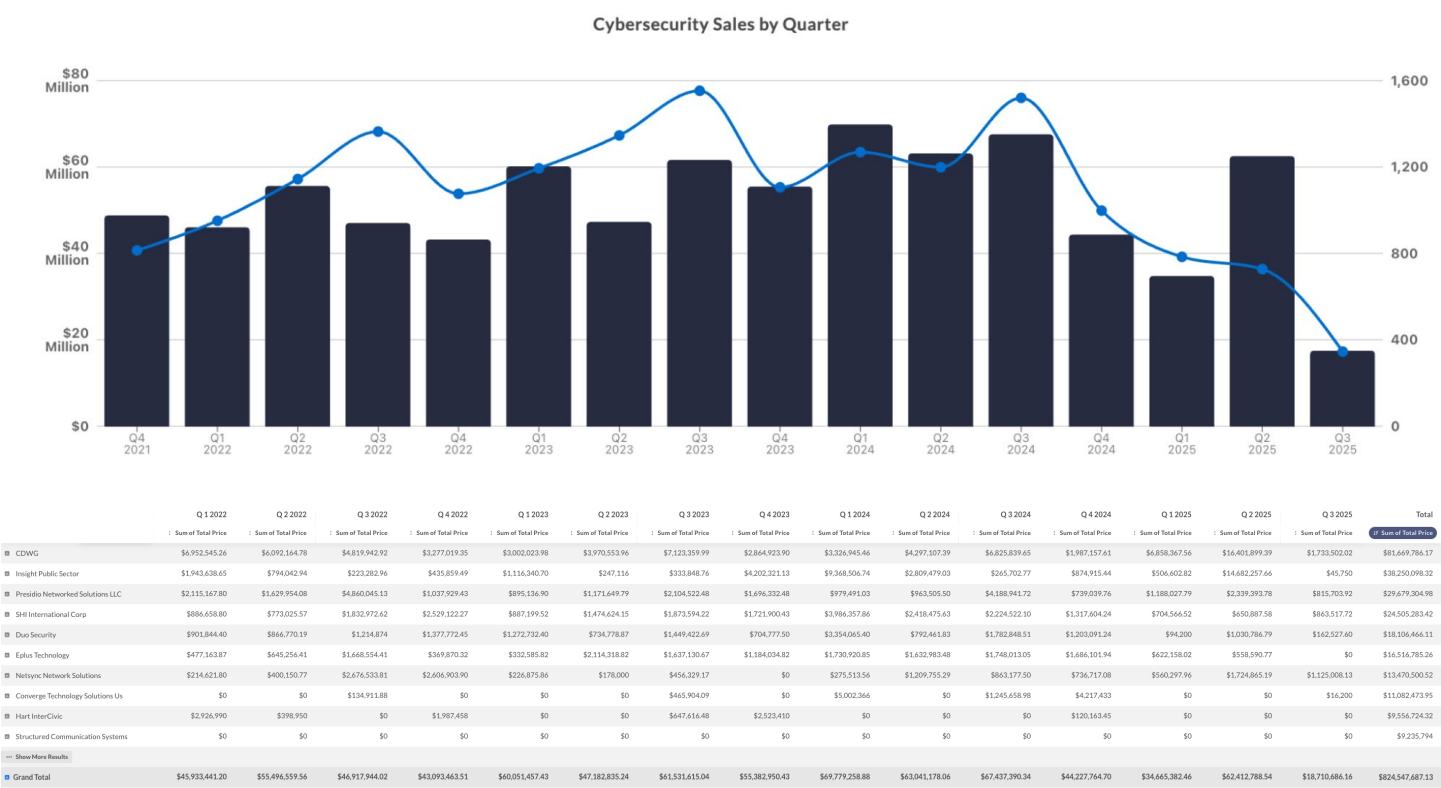


# Cybersecurity: A SLED Market Overview

GovSpend’s latest analysis highlights the continued growth and strategic importance of cybersecurity within state and local government. Over the past five years, 5,566 SLED agencies have spent more than \$2.28 billion on cybersecurity purchases, evidence of the sector’s enduring focus on strengthening digital defenses and protecting critical infrastructure.

Spending has followed a steady upward trajectory, rising from just over \$121 million in 2020 to more than \$138 million in 2025. The market reached its highest levels of quarterly activity in Q1 2024, with over \$70 million in purchases, followed by \$63 million in Q2 2024.

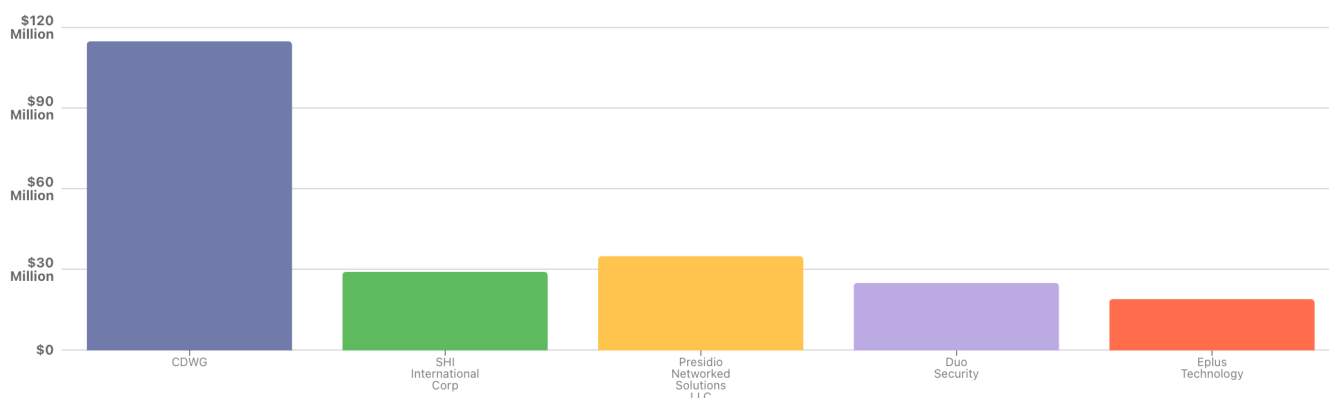


This sustained investment reflects cybersecurity’s growing role as a core operational priority across all levels of state and local government.

## Key Providers and Market Share

GovSpend data shows that a select group of vendors continues to drive a large portion of cybersecurity procurement, while competition among emerging providers remains active. CDW-G leads the market with more than \$114 million in sales over the past five years, followed by Presidio Networked Solutions LLC at \$34.7 million, Duo Security at \$24.7 million, and Eplus Technology at \$18.7 million.

Cybersecurity Sales by Company - Last 5 Years

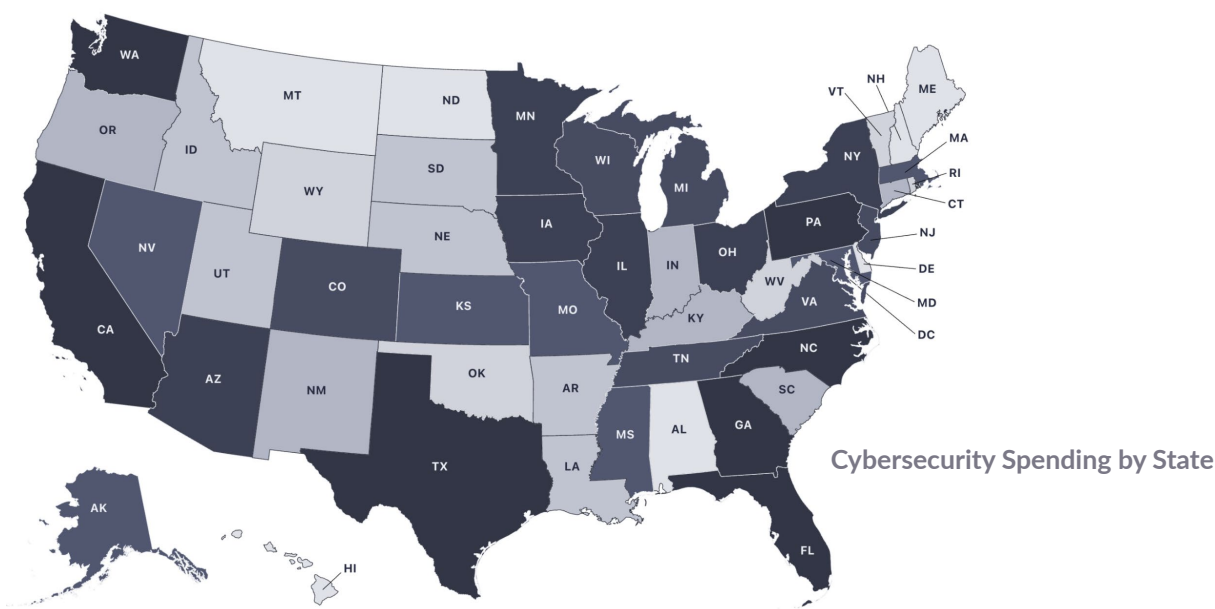


	CDWG	SHI International Corp	Presidio Networked Solutions LLC	Duo Security	Eplus Technology	... More	Total
	Sum of Total Price	Sum of Total Price	Sum of Total Price	Sum of Total Price	Sum of Total Price		Sum of Total Price
2020	\$1,411,558.29	\$1,574,819.03	\$898,202.97	\$2,012,970.91	\$0		\$121,198,970.41
2021	\$33,494,581.61	\$2,903,786.65	\$6,903,789.38	\$6,088,692.61	\$0		\$356,432,827.49
2022	\$21,166,223.45	\$6,095,438.47	\$9,820,737.14	\$3,880,678.04	\$0		\$584,144,312.57
2023	\$16,933,105.83	\$6,055,978.13	\$5,867,641.66	\$4,284,144.06	\$4,713,793.09		\$345,259,150.07
2024	\$16,644,086.59	\$10,104,055.39	\$6,870,978.01	\$6,991,143.23	\$6,798,019.33		\$384,314,025.29
2025	\$25,014,492.17	\$2,170,534.76	\$4,343,125.49	\$1,509,644.30	\$0		\$138,063,669.03
Grand Total	\$114,664,047.93	\$28,904,612.43	\$34,704,474.66	\$24,767,273.15	\$18,736,171.67		\$1,929,412,954.87

These figures go beyond traditional bid-based data, incorporating p-card and discretionary spending to present a complete picture of vendor activity. This holistic view provides valuable insight into how agencies are actually purchasing cybersecurity solutions, both through formal RFP processes and through smaller, direct transactions that reflect ongoing operational needs.

Geographic Trends

Cybersecurity investment remains concentrated in states leading large-scale digital modernization efforts. California, Texas, Florida, and Washington have emerged as top spenders, together representing a significant share of total market activity. These states are consistently at the forefront of initiatives designed to safeguard citizen data, modernize digital infrastructure, and strengthen resilience against cyber threats.



	California	Texas	Florida	Washington	North Carolina	Georgia	New York	Illinois	Ohio	Wisconsin
	Sum of Total Price	Sum of Total Price	Sum of Total Price	Sum of Total Price	Sum of Total Price	Sum of Total Price	Sum of Total Price	Sum of Total Price	Sum of Total Price	Sum of Total Price
> CDWG	\$13,409,989.53	\$5,441,254.06	\$10,430,567.11	\$6,185,057.73	\$2,549,723.26	\$31,430,470.14	\$20,917,217.08	\$43,163,673.87	\$5,021,706.14	\$5,441,521.24
> Presidio Networked Solutions LLC	\$9,476,356.29	\$9,770,558.34	\$14,508,806.90	\$341,991.45	\$14,288,583.38	\$1,850,603.16	\$1,890,037.28	\$4,015,673.70	\$216,817.17	\$2,708,396.39
> Duo Security	\$5,547,161.26	\$5,838,337.51	\$1,980,689.26	\$688,746.62	\$3,345,764.90	\$6,388,682.14	\$0	\$585,889.38	\$8,890,396.01	\$427,894
> Insight Public Sector	\$1,949,265.13	\$4,708,149.34	\$2,500,391.96	\$513,258.97	\$381,756	\$95,681.25	\$94,812.57	\$219,282.13	\$233,309.50	\$0
> SHI International Corp	\$3,609,866.97	\$539,492	\$3,975,627.71	\$1,919,182.68	\$3,266,893.92	\$2,785,871.77	\$5,463,824.61	\$3,046,372.68	\$263,158.07	\$673,178.73
> Netsync Network Solutions	\$643,407.72	\$29,834,946.71	\$1,400,106.70	\$0	\$0	\$158,529.16	\$0	\$15,264	\$0	\$0
> Eplus Technology	\$10,779,441.58	\$674,530.48	\$117,527.90	\$0	\$1,399,174.66	\$14,382	\$1,717,572.96	\$0	\$0	\$0
> Telligen	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
> Hart InterCivic	\$0	\$28,926,009.87	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
> Carahsoft Technology	\$9,358.92	\$144,487.78	\$0	\$0	\$106,680	\$454,371.10	\$0	\$60,450	\$64,920	\$0
--- Show More Results										
Grand Total	\$248,355,877.37	\$266,935,341.04	\$113,346,984.74	\$85,282,446.43	\$96,623,085.31	\$93,619,877.91	\$77,412,286.11	\$75,974,068.76	\$68,807,906.99	\$40,181,611.40

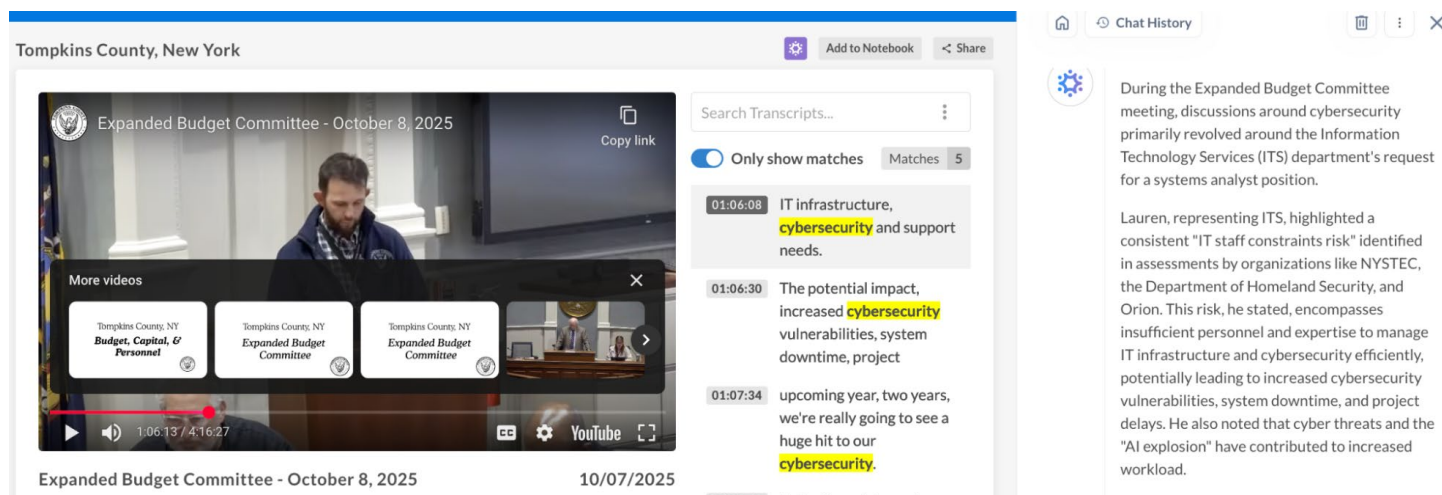
Sales data also shows that top vendors, including CDW-G, Presidio Networked Solutions, and Duo Security, have secured major contracts in these regions, underscoring where demand for cybersecurity expertise and advanced solutions remains strongest.

## Procurement Activity and Opportunity Outlook

The procurement landscape suggests that cybersecurity spending will remain active in the years ahead. GovSpend data shows 5,501 active contracts with 122 SLED agencies set to expire within the next 24 months, creating a strong pipeline of near-term opportunities. In addition, there are currently 98 open bids across 82 agencies, reflecting immediate demand for new solutions and services.

GovSpend has tracked more than 73,000 public meetings in the last five years where cybersecurity or risk management were discussed, including as recently as:

- On October 8, 2025 cybersecurity was discussed in the [Tompkins County, NY](#), expanded budget meeting in the context of the Information Technology Service (ITS) department's request for a new systems analyst. Increased cybersecurity vulnerabilities were listed as a potential impact of unstated IT resources, and a legislator emphasized the anticipated "huge hit to our cybersecurity" in the coming years and the importance of investing in staff to protect against hacking or ransomware. The approval of this new position indicates that future cybersecurity upgrades or purchases are likely.
- On October 7, 2025, [Buffalo Public Schools](#) discussed that the district received a \$1.25 million cybersecurity grant from E-RATE, which will be used for installing and acquiring an advanced firewall system.
- In the [City of Riverside, OH](#), council meeting on October 6, 2025, the city manager noted that the city has been working to comply with Ohio House Bill 96 (HB 96) requirements for municipal corporations to adopt cybersecurity plans and programs. A resolution for adopting a cybersecurity program for the city will be presented to the council by the end of the year, likely in November.
- On October 5, 2025 the [City of Goldsboro City \(NC\) Council](#) added a resolution to accept grant funds through the North Carolina Office of Emergency Management for IT cybersecurity needs.



Tompkins County, New York

Expanded Budget Committee - October 8, 2025

Search Transcripts...

Only show matches Matches 5

01:06:08 IT infrastructure, cybersecurity and support needs.

01:06:30 The potential impact, increased cybersecurity vulnerabilities, system downtime, project

01:07:34 upcoming year, two years, we're really going to see a huge hit to our cybersecurity.

During the Expanded Budget Committee meeting, discussions around cybersecurity primarily revolved around the Information Technology Services (ITS) department's request for a systems analyst position.

Lauren, representing ITS, highlighted a consistent "IT staff constraints risk" identified in assessments by organizations like NYSTEC, the Department of Homeland Security, and Orion. This risk, he stated, encompasses insufficient personnel and expertise to manage IT infrastructure and cybersecurity efficiently, potentially leading to increased cybersecurity vulnerabilities, system downtime, and project delays. He also noted that cyber threats and the "AI explosion" have contributed to increased workload.

This sustained level of engagement demonstrates that agencies are not only investing but continually reassessing their posture to keep pace with emerging threats and compliance requirements.

## Evolving Threat Landscape

The rise in spending is directly linked to the growing complexity of today's cyber threat environment. According to intelligence briefings from organizations such as the National White Collar Crime Center (NW3C), state and local governments are facing three primary categories of threats:

- **Advanced Persistent Threats (APTs):** Long-term, sophisticated attacks often backed by nation-state actors from countries such as Russia, China, Iran, and North Korea, targeting sensitive government data and systems.
- **Cryptographic and Ransomware Threats:** The emergence of Ransomware-as-a-Service (RaaS) has made ransomware deployment more accessible, allowing less-skilled attackers to carry out high-impact campaigns using advanced, leased tools.
- **Hacktivism:** Cyberattacks carried out for social or political purposes rather than financial gain, often intended to disrupt government operations or draw public attention to specific causes.

These threats are being amplified by the integration of AI technologies into cyber operations. Threat actors are now leveraging AI to enhance their tactics, techniques, and procedures (TTPs)—automating intrusion attempts, crafting realistic phishing schemes, and even developing adaptive malware capable of evading traditional defenses.

This rapidly changing landscape reinforces the need for a proactive, layered approach to cybersecurity that integrates detection, prevention, and continuous monitoring.

## Looking Ahead

The cybersecurity market within the SLED sector continues to expand, even amid broader IT budget tightening. Threat complexity, data privacy requirements, and federal guidance are all driving agencies to prioritize security investments as core to digital transformation.

For providers, the opportunity lies in anticipating needs, whether through scalable managed services, rapid response capabilities, or technologies that enhance visibility and control.

The message is clear: Cybersecurity is no longer a reactive purchase but an operational foundation for state and local governments. Understanding where and how that investment is happening will be key to staying competitive in 2025 and beyond.

*The data provided in this report comes from the GovSpend platform. For a deeper dive into spending intelligence specific to your business or competitive landscape, [request a personalized demo here](#).*