

Proven practices from high-threat environments for Massachusetts school districts

METAA Member Cybersecurity Program

A SIMPLER, STRONGER APPROACH TO CYBERSECURITY

Cyber threats are increasing in frequency and sophistication, yet many municipalities and school districts lack the budget and capacity to keep up. The Massachusetts Educational Technology Administrators Association (METAA) has partnered with CyberTrust Massachusetts to deliver a professionalized, high caliber cybersecurity capability, combining advanced technology, specialized operations, and national level expertise at a price point accessible to public sector organizations.

Services included in METAA Member Package:

- | | |
|--|---|
| 1 Cybersecurity Controls Assessment
Structured baseline evaluation against CIS Critical Security Controls | 2 Managed Detection & Response
24/7 monitoring, triage, and response via SentinelOne platform |
| 3 CyberTrust SOC Support
Expert threat hunting, remediation guidance, and ongoing tuning | 4  MS-ISAC® Membership
Access to the nation's premier state and local cybersecurity organization |
| 5 Managed Domain Blocking & Reporting Service
Block connections to malicious domains with MDBR+ premium service from MS-ISAC | |

MADE AFFORDABLE AND ACCESSIBLE FOR METAA MEMBERS

METAA Member Pricing

\$60

per endpoint / year
\$2,000 one-time onboarding fee

Grant Funding Opportunity

Most districts qualify for up to
\$25,000 through the Cyber
Resilient Massachusetts Grant
Program

CyberTrust is 30B Exempt

CyberTrust contracts are exempt
from Chapter 30B, creating a
simplified acquisition process.

CYBERSECURITY CONTROLS ASSESSMENT

Every engagement begins with a structured evaluation of your cybersecurity posture against the CIS Critical Security Controls — the standard trusted by school districts, municipalities, and state agencies, and the structured beginning of a stronger cyber program.

- Know your true security posture
- A practical baseline for stronger cyber decision making
- Interview based assessment with external scanning and dark web search
- A roadmap for reducing risk, improving controls, and guiding future investment

Gain visibility into current controls, gaps, exposures, and priorities to understand what matters most and what to do next.



ONGOING OPERATIONS: WHAT CYBERTRUST DELIVERS

Managed Detection & Response

Built on SentinelOne technology platform, with extensive automation and configuration by CyberTrust experts to serve local entities.

- Your foundation for cyber defense
- Twenty four hour monitoring, triage, and response operated for you
- Earlier detection. Faster response. Lower operational burden.
- A professionalized defense function for organizations that cannot run one alone
 - *SentinelOne Complete Protection Platform*
 - *SentinelOne Vigilance Respond*

Membership in the Multi-State Information Sharing and Analysis Center (MS-ISAC)

Access to the nation's premiere state and local cybersecurity organization, with access to best practices, intelligence and services tailored for local governments.

- Threat Intelligence and Distribution
- Incident Response & Forensic Services
- Security Operations Center (SOC) Support
- Cyber Early Warning Service, dark web monitoring

CyberTrust SOC Support

CyberTrust SOC team provides the monitoring, analysis, threat hunting, remediation prioritization, tuning, and operational judgment that turn the technology into a functioning defense capability.

- Monitoring of alert activity with autonomous and human response for containment and eradication
- Threat hunting that looks beyond standard detections to identify suspicious behavior earlier
- Prioritized remediation guidance based on what is actually exploited in the field and what matters most in the customer environment
- Policy tuning, reporting, and ongoing operational support that improve protection over time
- Detection engineering insight informed by real world customer environments and active analysis

Malicious Domain Blocking and Reporting + (MDBR+)

Provided in partnership with the MS-ISAC.

- Prevents connections to known or suspected malicious domains.
- Provides real-time reporting, enabling you to quickly identify and mitigate emerging threats.
- Customizable for your needs.
- Protects devices on premise and remote.

CyberTrust also offers higher-tier services such as XDR and Application Control / Zero Trust for organizations that need broader visibility or stronger prevention controls.

Ready to strengthen your cybersecurity posture without adding operational burden?

Contact CyberTrust Massachusetts to discuss fit, onboarding, and grant alignment.