2026 Chronology: Cyderes Managed Security Services

The Department of Information and Instructional Technology (DIIT) seeks approval to continue managed cybersecurity services provided by Cyderes. This chronology is intended to provide transparency regarding the District's cybersecurity investments while maintaining appropriate safeguards that protect digital privacy, safety, and security.

As the District continues to rely on technology to support teaching, learning, communication, and daily operations, protecting those systems has become increasingly important. School districts across the nation continue to face cyber threats such as ransomware attacks, phishing attempts, and unauthorized access to sensitive information. These incidents can disrupt school operations, impact instruction, and place student and staff information at risk.

To help address these challenges, the District maintains an ongoing cybersecurity program focused on protecting technology systems, monitoring for threats, responding to security incidents, and maintaining reliable access to critical services.

The District's cybersecurity efforts are guided by the National Institute of Standards and Technology (NIST) Cybersecurity Framework, a widely recognized model used by public and private organizations to manage cybersecurity risk. The framework provides a structured approach to identifying risks, protecting systems and data, detecting potential threats, responding to incidents, and restoring services when necessary.

Cyderes serves as an important cybersecurity partner by providing around-the-clock monitoring and support for the District's technology environment. Their services help identify potential threats, investigate suspicious activity, respond to security incidents, and strengthen the District's overall cybersecurity posture.

Please note that this chronology is intentionally written at a high level. Certain technical and operational details are not included in order to avoid disclosing information that could adversely impact the District's security posture.

Cyderes provides managed cybersecurity services that help protect the District's technology systems and sensitive information.

Key Services Include:

- Monitoring District technology systems 24 hours a day, 7 days a week to identify potential cybersecurity threats.
- Investigating suspicious activity and security alerts to determine whether action is needed.
- Responding to cybersecurity incidents and helping reduce the impact on District operations.
- Monitoring emerging cyber threats and vulnerabilities that could affect District technology systems.
- Providing expert cybersecurity guidance and recommendations to improve security practices.
- Supporting and maintaining security tools that help protect District systems and data.
- Continuously improving monitoring capabilities as new technology systems and services are added.

- Helping ensure technology services remain available, reliable, and secure for students and staff.

These services provide an additional layer of protection for the District by helping identify and address potential cybersecurity threats before they can cause significant disruption. The partnership with Cyderes supports the District's ongoing efforts to safeguard student, staff, and financial information while maintaining continuity of operations.

Procurement:

According to Board of Education Policy DJE II.B., the term "professional services" means services that require:

1. A degree in a particular professional field;
2. A license from a state oversight board or similar authority; or
3. The exercise of specialized skill, knowledge, creativity, or technical abilities.

Pursuant to Board Policy DJE Sections II.B and III.C.4, Cyderes meets the definition of professional services based upon its specialized cybersecurity skills, knowledge, and technical expertise.

Financial Impact:

Year	Cost
2026	$723,960 (included onboarding)
2027	$678,960 amount requested