomware Exploits Are Growing Fastest

Critical security debt — the most exploitable, most severe flaws left unresolved for over a year — now affects **60% of organizations**, having increased 20% year-over-year. <sup>[2]</sup> For SLED organizations that are prime ransomware targets, this finding is directly connected to the operational reality they experience in breach headlines.

Ransomware actors targeting schools and municipalities are not conducting sophisticated zero-day campaigns. They are discovering and exploiting known, highly exploitable vulnerabilities that organizations have not yet patched — the class of flaw that Veracode's critical security debt metric precisely identifies. Over 85% of schools experienced at least one cybersecurity incident in 2025, with unauthorized access and malware among the most common entry vectors. <sup>[39]</sup> These are not accidents. They are the predictable consequences of critical security debt remaining unresolved.

## Finding 3: Third-Party Software Is the Dominant Source of Critical Risk, EdTech Vendors Included

Third-party components represent 66% of the most dangerous, long-lived vulnerabilities in the application portfolio. <sup>[20]</sup> For SLED organizations heavily reliant on commercial EdTech platforms, cloud-based student information systems, and government software suites, this means a majority of their most dangerous security debt lives in software they did not develop and cannot directly control.

### EDTECH SUPPLY CHAIN RISK

#### The third-party fix half-life is nearly a full calendar year

The average time to remediate third-party flaws identified through software composition analysis is 358 days. <sup>[32]</sup> When a student information system vendor discovers a vulnerability in an embedded third-party library, the time from discovery to patch availability to district deployment to verification can span multiple semesters. During that interval, student PII, staff records, and financial data remain at risk. Continuous SCA scanning across the EdTech vendor portfolio — not annual assessments — is the standard required to manage this risk effectively.

Procurement teams have the most direct lever to address this: requiring EdTech and GovTech vendors to maintain active SCA programs and provide Software Bill of Materials (SBOM) documentation as a condition of contract award and renewal. This aligns with CoSN's legislative recommendation that procurement processes require vendors to meet minimum cybersecurity standards <sup>[38]</sup> and with the evolving direction of state procurement mandates nationwide.



## Finding 4: AI-Generated Code Introduces New Risk for SLED Development Projects

As SLED organizations adopt AI tools for administrative efficiency and digital modernization, the development pipelines leveraging AI code generation are producing a new category of security vulnerability. The 2025 GenAI Code Security Report found that in 86% of tests, AI-generated code failed security tests for cross-site scripting (XSS) <sup>[26]</sup> a vulnerability class particularly dangerous in public-facing web portals that could be handling student data, benefit applications, or permit submissions.

The implication is concrete: SLED organizations that have adopted AI development tools without implementing corresponding security scanning guardrails may be introducing a new and faster-moving class of vulnerabilities into their citizen-facing applications. Security scanning that covers AI-assisted development pipelines — not just traditional codebases — is the appropriate response. <sup>[33]</sup>

# Recommendations for SLED Leaders

The following recommendations are calibrated to the specific constraints and priorities of SLED organizations — resource-limited, compliance-driven, and operating under escalating threat conditions.

## 1 Adopt Risk-Based Prioritization to Focus Limited Capacity

Not all vulnerabilities carry equal risk. SLED organizations with constrained remediation capacity cannot treat a low-severity theoretical flaw with the same urgency as a critical, actively exploitable vulnerability in a student-facing web application. Prioritization frameworks that weight exploitability alongside severity — focusing first on the high-risk region vulnerabilities that enable the ransomware and breach incidents SLED organizations are experiencing — convert limited security bandwidth into maximum risk reduction. The cost of a single ransomware incident — recovery, forensic investigation, notification obligations, identity protection services — routinely exceeds the multi-year cost of a systematic application security program.

## 2 Require SCA and SBOM from EdTech and GovTech Vendors

Given that 66% of critical security debt originates in third-party components <sup>[20]</sup> and that the average third-party fix half-life is 358 days <sup>[32]</sup>, procurement is the most powerful lever SLED organizations have for reducing supply chain risk. Establish minimum SCA program requirements and SBOM documentation obligations as standard contract terms for all vendors handling student data, financial records, or public safety systems. This aligns EdTech vendor requirements with both CoSN legislative recommendations <sup>[38]</sup> and with evolving state procurement mandates.

## 3 Build the Cyber Insurance and Budget Case with Security Debt Data

Cyber insurers are requiring documented security controls for policy issuance and renewal. <sup>[42]</sup> Organizations with demonstrable, quantified, and improving application security programs are better positioned for coverage availability and competitive premiums. For district and agency technology leaders making budget cases to boards or elected officials, security debt metrics — tied directly to the SoSS benchmark of 82% organizational prevalence <sup>[15]</sup> — provide a concrete financial risk framing that resonates with non-technical decision-makers.

## 4 Leverage Grant Funding for Application Security Automation

State and Local Cybersecurity Grant Program funds and state cybersecurity appropriations are increasingly directed toward automation in security operations. <sup>[43]</sup> Application security automation — including continuous SAST, DAST, and SCA scanning with AI-assisted remediation — falls squarely within the automation and security operations improvement categories that 2026 grant guidance emphasizes. Organizations seeking to maximize grant impact should explicitly scope application security tooling within grant applications.



## 5

### Deploy AI-Assisted Remediation for the Long Tail of Security Debt

The bulk of security debt in most application portfolios consists of common, repetitive vulnerability patterns — SQL injection, cross-site scripting, insecure configurations, outdated dependencies — that AI-assisted remediation tools can address at scale with minimal developer effort. <sup>[28]</sup> For SLED organizations without dedicated security engineering staff, AI-generated fix suggestions with human review provide a force multiplier that makes meaningful security debt reduction achievable within normal operational rhythms. <sup>[45]</sup>

## 6

### Generate Audit-Ready Security Posture Documentation

Legislative oversight, school board reporting, and community accountability all demand clear, accessible communication about cybersecurity posture. Quantitative application security metrics — security debt prevalence, fix velocity, high-risk vulnerability counts — translate internal technical data into the mission-risk framing that elected officials and state auditors can evaluate and act on. Systematic application security programs generate exactly this documentation as a byproduct of normal operations, eliminating the significant effort currently required to prepare position papers before audit cycles.

## CONCLUSION

# The Path Forward

The 2026 State of Software Security data tells a story of transition. Detection is improving. Scanning programs are maturing. Fix velocity is edging forward. These are genuine achievements, and they reflect years of investment in application security programs across both the commercial and public sectors.

But the improvements in detection are outpacing improvements in remediation capacity, and the result is accumulating security debt — known vulnerabilities that age past one year because the capacity to eliminate them does not exist at the scale required. For public sector organizations, this structural challenge is compounded by staffing constraints, procurement complexity, budget competition, and the specific pressure of serving constituents who depend on the availability and integrity of government systems. <sup>[46]</sup>

The 2026 findings are not a story of failure. They are a story of a sector at an inflection point. The organizations achieving top-quartile security performance are not doing so through brute-force manual remediation. They are investing in automation, deploying AI-assisted fix capabilities, using risk-based prioritization to focus limited capacity on the vulnerabilities that matter most, and establishing governance structures that hold security outcomes accountable at the leadership level. <sup>[47]</sup>

*"Organizations have spent the last decade learning to find vulnerabilities. The next decade must be about learning to fix them in a prioritized way while simultaneously preventing their introduction in the first place."*

**Veracode, 2026 State of Software Security Report <sup>[30]</sup>**



The policy environment in 2026 is, for the first time, providing the mandate structure to make this shift real in the public sector. BOD 22-01 sets remediation velocity standards that exceed what manual-only programs can achieve. M-26-05 creates procurement pressure for continuous supply chain visibility. State legislative mandates are extending application security requirements into K-12 districts and municipalities that have historically been underserved by federal frameworks. Cyber insurance requirements are creating financial accountability for organizations that cannot demonstrate systematic programs.

The data, the mandates, and the tooling are aligned. The security debt crisis is solvable — but it requires treating remediation capacity as a strategic investment, not a line item to be optimized away. Public sector organizations that make that investment in 2026 will be materially better positioned to protect citizen data, maintain mission continuity, and meet the accountability standards their constituents and regulators increasingly demand.



# Appendix: Methodology & Data Attribution



## DISCLAIMER

The information provided in this document is for general informational and educational purposes only. It does not constitute legal advice, and should not be relied upon as legal advice. Regulatory and compliance requirements vary by organization, jurisdiction, and context. Organizations should consult qualified legal counsel and compliance professionals to understand and address their specific regulatory obligations. Veracode makes no representations or warranties regarding the completeness, accuracy, or applicability of the information contained in this document. Regulatory frameworks discussed in this article are subject to change; readers should consult the official regulatory bodies and legal resources for the most current requirements.

## DATA ATTRIBUTION

# Third-Party Data Sources

**Veracode State of Software Security (SoSS) 2026 Dataset** Unless otherwise explicitly noted, all statistics, telemetry, and vulnerability trends presented in this public sector edition are derived exclusively from Veracode's 2026 State of Software Security research. This annual dataset is grounded in the analysis of 1.6 million unique applications and over 141.3 million raw security findings spanning global commercial, government, and open-source sectors. The telemetry is gathered via Veracode's cloud platform using Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Software Composition Analysis (SCA).

### Veracode State of Software Security 2026

- [\[1\]](#) Veracode State of Software Report 2026, p.32
- [\[2\]](#) Veracode State of Software Report 2026, p.7
- [\[3\]](#) Veracode State of Software Report 2026p.32
- [\[4\]](#) Veracode State of Software Report 2026 p.5
- [\[5\]](#) Veracode State of Software Report 2026, p.15
- [\[6\]](#) Veracode State of Software Report 2026 p.15
- [\[7\]](#) Veracode State of Software Report 2026 p.24



## DATA ATTRIBUTION

# Third-Party Data Sources

**Third-Party Market Intelligence** To provide comprehensive operational and regulatory context for Federal and SLED leaders, this report integrates external market intelligence and federal policy directives. The truncated URLs from the original draft have been validated and fully expanded for reader reference:

## Federal Policy & Regulatory Frameworks

- **[8]** NIST: Software Security in Supply Chains: Software Cybersecurity for Producers and Users  
URL:  
<https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software>
- **[9]** Federal Register: Sustaining Select Efforts To Strengthen the Nation's Cybersecurity and Amending Executive Order 13694  
URL:  
<https://www.federalregister.gov/documents/2025/06/11/2025-10804/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity>
- **[10]** Inside Government Contracts / OMB: OMB Rescinds the “Common Form” Secure Software Attestation Requirement  
URL:  
<https://www.insidegovernmentcontracts.com/2026/02/omb-rescinds-the-common-form-secure-software-attestation-requirement/>
- **[11]** CISA: CISA Adds Eight Known Exploited Vulnerabilities to Catalog \*  
URL: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- **[14]** CISA: Cybersecurity Strategic Plan FY2024-2026  
URL: <https://www.cisa.gov/cybersecurity-strategic-plan>
- **[13]** Nextgov/FCW / GSA: GSA quietly rolls out CMMC-like cybersecurity framework for contractors  
URL:  
<https://www.nextgov.com/cybersecurity/2026/01/gsa-quietly-rolls-out-cmmc-like-cybersecurity-framework-for-contractors>

## Threat Landscape & Sector Analysis

- **[36]** Comparitech: Education Ransomware Roundup: 2025 stats on attacks, ransoms, and data breaches  
URL: <https://www.comparitech.com/studies/ransomware-studies/>
- **[37]** Action1: Cybersecurity in Education Report 2025–2026  
URL: <https://www.action1.com/cybersecurity-in-education-report/>
- **[38]** Consortium for School Networking (CoSN): CoSN Unveils 2025 State Cybersecurity Legislation Report  
URL: <https://www.cosn.org/cosn-unveils-2025-state-cybersecurity-legislation-report/>
- **[39]** Campus Technology: Ransomware Attacks Plateau in Education Sector, While Third-Party Risks Loom  
URL: <https://campustechnology.com/articles/2026/01/ransomware-attacks-plateau.aspx>
- **[40]** Information Technology and Innovation Foundation (ITIF): Improving State and Local Government Cybersecurity  
URL: <https://itif.org/publications/2026/04/improving-state-and-local-government-cybersecurity/>
- **[41]** Civic IQ Blog: Government Cybersecurity Spending in 2026: Municipal & K-12 Vendors  
URL: <https://blogs.civiciq.com/government-cybersecurity-spending-2026>
- **[42]** HUB Tech: SLED Cyber Resilience Readiness Guide for 2026  
URL: <https://www.hubtech.com/sled-cyber-resilience-readiness-guide-2026/>
- **[43]** StateTech Magazine: Tech Trends: What States Should Fund With 2026 Cybersecurity Grants  
URL: <https://statetechmagazine.com/article/2026/01/tech-trends-states-cybersecurity-grants>







## About Veracode

Veracode is a global leader in Application Risk Management for the AI era. Powered by trillions of lines of code scans and a proprietary AI-assisted remediation engine, the Veracode platform is trusted by organizations worldwide to build and maintain secure software from code creation to cloud deployment. The 2026 State of Software Security report is Veracode's seventeenth annual analysis of enterprise application security trends. <sup>[48]</sup>

**For more information, visit** [www.veracode.com](https://www.veracode.com)

**Contact:** [info@veracode.com](mailto:info@veracode.com)

**Phone:**

+1 888 937 0329 (Sales)

+1 877 837 2203 (Support)