Establish a Regional K-12 and Local Government Security Operations Center

Current Reality: School divisions and local governments are increasingly dependent on digital systems to deliver instruction, payroll, transportation, food service, special education, communications, safety operations, and public services. These same systems now face persistent cyber threats, including ransomware, phishing, business email compromise, denial-of-service attacks, data breaches, and attacks against third-party vendors. The Cybersecurity and Infrastructure Security Agency (CISA) describes K-12 organizations as frequent targets because they maintain extensive student, staff, operational, and financial data while often lacking the resources needed for mature cybersecurity programs. The Center for Internet Security and the Multi-State Information Sharing and Analysis Center (MS-ISAC) reported that 82% of K-12 organizations that reported experienced cyber threat impacts during an 18-month study period, with nearly 14,000 security events and 9,300 confirmed incidents. These attacks do not simply affect technology systems; they disrupt meals, testing, counseling, instruction, childcare, and community trust.

The staffing reality is equally concerning. National K-12 technology leadership research continues to show that cybersecurity is one of the top concerns for school technology leaders, yet dedicated security staffing remains limited. The Consortium for School Networking (CoSN) and SETDA (Formerly known as the State Educational Technology Directors Association) reported that only 21% of districts had a full-time equivalent employee dedicated to network security, and later reported that the CoSN survey findings indicated that only about one-third of districts had a full-time employee focused on cybersecurity. This gap is most acute for small and mid-sized school divisions, where technology staff must also support devices, networks, help desk operations, instructional systems, procurement, data privacy, compliance, and physical operations. Expecting every school division to independently build and sustain a 24x7 security operations center, or to have this capability, is neither realistic nor fiscally efficient.

RCPS also notes that the previous Virginia VAST resource is no longer available. The attached Virginia Fusion Center communication states that VAST was retired effective June 1, 2026, that all data provided to the service would be securely and permanently deleted, and that no replacement service had been announced at the time of decommissioning. This leaves school divisions and local governments without a known equivalent statewide service at a time when cyber risks are increasing, and federal, state, and local expectations for cyber readiness continue to grow.

A regional Security Operations Center (SOC) model would create economies of scale by centralizing 24x7 monitoring, alert triage, threat intelligence, incident escalation, vulnerability coordination, and after-action support for K-12 divisions and local governments. Building a true 24x7 in-house SOC generally requires multiple analysts to cover continuous shifts, supervision, tools, training, incident response capacity, and retention costs. Industry cost guidance indicates that managed SOC services commonly range from approximately $10-$20 per protected asset per month for basic managed coverage, with broader detection-and-response services often ranging from roughly $15-$50 per endpoint per month. For an individual division with 10,000 monitored assets, this could translate to approximately $1.2 million to $6 million annually if procured independently, before implementation, incident response retainers, log storage, and internal staffing are considered. A state-funded regional SOC could reduce duplicated procurement, standardize service levels, improve visibility across jurisdictions, and provide smaller divisions access to capabilities they could not otherwise sustain.

RCPS recommends the General Assembly:

RCPS recommends that the General Assembly create, support, and fund an ongoing regional Security Operations Center dedicated to K-12 school divisions and local governments. The SOC should provide 24x7 monitoring, threat detection, incident triage, coordinated response support, vulnerability and patch-priority guidance, threat intelligence, cybersecurity awareness support, tabletop exercises, and executive-level reporting aligned to CISA, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Center for Internet Security (CIS) Controls, and MS-ISAC best practices. The program should be funded as a recurring state service rather than a one-time grant so participating school divisions and local governments can plan around stable, predictable cyber defense capacity.

A reasonable state planning estimate is $8 million to $15 million annually for a regional SOC serving K-12 divisions and local governments, depending on the number of participating entities, protected endpoints, log sources, service levels, and incident response scope. This estimate should include core SOC staffing or contracted managed detection and response, security information and event management (SIEM)/Extended Detection and Response (XDR) licensing, endpoint and identity telemetry integration, network detection capabilities, onboarding and engineering support, governance, reporting, cyber exercise support, and a reserve for incident-response surge capacity. Even at that level, a regional service would likely cost less than each locality attempting to procure or staff comparable capabilities independently. It would also create statewide consistency, allow cybersecurity personnel to be shared across jurisdictions, strengthen incident coordination, and provide better protection for students, families, employees, and public services.