DEANDORTON
TECHNOLOGY

June 18, 2026

Dr. Kermit Belcher
DeKalb County School District
1701 Mountain Industrial Boulevard
Stone Mountain, GA 30083

Dear Dr. Belcher:

Based on our recent discussion, it is our understanding that DeKalb County School District (DCSD) has expressed interest in Cybersecurity assessment services. Dean Dorton's Cybersecurity Risk and Compliance team is ready to assist DCSD in addressing these critical needs.

Scope and Objectives

Dean Dorton is proposing to deliver a Cybersecurity assessment that includes external and internal security testing services, as well as an optional Google Workspace security review, and an Attack Simulation testing.

Cybersecurity Assessments

Dean Dorton's Cyber Security Assessment Services are designed to provide organizations specific information about the state of their Information Security posture and to validate that key controls are working as expected. We offer a variety of services to accommodate any of your requirements, network architecture, and scenarios.

Our methodology follows project management best practices so you know at any point of time during the project what is going on, what the next steps are, and when you will receive your Security Assessment report. Our commitment to you is to deliver the Security Assessment Report when we said we would and to provide an easy-to-read report with incredibly insightful and actionable information.

External Security Assessment – The External Security Assessment is performed from outside the organization's security perimeter, usually from the Internet. During the External Assessment, we work closely with your IT department to make sure that all critical systems are in scope for the review.

Objectives:

- Identify all known systems and network vulnerabilities that could be exploited by an external hacker.
- Meet security assessment requirement for regulated entities even though it is now a common practice across all industries.
- Recommend additional controls to improve the external cybersecurity posture.

Assumptions:

- Up to 12 live IP addresses

Internal Security Assessment – The Internal Security Assessment is conducted from an organization's internal network to identify vulnerabilities on internal systems. In addition to vulnerabilities identification, the Internal Security Assessment also encompasses deep-dive security reviews of specific areas to include security configuration management, hardening, and best practice reviews. The Internal Security Assessment has multiple optional components to address multiple environments and scenarios: firewall configuration review, network security review, users' security review, endpoint security review, and wireless security review.

Objectives:

- Show the damage that a hacker who has gained access to the internal network can inflict.
- Meet security assessment requirement for regulated entities even though it is now a common practice across all industries.
- Recommend additional controls to improve the internal cybersecurity posture.

Assumptions:

- DCSD will provide necessary network access and credentials to conduct testing activities.
- Up to five (5) /24 internal subnets.
- About 360 servers.
- Internal vulnerability scanning and exploitation validation.

Combined, the External and Internal Assessments will cover the following control areas:

Cloud Security Review – More organizations are moving some or all their IT infrastructure and information in the cloud. Each cloud solution requires specific configuration settings to be enabled to ensure that the data and systems are protected from unauthorized access. Dean Dorton's Cloud Security Review is a measurement of an organization's security posture, with a higher number indicating more improvement actions taken. Our recommendations can protect organization from threats.

Objectives:

- Review security configuration settings of cloud storage.
- Report on the current state of the organization's security posture.
- Recommend configuration settings or additional controls to maintain the confidentiality of the data stored in cloud environments.

Assumption:

- Google Workspace in scope.

Attack Simulation **–** This engagement will consist of a simulated threat actor targeting the client's internal sensitive data, with the objective of obtaining access to this from data from the internal network. The scenario will assume a compromised user workstation. Testers are authorized to use technical attacks, command and control infrastructure, and credential theft methods to achieve their goals. The approach will focus on stealth and evasion ("low and slow") to realistically simulate a motivated attacker while adhering to industry-standard safety practices to minimize the risk of service disruption. Dean Dorton will begin the simulation with valid domain credentials and access to a domain workstation ("assumed breach" scenario. Dean Dorton will simulate a threat actor who is attempting to access sensitive data (which can be specified by DCSD) through various means including:

- Reconnaissance of network & organizational resources.
- Privilege escalation, including credential harvesting and further account compromise.
- Lateral movement between hosts and other resources.
- Data exfiltration attempts

Objectives:

- Assess detection and response capabilities in a simulated attack scenario, including:
    - Assurance that overall attack can be detected.
    - Determine effectiveness of potential response efforts.
    - Identification of potential blind spots and detection gaps / weaknesses.

Scope: Dean Dorton will include the following environments / components in scope (though not all may end up being accessed during the engagement

- Internal network / Active Directory environment.
- Microsoft Azure / M365.

- Google Workspace.

Dean Dorton will work closely with DCSD to minimize the risk of disruption to business operations that could be caused by these assessment procedures. The service necessarily involves the use of network tools and techniques designed to detect security vulnerabilities, and that it is impossible to identify and eliminate all the risks involved with the use of these tools and techniques.

Dean Dorton will finalize all its assessment activity and documentation of the security assessment into a final deliverable for the DCSD that includes remediation recommendations. It is our understanding that this report is intended for the information and use of the DCSD and is not intended to be, nor should be, used by anyone other than these parties.

Web API Discovery & Risk Assessment - In this engagement, Dean Dorton will work with DCSD to identify and classify web API usage across the organization, and evaluate potential risks that may arise. The engagement will consider internal APIs deployed by DCSD, as well as third-party APIs that DCSD is interacting with over the Internet. Dean Dorton will take a multi-phase approach as follows:

- Discovery
    - Collect documentation and interviews from DCSD staff about known API usage, for both internal and third-party systems.
    - Design and execute technical testing to collect data from various sources, including network scanning, network log analysis, and EDR systems analysis where appropriate.
    - Document resulting instances of API usage in a comprehensive inventory, classifying APIs based on data types, and including examples of associated data.
- Risk Analysis
    - Prioritize and review each API to determine capabilities.
    - Review any available testing data to determine actual API usage.
    - Document potential risks associated with each API and incorporate into risk registry.

Objectives:

- Produce an inventory of APIs used by DCSD and associated data, for ongoing risk assessment purposes.
- Provide a risk analysis of API usage, based on data classification and behavior.

Assumptions:

- Up to 50 hours will be spent on the discovery phase.
- DCSD will provide an internal point-of-contact for Dean Dorton when dealing with any third-party vendor or service.
- Up to 40 APIs will be analyzed in-depth for risk assessment purposes.

Staffing

Dean Dorton strongly believes that a team approach to this project provides the best possible deliverable for DCSD. As such, we will compile a team that consists of members from various areas of specialty within our Cybersecurity and Technology Consulting Group. If the need were to arise, we can also involve members from our accounting and business consulting groups. The combined experience of these resources will provide a fully qualified team that understands the compliance, technical, and practical aspects of your organization.

Pricing

Project	Description	Fees
Cybersecurity Security Assessment	• External Security Assessment • Internal Security Assessment	$30,000
	• Cloud Security Review (Google Workspace)	$5,000
	• Attack Simulation	$15,000
	• Web API Discovery and Risk Assessment	$31,000
Total		**$81,000**

Additionally, DCSD will be invoiced for all out-of-pocket administrative and travel expenses including mileage.

Terms

This engagement does not anticipate the compilation, review, or audit of financial records or financial statements. At no time shall any member of the Dean Dorton team make any management decisions on behalf of DCSD. We will only provide technical expertise, support and recommendations to management throughout this engagement. It will be your responsibility to assign a resource to act as our primary contact and to be responsible for making all decisions on behalf of DCSD.

In the unlikely event that differences concerning our services or fees should arise that are not resolved by mutual agreement, in order to facilitate resolution of the differences and to save all parties time and expense, DCSD and Dean Dorton agree to try in good faith to settle their differences by mediation administered by the American Arbitration Association under the *Dispute Resolution Rules for Professional Accounting and Related Services Disputes* before resorting to litigation. In the event that litigation cannot be avoided, DCSD and Dean Dorton agree not to demand a trial by jury.

If any portion of this letter is held to be void or otherwise unenforceable, in whole or in part, the remaining portions of this letter shall remain in effect.

Thank you again for the opportunity to assist DCSD in these matters. If you have any questions related to this proposal, please let me know.

Sincerely,

DEAN DORTON ALLEN FORD, PLLC

By: _____
Gui Cozzi

Cybersecurity Risk and Compliance Director

ACKNOWLEDGEMENT:

This letter correctly sets forth the understanding of DeKalb County School District:

_____ _____
Signature Date

_____
Printed Name