RFP 24-577 Proposal for Disaster Recovery as a Service (DRaas) Renewal 1

DeKalb County School District

January 7, 2025

Submitted by:

Alex Chitty
SENIOR ACCOUNT MANAGER, LAYER 3 COMMUNICATIONS, LLC
1450 Oakbrook Drive, Suite 900
Norcross, GA 30093
(770) 225-5300

Table of Contents

1. Addendum 1 and RFP 24-577

DeKalb County School District

1701 MOUNTAIN INDUSTRIAL BOULEVARD, STONE MOUNTAIN, GA 30083
https://dekalbschoolsga.ionwave.net/Login.aspx

TO: ALL OFFERORS UNDER REQUEST FOR PROPOSAL)

RFP 24-577 Disaster Recovery as a Service (DRaaS)

FROM: Procurement Department, DeKalb County School District

ADDENDUM NO. 1

RFP 24-577 Disaster Recovery as a Service (DRaaS) is hereby amended as follows:

1. This addendum was created to provide responses to the Q&A via IonWave.

2. All other conditions remain in full force and effect.

3. All offerors under this solicitation are kindly requested to acknowledge receipt of this Addendum 1 by signing the page below and uploading with your proposal.

COMPANY NAME/CERTIFYING OFFICIAL SIGNATURE

Q & A Response

The purpose of this document is to provide answers to vendor questions. Please see Questions and Answers included herein.

Solicitation Number: RFP 24-577	**Solicitation Title:** Disaster Recovery as a Service (DRaaS)
Requesting Department: Information Technology	**Date:** 1/4/2024
Buyer: Fred Christopher	**RFP Initially Posted to Internet:** 12/14/2023
Email Address: solicitationquestions@dekalbschoolsga.org	**Telephone:** 678-676-0120

RESPONSES MUST BE RECEIVED ELECTRONICALLY:

DEADLINE TIME - Before 2:00 PM, Tuesday, January 9, 2024

VIRTUAL PUBLIC ACKNOWLEDGEMENT OPENING
At 3:00 PM, Tuesday, January 9, 2024

RESPONSES TO BE OPENED: Beginning at 3:00 PM EST.

Via Microsoft Teams
DeKalb County School District
Purchasing Department
1701 Mountain Industrial Boulevard
Stone Mountain, GA 30083

#	Questions	Referenced RFP Section	Answers
1.	Due to the holidays and associated closures of businesses interested in providing competitive submissions, would the DCSD please extend the time for responses for two additional weeks: 1/23?		No.
2.	With regard to PART II GENERAL REQUIREMENTS,		No, this information is required at the time of proposal submission.

#	Questions	Referenced RFP Section	Answers
	section R. Financial Stability, would DCSD accept the proofs of financial stability upon notice of award instead of at response submission?		
3.	Due to the complexity of the response and holidays, is there a possibility of an extension of 30 days?		No.
4.	Are you looking more for a DRAAS software solution or DRAAS personal services?		The district is looking for a DRaaS software solution with operational support.
5.	How is the replication of the physical databases handled today? Would Dekalb keep that responsibility?		Physical databases are backed up to local tape and FedEx-ed to provider. Yes, it's not in the current scope. We are open to a value added solution if possible.
6.	How is DR for the IBM Power servers done today?		Backup LTO tapes are restored to the DR site and connectivity is made to test the availability of the data.
7.	How/Who does the management of Dekalb firewalls today?		The district manages the firewall.
8.	When is the expected timeline for implementation?		2nd or 3rd quarter 2024
9.	What version of VMware do you run on the production side?		version 6.5 - note: By the end of 1st quarter 2024, the district will be upgraded to the latest and greatest version
10.	Regarding the Indemnification section, is it limited to a strict 'yes or no' response, or is there an opportunity to modify it? For example, can we specify that the 'offeror will assume responsibility only for areas under its control'? Additionally, are you open to minor amendments to this clause?"		The indemnification language as stated in the solicitation is preferred. However, DCSD is willing to consider changes with the awarded vendor based on the reason for the changes.
11.	"13. DCSD would expect at least two weeks to assess potential impacts and implement mitigating measures in the event of an		DCSD is willing to consider changes with the awarded vendor based on the reason for the changes.

#	Questions	Referenced RFP Section	Answers
	emergency during an offeror outage" Are you open to minor amendments to this requirement?		
12.	What is expected to be proposed for Dekalb's networking environment? Can you provide a network tolopogy?		The expectation that the DR data is traversed across a secured link to the successful respondent.
13.	What is the business requirements for RPO / RTO? Solution price points will vary depending on RPO / RTO requirements.		RTO = 0-4 hr for critical applications, no additional information provided for RPO.
14.	DR Testing Events: What does Dekalb envision for these testing events? Testing in isolation? Full Failover and run for a maximum period of time?		Full failover testing
15.	What do you expect the x86 DR capacity to be? (Compute, memory and storage). Is the expectation is that you would activate all of the remote sites in the single DR location?		The district does not have a need for x86 DR capacity. A single DR location is acceptable as long as it is not in the SE region of the United States
16.	IBM i V7R1 is no longer supported, does Dekalb expect to bring this up to support?		The district currently has support for IBM iV7R2.
17.	On Prem IBM hardware (P7) is no longer supported, does Dekalb expect to bring this up to support?		The district currently has support for on-prem hardware and software.
18.	In regard to Part II, Scope of Work, B. Project Scope of Work, Item 1 - Access to site (page 21). In offering a cloud solution, the customer would not be allowed physical access to datacenter. Will this render the proposal non-compliant? The intended cloud solution data center can provide various certifications, if requested; will this still allow the District to meet it's facility and audit requirements?		Not allowing physical access to the data center will not render a respondent non-compliant. Yes, providing the district various certifications will meet the facility and audit requirements.

#	Questions	Referenced RFP Section	Answers
19.	Is all of the localized telecom equipment responsible for transmitting data to/from individual schools and facility buildings in scope of the DR? Ex: hurricane destroys 20% of facilities.		Servers and VMS are located at Core sites and route calls to local schools. Yes, telecom servers need to be included in the scope of the DR services.
20.	Cloud based solutions will provide network traffic conveyance inside the cloud up to the edge; is this satisfactory?		Yes, network traffic conveyance inside the cloud up to the edge is satisfactory. We are also looking for the solution to include connectivity from the edge of the proponent's cloud to the district's edge.
21.	Where do you anticipate connections to the DR site to be made from in the event of a disaster that removes the ones put in place already?		More information is needed to answer this question.
22.	What does the District's data change rate look like on a daily basis?		Data change rate is unknown; however, the district has provided a growth rate on p. 27 in the solicitation.
23.	Is there a single physical datacenter that the District can channel the migration traffic through?		Yes, there is one main data center.
24.	Will multiple fast connects to different datacenters be necessary?		Please include the cost for one on Attachment A. Please provide a cost option for a second and attach to Attachment A.
25.	We understand that there are 3 domain controllers, 57 physical ESX hosts (3 hosts per site), how many physical sites do these ESX hosts occupy?		The ESX hosts occupy two sites.
26.	Can you provide a diagram showing where your servers are - how many physical locations are your ESX servers located in? How many physical sites do these ESX hosts occupy?		No. The ESX hosts are located in two separate locations.
27.	What is 100% of your peak network demand to the production VMware servers? This		Unknown

#	Questions	Referenced RFP Section	Answers
	consideration will help to shape the connection needed to facilitate the traffic to the Cloud solution.		
28.	What are the characteristics of the 239 Virtual servers in production? i.e. Total virtual CPUs? Total memory assigned to those VMs?		See p.26 in the solicitation. Note: By the end of 1st quarter, this information will change.
29.	Please provide the characteristics of any physical servers that need to be included in the solution. Ex: CPU cores, memory, storage, network, etc. for each individual server		See p.26 in the solicitation. Note: By the end of 1st quarter, this information will change.
30.	What is the desired/required RPO & RTO for the DR solution?		Please refer to answer 13.
31.	What is the preferred connectivity to the DR datacenter? SD-WAN, MPLS, P2P, IPSC VPN		VPN, but subject to change.
32.	Is this the current Prod or DR system? Power 7 has been EOL since December 31, 2020.		It is production.
33.	If this is the Prod system are their plans to upgrade to a supported version? I.E. Power10		At this time, the district has no plans to upgrade.

DeKalb County School District	**Vendor Services Department** Procurement 1701 Mountain Industrial Boulevard Stone Mountain, Georgia 30083

REQUEST FOR PROPOSAL (RFP) 24-577

Disaster Recovery as a Service (DRaaS)

Schedule of Events

EVENT	DATE(S)	TIME	LOCATION
Solicitation Posts	12/14/2023		https://dekalbschoolsga.ionwave.net
Mandatory Pre-Proposal Conference	N/A	N/A	Via Microsoft Teams (registration required)
Mandatory Site Visit	N/A	N/A	N/A
IonWave Virtual Demo Session (Optional)	12/28/2023	11:00 AM	Via Microsoft Teams (registration required)
Deadline to Submit Questions (Q&A)	12/29/2023	12:00 PM	https://dekalbschoolsga.ionwave.net
Q&A Deadline Responses	1/4/2024	4:30 PM	https://dekalbschoolsga.ionwave.net
Submission Deadline	1/9/2024	2:00 PM	https://dekalbschoolsga.ionwave.net
Virtual Public Acknowledgement	1/9/2024	3:00 PM	Via Microsoft Teams (Registration required)

SUBMISSIONS MUST BE RECEIVED ELECTRONICALLY VIA https://dekalbschoolsga.ionwave.net

DeKalb County School District Solicitation Contact Person:
Fred Christopher, Procurement Manager III Non-Capital
(678) 676- 0120 and/or email at solicitationquestions@dekalbschoolsga.org

DeKalb County School District

1701 MOUNTAIN INDUSTRIAL BLVD, STONE MOUNTAIN, GEORGIA 30083

https://dekalbschoolsga.ionwave.net/Login.aspx

REQUEST FOR PROPOSAL

RFP 24-577

Disaster Recovery as a Service (DRaaS)

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT'D)

PART III – SCOPE OF WORK

ATTACHMENTS

DeKalb County School District ("DCSD") extends this offer to submit a proposal for the possible purchase or lease of goods and/or services conforming to the following designated specifications, terms, and conditions. This solicitation will require DCSD Board of Education approval.

Format and Submission of Proposals

Submittal responses to this solicitation will be received electronically on the DeKalb County School District website at ***https://dekalbschoolsga.ionwave.net/Login.aspx.***

The format requirements for RFP responses are designed to ensure uniformity in the responses, provide the information necessary to understand each offeror's proposal, and facilitate an efficient and comprehensive evaluation of all responses. Proposals must comply with the specifications and detailed instructions stated in this RFP document, be signed by the certifying company official, and be presented to the DCSD Purchasing Department according to the detailed instructions stated in this document.

- RFP responses must be submitted electronically via *https://dekalbschoolsga.ionwave.net/Login.aspx*.
- Proposals must be presented in a PDF format. All attachments must be identified properly for easy recognition and association.
- Each page of the response must be numbered.
- Each proposal must contain a detailed Table of Contents and must be organized in the same order as the requirements are outlined in this RFP document. Each separate bullet point must be addressed individually. A response that does not adhere to a "point-by-point" format may be disqualified.
- Responses shall be organized simply and economically. Emphasis must be placed on completeness and clarity. Proposals that do not include all the required information may be disqualified.

All potential respondents must register as a vendor at https://dekalbschoolsga.ionwave.net/Login.aspx.

Time is of the essence. Specify your earliest 6 weeks and latest 9 weeks service commencement dates after receipt of award letter.

Approval by the DeKalb County Board of Education
Official approval by the DeKalb County Board of Education is required for this procurement. No contract shall be construed to be formed without the advance official approval of the DeKalb County Board of Education. **The successful offeror will be notified after DeKalb County Board of Education approval.**

Funding Provisions
No award or contract will be made if funding is not approved by the DeKalb County Board of Education.

Compliance with Requirements
Offeror must indicate below whether or not their proposal is in complete compliance with the stated requirements. If there are any deviations from these requirements, offeror must indicate in writing what the exact deviations are and what actual services will be provided. Attach and label additional sheets if necessary.

_X__ Proposal is in complete compliance with proposal requirements.
___ Proposal deviates from stated requirements as follows:

_____

_____

_____

_____

Cancellation
Awards, contracts, and extensions may be canceled for convenience by the DeKalb County School District (DCSD) at any time. In the event of termination of contract by DCSD, the DCSD will be responsible only for those services that have been delivered and accepted according to the RFP requirements. Any cancellation for convenience by DCSD shall be effective three (3) business days after receipt of the Notice of Cancellation for convenience from DCSD by the Offeror.

Fiscal Year Funding Implications
The fiscal year for DCSD begins July 1 and ends June 30. This solicitation and any resulting contract(s) may contain renewal and extension options.
This solicitation, any resulting contract(s), and any renewal and extension options shall terminate absolutely without further obligation on the part of DCSD at the end of the fiscal year in which this solicitation was issued and at each June 30 renewal anniversary date thereafter unless the successful offeror is notified otherwise and agrees in writing to the exercise of renewal and extension options.

Payment to Successful Vendor(s)
Payment for goods and services will be made by electronic funds transfer (EFT). Vendor(s) doing business with DCSD are required to provide EFT payment information when registering as a DCSD vendor at: *https://www.dekalbschoolsga.org/purchasing/.*

Rights Reserved
DCSD reserves the right to accept or reject any and/or all parts of responsive proposals received and/or to reject all proposals submitted. DCSD reserves the right to award any resulting contract in the manner that is in the best interest of and most advantageous to DCSD. DCSD reserves the right to waive any technicalities or minor irregularities in responses received and to award the contract in the most beneficial manner for DCSD. The decision of DCSD shall be final.

DCSD reserves the right to request and negotiate a “best and final” response from offerors.

Taxes
Purchases made by DCSD are not subject to federal, state, or local sales tax. A Sales Tax Exemption Certificate will be furnished upon request.

F.O.B. Delivery
All prices are to be F.O.B. delivery to various DCSD locations.

Estimated Quantities
The quantities shown in this RFP document are estimates, which are provided for your information. However, actual quantities purchased by DCSD may vary.

Exclusions of Trade Usages
This RFP contains all of the terms, conditions and obligations to which the parties agree, and shall not be modified, controlled, explained, supplemented or affected in any way by any usage of trade not expressly included in this agreement.

Conditional Proposals
Proposals that are conditional and/or in any way qualify or vary the terms of these instructions, conditions, and specifications shall be considered non-responsive and disqualified.

Offeror Failure
In the event services to be furnished by the successful offeror should for any reason fail to conform to the scope of work contained herein, DCSD reserves the right to reject the services and further reserves the right to terminate the contract.

Failure of the successful offeror to perform contracted services may also result in the removal of that offeror from doing business with DCSD for a period of not less than one year.

Georgia Open Records Act
All proposals submitted in response to DCSD solicitations may be subject to the Georgia Open Records Act, which permits any member of the public to inspect and/or copy documents prepared and maintained or received in the course of the operation of the public office or agency.

No Assignment of Award
The successful offeror may not assign the award or contract to or subcontract with another party without the express written permission of DCSD.

The Laws of the State of Georgia
This RFP and subsequent agreement are subject to the laws of the State of Georgia.

2 CFR 200.322(a)
§ 200.322 Domestic preferences for procurements.
(a) As appropriate and to the extent consistent with law, the non-Federal entity should, to the greatest extent practicable under a Federal award, provide a preference for the purchase, acquisition, or use of goods products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, or other manufactured products).

Additional Terms
In the event an award is made to an offeror, the resulting contract shall not depart from this document unless agreed to in writing by DCSD and the successful offeror. DCSD shall not be bound by additional terms and conditions and/or extraneous language added to this document by offerors.

ALL SOLICITATIONS ISSUED BY DCSD ARE ADVERTISED IN THE LEGAL SECTION OF THE CHAMPION NEWSPAPER, POSTED ON THE DCSD IONWAVE WEBSITE, AND POSTED IN THE TEAM GEORGIA MARKETPLACE'S GEORGIA PROCUREMENT REGISTRY. *Offerors are solely responsible to review and make themselves aware of DCSD solicitations posted on the following website:*

https://dekalbschoolsga.ionwave.net/Login.aspx

PART I
BACKGROUND AND INFORMATION

A. Objectives

The DeKalb County School District (DCSD) is seeking proposals from qualified offerors with professional qualifications, technical competence, and specialized experience to provide **Disaster Recovery as a Service** as outlined in the scope of work in Part III of this RFP.

Awarded offeror shall provide services in accordance with the specifications, requirements and terms and conditions stated herein. Services shall include all labor, materials, tools, specialized equipment, supplies, trained personnel, insurance, travel, per diem, direct and indirect administrative costs, overhead, tolls, parking, fuel, lodging, all other cost and charges, and all things and services necessary to provide **Disaster Recovery as a Service**, in accordance with the requirements of this RFP. There shall be no add-on charges of any kind. DCSD reserves the right to make multiple awards.

B. General Information

DCSD is a metropolitan Atlanta public school system organized and existing under the Constitution and laws of the State of Georgia. DCSD is located in the fourth largest county in Georgia. DeKalb County is one of the most culturally diverse counties in the nation. DCSD has a student enrollment of approximately 93,000 students in pre-kindergarten through grade 12. With 139 schools and centers, DCSD educates the third largest pre-kindergarten through grade 12 student population in the State of Georgia. DCSD is the second largest employer in DeKalb County with approximately 14,000 employees.

DCSD is dedicated to giving every student the best possible education through an intensive core curriculum and specialized, challenging instructional and career programs. DCSD is striving to become the premier K-12 school system of choice and desires to significantly improve leadership, teaching, and student learning to fulfill its mission as an organization for public education.

DCSD includes approximately:

- 77 Elementary Schools
- 19 Middle Schools
- 22 High Schools
- 8 Start-up Charter Schools
- 12 Specialized Learning Centers
- 6 Administrative Centers, and
- 5 Athletic Stadiums

DCSD's wide-area network connects instruction and administration sites to deliver technology and learning tools to every child. The main administrative offices are located at 1701 Mountain Industrial Boulevard, Stone Mountain, Georgia 30083. DCSD is governed by a seven-member Board of Education.

C. Procurement Process

The procurement will be on a formally advertised basis. Proposals must be responsive to all aspects of this RFP.

D. Addenda

It is the responsibility of offerors to frequently check for any addenda, questions, and answers posted on the Purchasing Bulletin Board on the DCSD website. Failure on the part of offerors to make themselves aware of and comply with addenda requirements will not relieve them of this obligation.
All posted addenda must be printed, signed by the offeror, and included in the offeror's RFP submission. Click on the following link to the Purchasing Bulletin Board:

https://dekalbschoolsga.ionwave.net/Login.aspx

E. Proposal Contact Person
The assigned contact person for offerors is Fred Christopher, Procurement Manager III Non-Capital. Mr. Christopher can be reached at (678) 676-0217 or by email to ***solicitationquestions@dekabschoolsga.org.***

F. Prohibited Contact(s)
Except with the consent of the proposal contact person, all offerors, including any persons affiliated with or in any way related to the offeror, are strictly prohibited from contacting DeKalb County Board of Education members and DCSD employees or consultants on any matter having to do in any aspect with this RFP, other than as provided herein. Any and all contacts with such persons associated with DCSD shall be in writing, in appropriate circumstances or cases, as directed by the contact person. Furthermore, no employee, officer, or agent of the DeKalb County Board of Education or DCSD may participate in the selection, award or administration of a contract if he or she has a real or apparent conflict of interest.

Board Member Communication with Prospective Vendors
Vendors shall not contact Board members individually for the purpose of soliciting a purchase or contract between the time a request for proposal is formally released and a recommendation is made by the administration to the Board. If a vendor violates this prohibition during this timeframe, consideration for the vendor for award shall be invalidated. Board members shall be notified of possible violations and actions taken.

G. Virtual Demo Session
The DeKalb County School District Vendor Services department is hosting a virtual demo session on how to submit an electronic bid via IonWave. The virtual demo session will be held through Microsoft Teams on **Thursday, December 28, 2023, at 11:00 AM EST.**

Those who would like to attend the virtual session, must register no later than **Wednesday, December 27, 2023**, by **4:00PM EST**, by sending an email to ***solicitationquestions@dekalbschoolsga.org.***

Please enter **"Virtual Session – RFP 24-577 Disaster Recovery as a Service (DRaaS)"** in the subject line of your email. An invitation will be sent via Microsoft Teams to those participants no later than **Thursday, December 28, 2023, by 10:00 AM EST. (Attendance is not mandatory.)**

H. Mandatory Virtual Pre-Proposal Conference

This solicitation does not require a mandatory virtual pre-proposal conference.

I. Proposal Submission Deadline
Responses to this solicitation will be received electronically on the DeKalb County School District website at ***https://dekalbschoolsga.ionwave.net/Login.aspx.***

All potential offerors must register as a vendor at https://dekalbschoolsga.ionwave.net/Login.aspx.
Proposals in response to this RFP must be received by the DCSD Vendor Services Procurement Department via IonWave no later than **2:00 PM on Tuesday, January 9, 2024**. Proposals received after the stated deadline will not be considered.

J. Virtual Public Acknowledgement
The public acknowledgment will be held virtually through **Microsoft Teams on Tuesday, January 9, 2024, at 3:00 PM EST**. Those who would like to attend the acknowledgement, please register no later **than Monday, January 8, 2024, by 4:00 PM EST**, by sending an email to ***solicitationquestions@dekalbschoolsga.org***.

Please enter "**Public Acknowledgement** - **RFP 24-577 Disaster Recovery as a Service (DRaaS)**" in the subject line of your email.

An invitation will be sent via Microsoft Teams to those participants no later than **Tuesday, January 9, 2024, by 11:00 AM EST.**

K. Questions and Answers

It is intended that this RFP be adequate for any offeror to respond to DCSD's requirements. However, should offerors have questions, all questions shall be submitted electronically to: ***https://dekalbschoolsga.ionwave.net/Login.aspx.*** Questions submitted to any other mailbox, voice mail or e-mail address will not be considered for response. The deadline to submit questions is **Friday**, **December 29, 2024 at 12:00 PM EST**. Questions received after the deadline will not be considered. All questions received by the deadline shall be answered in writing and both the questions and answers will be posted to the website ***https://dekalbschoolsga.ionwave.net*** no later than **Thursday, January 4, 2024, at 4:30 PM EST.** Responses to questions will not be posted on official DCSD holidays.

PART II
GENERAL REQUIREMENTS

A. Offeror Performance

The successful offeror is required to perform and fulfill all the undertakings, covenants, terms, conditions, and agreements of this RFP document and any negotiated contract(s). Specifications contained herein and in the successful response will become contractual obligations if an award ensues. Failure of the offeror to fully perform these obligations may result in the cancellation of the award and contract.

DCSD will look to the offeror and his/her identified personnel to coordinate and deliver the services described in this RFP. The services shall not be delegated to sub-offerors or assigned to any third party.

B. News Release

Any news release or publicity pertaining to any phase of this project must be cleared through the DCSD Executive Director of Communications.

C. Non-Discrimination

DCSD does not discriminate based on race, color, religion, sex, national origin, age, or disability in any of its employment practices, education programs, services or activities.

DCSD supports an open, fair, and impartial free-market system which maximizes competition and seeks to include all responsible businesses and to provide ample opportunities for business growth and development. Minority businesses are encouraged and given the opportunity to bid on various projects; however, all responses will be evaluated on the same criteria. It is not the intention or desire of DCSD to restrict or impede competition, nor to increase the cost of the work.

D. Drug-Free Workplace

By submission of a response to this RFP, the offeror certifies that he/she and his/her employees shall not engage in the unlawful manufacture, sale, distribution, dispensation, possession, or use of controlled substance or drugs during the performance of the contract.

E. Smoke-Free Workplace

By submission of a response to this RFP, the offeror certifies that he/she and his/her employees shall not use tobacco products on DCSD property at any time during the performance of this contract.

F. Background Checks

A criminal background check must be performed on all contractors, consultants, subcontractors, volunteers and vendors (hereinafter jointly referred to as "Individuals") who provide services on DCSD premises, supervise services on DCSD premises, or has contact with students. These Individuals shall undergo the same criminal background check, within the last 365 days, as required by DCSD employees. Such background checks will be performed by DCSD at the expense of the Individual at a cost of $45.00 per individual.

Additionally, any charges against the Individual, may be deemed unacceptable in DCSD's sole discretion regardless of whether dismissed, expunged, sealed, removed from the record, treated as a "first offender" or dead docketed. Upon receipt and evaluation of DCSD's background check results, DCSD may demand that the Individual have no contact with DCSD students or parents, or provide services to DCSD premises.

Any failure of the contractor to obtain a criminal records background check through DCSD, as stated herein, may result in termination of any resulting contract between contractor and DCSD.

G. Costs Incurred

DCSD is not liable for any costs incurred by an offeror in preparing and/or submitting a response to this RFP or for any interview if requested. Any and all costs incurred by the offeror in preparing and/or submitting a response to this RFP and interviewing with DCSD (if requested) shall be the sole responsibility of the offeror and shall not be reimbursed by DCSD.

There is no guarantee of any offeror receiving an award as a result of submitting a response to this RFP.

H. Insurance

Certificate of Insurance and/or ACORD Form is required with solicitation submittal and required upon award. Upload this documentation under the Response Attachment tab via IonWave titled "Certificate of Insurance".

The DCSD Director of Risk Management sets insurance and indemnification requirements for each Solicitation.

Certificate of Insurance / Accord Form is required with solicitation submittal upon award. **Provision of Certificate of Insurance is a mandatory requirement.** Proposals submitted with certificates of insurance will be considered conditionally responsive to the insurance and indemnification requirement. Final award of this RFP will be contingent upon receipt within six (6) business days of request for insurance documentation complete with the following requirements and fully acceptable to the DCSD Risk Manager. No work will commence / no purchases will be made without the written statement of approval of insurance coverage from the DCSD Risk Manager. In the event the awarded offeror cannot produce insurance coverage acceptable to the Risk Manager within the time provided, DCSD reserves the right to award this solicitation to the first runner-up.

(1) The successful Offeror shall procure and maintain throughout the term of this agreement a policy or policies of insurance providing coverage as set forth below that shall protect the offeror and the Indemnitees (as defined in Part II, Section I of this RFP) from any claims for bodily injury, property damage, or personal injury which may arise out of offeror's operations under this agreement. The foregoing policies shall be obtained from insurance companies approved to do business in the State of Georgia and companies acceptable to DCSD. Offeror shall procure the insurance policy(ies) at the offeror's own expense and shall furnish to DCSD a certificate of insurance containing the following:

(a) Name and address of authorized agent;
(b) Name and address of insured;
(c) Name of insurance company;
(d) Description of coverage in standard terminology;
(e) Policy period;
(f) Policy Number;
(g) Limits of liability;
(h) Name and address of certificate holder;
(i) Acknowledgment to the DCSD of notice of expiration or cancellation;
(j) Signature of authorized agent;
(k) Telephone number of authorized agent; and
(l) Details of policy exclusions applicable to this agreement in comments section of insurance certificate.

All certificates evidencing primary and excess layers shall be renewed and kept current and up to date on an annual basis.

(2) Offeror is required to maintain the following insurance coverage during the term of this

agreement:

(a) Workers Compensation Insurance in the amounts of the statutory limits established by The General Assembly of the State of Georgia. Offeror shall have the ability to self-insure its required workers' compensation coverage if offeror is an approved self-insurer in the State of Georgia.

(b) Commercial General Liability Policy, or equivalent coverage, to include products and completed operations liability and contractual liability. The Commercial General Liability Policy shall have dollar limits sufficient to insure that there is no gap in coverage between this policy and any excess or Commercial Umbrella Policy described below.

(c) Automobile Liability Policy to include but not be limited to liability coverage on any owned, non-owned and hired vehicle used by offeror or offeror's personnel in the performance of this agreement. The Comprehensive Automobile Policy shall have dollar limits sufficient to insure that there is no gap in coverage between this policy and the excess or Commercial Umbrella Policy required under this agreement.

(d) Commercial Umbrella or Excess Liability Policy, which must provide the same or broader coverage than those provided for in the above Comprehensive General Liability and Business Auto Policies. Policy limits for the Commercial Umbrella or Excess Liability Policy shall have an annual occurrence and annual aggregate limit not less than $2,000,000 per claim.

(e) Professional Liability or Errors & Omissions coverage with limits not less than $2,000,000 per claim/$2,000,000 aggregate. The deductible shall not exceed $10,000 per claim.

(f) Under all coverage and certificates required hereunder, policies shall or be endorsed to include the following terms and conditions:

(i) All policies and coverage shall be on an "occurrence" not "claims made" basis (excepting (e) above)

(ii) The foregoing policies shall contain a provision that coverage afforded under the policies will not be canceled, or not renewed, allowed to lapse for any reason until at least thirty (30) days prior written notice has been given to DCSD.

(iii) Shall waive all right of subrogation against Indemnitees (as defined in Part II, Section I of this RFP) for losses arising out of this agreement.

(iv) A severability of interest or cross liability clause or endorsement applies to commercial general liability and excess liability policies.

(v) Certificates of Insurance showing such coverage to be in force shall be filed with DCSD prior to commencement or continuation of any work under this agreement.

(vi) All such coverage shall remain in full force and effect during the term and any renewal or extension thereof.

(g) Under coverage and certificates required under Sections 2(a), 2(b), (c), and (d) above, policies shall be endorsed to include the following terms and conditions:

(i) Minimum limits of $1,000,000 per occurrence $2,000,000 in the annual aggregate. Primary limits of coverage in the amount of $1,000,000 per occurrence must be with insurers approved to conduct business in the State of Georgia. Excess or umbrella liability insurance

may be placed with any insurer submitted by offeror, including captive or self-insured programs, with the prior written approval of DCSD.

(ii) Contractual liability coverage, specifically referencing this agreement and its Indemnity applies to liability assumed by the named insured.

(iii) Shall include Indemnitees as additional insured except on coverages (2) (a) and (2)(e).

(iv) Shall waive all right of subrogation against Indemnitees (as defined in Part II, Section I of this RFP) for losses arising out of this agreement.

(v) A severability of interest or cross liability clause or endorsement applies to commercial general liability and excess liability policies.

(vi) Shall be primary and not excess to any other coverage provided by or available to the Indemnitees (as defined in Part II, Section I of this RFP).

(h) Offeror shall require any and all subofferors performing work under this agreement to carry insurance of the types and with limits of liability as offeror shall deem appropriate and adequate for the work being performed. However, the obligations of the offeror to the Indemnitees assumed in Sections of Indemnification, and Insurance shall not be reduced or diminished by the standards set for the subofferors. Further, offeror agrees that their obligations to indemnify and insure the Indemnitees shall pertain to all losses arising out of the subofferor's acts or negligence in the same manner and to the same extent as if committed by the offeror. Offeror shall obtain and make available for inspection by DCSD, current certificates of insurance evidencing insurance coverage by such subofferors.

I. Indemnification

1) The successful offeror shall indemnify, defend, and hold harmless the DeKalb County School Board, the DeKalb County School District, DCSD, and their officials, officers, employees, agents, volunteers, and assigns (all of whom may collectively be referred to as "Indemnitees" throughout this RFP), from any and all claims, demands, suits, actions, legal or administrative proceedings, losses, liabilities, costs, interest, and damages of every kind and description, including any attorneys' fees and/or litigation and investigative expenses, for bodily injury, personal injury, (including but not limited to offeror's employees), or loss or destruction of property (including loss of use, damage or destruction of DCSD owned property) to the extent that any such claim or suit was caused by, arose out of, or contributed to, in whole or in part, by reason of any act, omission, professional error, fault, mistake, or negligence whether active, passive or imputed, of the offeror its employees, agents, representatives, or their employees, agents, or representatives in connection with or incidental to offeror's performance of the agreed-upon services regardless of whether such liability, claim, damage, loss, cost or expense is caused in part by an Indemnitee.

2) The successful offeror shall also indemnify, defend, and hold harmless the Indemnitees from any and all costs, expenses, claims, demands, rights, liabilities and causes of action inuring to offeror from events over which the Indemnitees exercise no control, such as Acts of God, strikes or government restrictions.

Offeror's obligation to indemnify any Indemnitee shall survive the completion, expiration, or termination of offeror's agreed-upon services for any reason.

J. Illegal Immigration Reform and Enforcement Act of

Upload this documentation under the Response Attachment tab via IonWave titled "IMMIGRATION SECURITY DOCUMENTATION".

The Illegal Immigration Reform and Enforcement Act of 2011 applies to and is a requirement for all DeKalb County School District solicitations for physical performance of services (i.e., public works contracts). **The Illegal Immigration Reform and Enforcement Act of 2011 does not apply to solicitations for items, commodities and products.**

Offerors must complete and/or have their subcontractors complete the following forms:

1) Immigration and Security Certification
2) Offeror E-Verify Affidavit
3) Contractor Affidavit (Contractor Only)
4) Subcontractor Affidavit (Subcontractor Only); and
5) Sub-Subcontractor Affidavit (Sub-Subcontractor Only)

The Immigration and Security Certification, the Offeror E-Verify Affidavit, the Contractor Affidavit, Subcontractor Affidavit and the Sub-Subcontractor Affidavit must be completed, notarized and submitted with your bid response.

I acknowledge the Illegal Immigration Reform and Enforcement Act of 2011 requirements for service providers and confirm by my signature below that the Immigration and Security Certification, the Contractor Affidavit, the Subcontractor Affidavit and the Sub-Subcontractor Affidavit are each completed, notarized and made a part of this solicitation response package. I also acknowledge that all items or services furnished to DCSD must comply with applicable federal and state immigration laws, and regulation.

_____Please check here if the Illegal Immigration and Reform Act of 2011 **does not** apply to your solicitation, because it is one for items, commodities, or products. If this does not apply to any portion of the solicitation, then the Offeror is not required to complete the Contractor Affidavit, the Subcontractor Affidavit and the Sub-Subcontractor Affidavit (reference Attachment page).

K. Interviews

DCSD reserves the right to require offerors to participate in one or more interviews with DCSD board members and/or staff. Offerors must be prepared to discuss the salient points of their proposal within two (2) normal working days of being asked to participate in interviews. There are to be no presentations, individually or collectively, without such invitation.

L. Contract Terms

In the event DCSD determines that outsourcing these services are in its best interest, with the approval of the DeKalb County Board of Education, the successful offeror will be notified in writing. A contract confirming firm fixed price and other terms shall be signed by the parties**. Services will begin on or about January 2024. The initial contract duration shall be through June 30, 2024**. The contract may contain **four (4) years extension options** contingent upon DCSD's offer of such extension, the successful offeror's acceptance and the approval of the DeKalb County Board of Education to extend the contract. The contract is subject to the approval of the DeKalb County Board of Education and to fiscal year funding limitations. The contract price must be held firm for the entire term of the contract.

DCSD reserves the right to terminate any resulting contract for convenience. In the event of contract termination by DCSD, the DCSD will be responsible only for those services and deliverables that have been received and accepted. Any cancellation for convenience by DCSD shall be effective three (3) business days after receipt of the Notice of Cancellation for convenience from DCSD by the offeror. Non-performance of contract terms shall give sufficient cause for DCSD to cancel the contract. Non-performance shall be construed to include, but is not limited to, failure of the offeror to deliver equipment or perform services in the time specified or in the manner required.

A contract is attached which includes all of the terms and conditions that the offeror must affirm and comply. ***Refer to Attachment I***, *Sample Service Agreement for Non-Capital Professional Services.* Please review DCSD's attached contract terms and conditions prior to submitting a response to this RFP. Offerors should plan on the contract terms and conditions attached to this RFP being included in any award as a result of this RFP. Therefore, all costs associated with complying with these requirements should be included in any pricing quoted by the offeror.

M. Permits and Applicable Laws

By submitting a proposal, offeror acknowledges its acceptance of the RFP specifications and the contract terms and conditions without change except as otherwise expressly stated in the submitted proposal.
If an offeror takes exception to a contract term or provision, the offeror must state the reason for the exception and state the specific contract language it proposes to include in place of the provision. Any exceptions to the contract must be submitted as an attachment to the offeror's response. Proposed exceptions must not conflict with or attempt to preempt mandatory requirements specified in the RFP.

Offerors shall at their own expense obtain all necessary permits, certifications, and licenses and shall comply with all applicable local, state, and federal laws, ordinances, rules, and regulations necessary to the full execution of the requirements stated herein. Offerors shall maintain all such permits, licenses, certifications, and compliances in a current status throughout the course of the contract. Offerors shall submit copies of permits, licenses, and certifications evidencing proof of the aforementioned immediately upon request of DCSD. Offerors shall be in compliance with registration with the Georgia Secretary of State's office as applicable.

N. Infringement

Offeror shall fully indemnify Indemnitees against any claims of infringement of any patent, copyright, trade secret, trademark, or other intellectual property rights related to the offeror's response to this RFP or services performed upon contract award. Offeror's obligation to indemnify any Indemnitee shall survive the completion, expiration, or termination of offeror's agreed-upon services for any reason.

O. Ownership Rights

DCSD shall retain ownership rights to the contents of all documents, supporting literature, and data submitted by offerors to this RFP.

P. Non-Collusion

Upload this documentation under the Response Attachment tab via IonWave titled "NON-COLLUSION"
Offerors shall fully certify that they, as individuals or as officials of a business entity, have not entered into any agreement, participated in collusion, or otherwise taken any action in restraint of free and competitive responses to this RFP. Further, offerors guarantee that their response is not made in conjunction with or on behalf of another party and that they have not been directly or indirectly induced in any manner or taken any action to result in a restriction of trade or in an unfair advantage.

Q. Conflict of Interest

Upload this documentation under the Response Attachment tab via IonWave titled "Conflict of Interest".
Offeror shall use its best efforts to disclose with their proposal the name of any officer, director, or agent who also is a DCSD employee, agent, representative, contractor, immediate family member (spouse, child, sibling, or parent or the spouse of a child, sibling or parent) or DeKalb County Board of Education member.

Offerors shall also disclose the name of any DCSD employee, agent, representative, contractor, immediate family member or board member who owns, directly or indirectly, an interest in five percent or more in the Offeror's company or any of its branches. In the event the Offeror was aware of a conflict of interest prior to the award of the contract and did not disclose the conflict DCSD may, at its discretion, terminate the contract for default. The Offeror further agrees that, if after award, a conflict of interest is discovered, an immediate and full disclosure in writing must be made to the DCSD Purchasing Department which must include a description of the action which the Offeror has taken or proposes to take to avoid or mitigate such conflicts. If a conflict of interest is determined to exist, DCSD may, at its discretion, cancel the contract. Offerors shall certify that their response

to this RFP is impartial, at arms-length, and free of any conflict of interest at this time, unfair advantage, or personal benefit to any DCSD official.

R. *Financial Stability*

Upload this documentation under the Response Attachment tab via IonWave titled "FINANCIAL STATEMENTS".

1. Offerors shall provide a copy of their company's audited financial statements for the previous two (2) years – 2021 and 2022. A certified audit is preferred however, an offeror's 2021 and 2022 tax returns and balance sheets will be accepted.
2. Indicate here if your company is publicly traded or not publicly traded:
   My company is publicly traded. _____/
   My company is not publicly traded. __X___/
3. If your company is a publicly traded company, provide a copy of your company's annual report for the previous two (2) years – 2021 and 2022.
4. List all civil and criminal proceedings your company has been the subject of, or named a party in, and provide the outcome of those proceedings. This list should include any lawsuits, administrative actions, or litigation to which your company is currently a party or has been a party. Please explain the basis for all claims, your response to those claims and state whether a settlement was reached, or a judgment entered.
5. State whether your company, or any affiliate currently or previously associated with your company, has ever filed a petition in bankruptcy, taken any actions with respect to insolvency, reorganization, receivership, moratoriums or assignment for the benefit of creditors, or otherwise sought relief from creditors.
6. State whether your company was the subject of any order, judgment or decree not subsequently reversed, suspended or vacated by any court permanently enjoining your company from engaging in any type of business practice.

S. *No Obligation/No Award Guaranteed/Cost to Propose*

This RFP does not commit DCSD to contract with any offeror to this RFP. There is no guarantee of any offeror receiving an award or contract as a result of submitting a response to this RFP. The contract, if any, will be awarded to the offeror whose proposal offers the best value to DCSD in meeting the required scope of work described herein, if the appropriate funds are available and the contract is approved by the DeKalb County Board of Education. No obligation or commitment is incurred by the DeKalb County Board of Education from the receipt of any proposal, marketing materials, or presentations. There is no guarantee that any offeror will receive an award as a result of submitting a proposal. Any/all costs incurred by the offeror in preparation and submission of this proposal are the sole responsibility of the offeror. Expenses incurred by the offeror will not be reimbursed by DCSD or become a reason for contracting with the offeror.

T. *Confidentiality and Non-Disclosure*

Information made available to offerors by DCSD shall be used only for purposes related to responding to this RFP and shall not be used for any other purpose without the express written permission of DCSD.

Offerors to this RFP unequivocally agree to assume responsibility for protecting and safeguarding the confidentiality of DCSD records that are not public information. Such information may include but is not limited to student and human resource file contents.

U. Business License

Upload this documentation under the Response Attachment tab via IonWave titled "BUSINESS LICENSE".

Offerors shall submit with their proposal, a copy of their valid company business license. If the offeror is a Georgia corporation, offeror shall submit a valid county or city business license. If the offeror is not a Georgia corporation, offeror shall submit a certificate of authority to transact business in the state of Georgia and a copy of their valid business license issued by their home jurisdiction. If offeror holds a professional certification which is licensed by the state of Georgia, offeror shall submit a copy of their valid professional license. Any license submitted in response to this requirement shall be maintained by the offeror for the duration of the contract.

V. Protest Process

This section describes the mandatory administrative procedure whereby Offerors submitting sealed competitive bids/proposals (hereinafter referred to as "bidders") to DCSD for proposals worth $100,000 or more may challenge the solicitation process, and whereby bidders/Offerors on sealed competitive bids directly related to Vendor Services for proposals worth $100,000 or more, may challenge contract awards.

1. **Protests**. A bidder may file a written protest challenging DCSD's compliance with applicable procurement procedures subject to the bidder's compliance with the provisions outlined below. Any such written protest will be resolved in accordance with these provisions:

   a) appropriate identification of the solicitation;
   b) a statement of reasons for the protest;
   c) supporting exhibits, evidence, or documents to substantiate any claims unless not available within the filing time (in which case the Offeror must proceed to file the protest during the filing period identified below but state the expected availability of the material); and the desired remedy.

2. **Types of Challenges.** Any bidder interested in and capable of responding to a competitive solicitation may file a protest with respect to the competitive solicitation process including, but not limited to, a challenge to specifications or any events or facts arising during the solicitation process. Any bidder submitting a timely bid/proposal in response to a competitive solicitation may file a protest with respect to DCSD's intended or actual contract award including, but not limited to, events or facts arising during the evaluation and/or negotiation process.

3. **Form of Protest**. At a minimum, the written protest must include the following:

   a) the name and address of the protestor;
   b) appropriate identification of the solicitation;
   c) a statement of reasons for the protest;
   d) supporting exhibits, evidence, or documents to substantiate any claims unless not available within the filing time (in which case the Offeror must proceed to file the protest during the filing period identified below but state the expected availability of the material); and the desired remedy.

   DCSD, at its discretion, may deem issues not raised in the initial protest as waived with prejudice by the protesting Offeror.

4. **Filing Protests.** A protest is considered to be properly filed when it is in writing, signed by a company officer authorized to sign contracts on behalf of the Offeror, and is received by the Vendor Services. The protest may be sent by any of the following means:

MAIL: Attention: Carla Smith, *Executive Director*
DeKalb County School District
Vendor Services
1701 Mountain Industrial Boulevard
Stone Mountain, Georgia 30083
Email: *solicitationquestions@dekalbschoolsga.org*

The Offeror must observe the following deadlines when filing a protest:

Type of Protest	Protest Filing Deadline
Challenge to Competitive Solicitation Process	Two (2) business days prior to the closing date and time of the solicitation as identified on the Invitation to Bid.
Challenge to an Intended or Actual Contract Award	In the event DCSD posts a Notice of Intent to Award ("NOIA"), the protest must be filed within ten (10) calendar days of the date the NOIA is posted.
	In the event DCSD does not post a NOIA, the protest must be filed within ten (10) calendar days of the date the Notice of Award ("NOA") is posted.

If a bidder fails to file a protest by the applicable deadline, such failure shall be deemed as a waiver with prejudice of any grounds the bidder may have for protest.

5. **Stay of procurement during protest review**.
When a protest challenging the competitive solicitation process has been timely filed at least two (2) business days prior to the closing date and time, the solicitation shall not close until a final decision resolving the protest has been issued, unless the facilities management department makes a written determination that the closing of the solicitation without delay is necessary to protect the interests of DCSD.

When a protest challenging an intended contract award has been timely filed, DCSD shall not proceed to actual contract award unless the **Vendor Services Department** makes a written determination that the issuance of a contract or performance of the contract without delay is necessary to protect the interests of DCSD. If it is determined that it is necessary to proceed with contract performance without delay, the bidder/Offeror with this contingent contract may proceed with performance and receive payment for work performed in strict accordance with the terms of the contract. The provisions of this paragraph are not applicable to a protest pertaining to events or facts arising during the solicitation process.

6. **Protest Resolution.**
The Vendor Services Department shall review and issue a written decision on the protest within seven (7) business days. This decision shall be deemed final. Available remedies for sustained protests are as follows:

- If a protest is sustained prior to the closing date and time of the solicitation, available remedies may include, but are not limited to, the following: modification of the solicitation document including, but not limited to, specifications and terms and conditions; extension of the solicitation closing date and time (as appropriate); and cancellation of the solicitation.
- If a protest of the intended/actual contract award is sustained, available remedies may include but are not limited to, the following: revision or cancellation of the NOIA/NOA, re-evaluation and re-award, or re-solicitation with appropriate changes to the new solicitation.

7**. Costs**
In no event shall a bidder be entitled to recover any costs incurred in connection with the solicitation or protest process, including, but not limited to, the costs of preparing a bid/proposal, the costs of participating in the protest process, or any attorney fees.

PART III
SCOPE OF WORK

A. Purpose/Project Overview

DCSD is seeking proposals for a **Disaster Recovery as a Service (DRaaS)** solution and to implement the DRaaS solution proposed. This Request for Proposals (RFP) documents DCSD's Disaster Recovery objectives and expectations and their solution, support, and pricing requirements in accordance with the scope of work of this RFP.

The DeKalb County School District serves over 92,000 students in Pre-Kindergarten through Grade 12. The breakdown of DCSD sites is as follows:

- 77 Elementary Schools
- 19 Middle Schools
- 22 High Schools
- 12 Specialized Learning Centers
- 4 Administrative Centers
- 5 Athletic Stadiums

The DCSD Data Center is in the William Bradley Bryant Center for Technology in Decatur, GA, one of the district's three Wide Area Network (WAN) core sites. Additional servers are at the other two core sites.

As our data center is in the Greater Atlanta Area, it is critical that the chosen offerors hosting site is NOT located in any of the southeastern states but is in the continental United States.

Awarded offeror shall provide equipment and services in accordance with the scope of work, requirements and terms and conditions stated herein. Services shall include all labor, materials, tools, specialized equipment, supplies, trained personnel, insurance, travel, per diem, direct and indirect administrative costs, overhead, tolls, parking, fuel, lodging, all other cost and charges, and all things and services necessary and in accordance with the requirements of this RFP. There shall be no add-on charges of any kind.

DCSD, at its discretion, determines the criteria and process whereby proposals are evaluated and awarded. No damages shall be recoverable by any challenger as a result of these determinations or decisions by DCSD.

DCSD reserves the right to add or remove DCSD facilities (schools, centers and portable classrooms) as needed.

DCSD reserves the right to make multiple awards and will be responsible for administration of this contract.

B. Project Scope of Work

The scope of this RFP is to encompass a DRaaS environment that includes:

1. DCSD access, as needed, to the DRaaS site (This would be used for facility inspection and audit requirements).
2. Cloud data storage and replication.
3. DCSD's ability to remotely configure and monitor assigned environments.
4. The requisite tools and support required to configure and monitor the environment. NOTE: DCSD is a VMWare shop and will be looking for DRaaS models that utilize the VMWare toolset. There are other standalone servers that will also need to be included with a cloud-based Disaster Recovery (DR) solution.
5. Pricing models and details that show basic charges for connectivity, tools, storage, processing, etc.
6. All backed up data is encrypted and in transit and at rest.
7. Perform up to four failover tests per year.
8. Must have a dedicated team to work with DCSD for support activities (or dedicated support).
9. Develop DR declaration run books to be used for daily operations, emergencies, and failover testing.

This RFP makes no attempt to dictate what the offeror infrastructure configuration should be to meet DCSD requirements. The expectation is that the bidding offerors will propose adequate solutions and options to DCSD, and the chosen offeror will include a discovery phase in their project plan to determine suitable configurations at the hosted site.

C. Minimum Requirements

This section documents DCSD's minimum requirements and expectations for a DRaaS solution. Please consider and provide detailed responses to all questions, requirements, and statements.

In addition, please complete the Security Questionnaire in Attachment K and include it with your response.

C.1 Considerations – (**Please label your response to this section as C.1 in your technical proposal**)

The information below should assist with the sizing and structure of services for the RFP response. Also, please refer to section D for an overview of DCSD's current data center environment.

1. DCSD utilizes VMWare for virtualization and wishes to find a DRaaS service that utilizes this tool set.
2. Document how non-VMWare servers will be replicated and restored.

3. The offeror should clearly document how their cloud based DRaaS solution functions.
4. The offeror should clearly document how data is replicated to the DRaaS service.
5. The offeror should clearly document the type of connectivity offered as part of their solution.
6. The offeror should clearly document how additional connectivity/bandwidth usage is managed/ handled when DCSD needs to utilize the DRaaS solution.
7. The offeror should clearly document how their own Disaster Recovery procedures and solution operate and what, if any, are the potential impacts to DCSD's DRaaS service.
8. The offer should document all service tiers, along with associated Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets, tier pricing and daily resource usage charges.
9. Offeror must prove scalability of their services and that they can support any changing and growing needs DCSD may have.
10. The offeror should be forthright about the size of their existing production customer base and the number of actual declarations that the offeror has supported over the past year.
11. It is preferable that the offeror provides a private cloud (non-shared infrastructure) solution rather than public cloud solution.

C.2 Meeting Requirements and Minimum Expectations

The RFP response must address all DCSD's requirements and expectations documented in this section. Please provide quantifiable details of your proposed solution along with any associated processes, procedures, and protocols. Copies of these documents should be provided if available.

If a requirement cannot be met please indicate the performance level offered or an alternative option.

The solutions proposed will be evaluated across all responding offerors and will be subject to scoring.

C.3 Support / Procedures - (Please label your response to this section as C.3 in the technical proposal)

1. The offeror's proposal shall allow for support up to four DR tests per year at the discretion of DCSD (please provide supporting processes and procedures). DCSD would expect that testing should last no longer than 12 hours.
2. The offeror must describe the timing and processes in place that describes the procedures for DCSD to create additional resources.
3. The offeror will need to express their own DR procedures and capabilities in the event the offeror's cloud platform encounters a disaster.
4. The offeror should describe the procedures for DCSD to unilaterally execute fail over into the DRaaS location.

5. The offeror should provide details if they are not solely responsible for elements of the solution including procurement, configuration, management, operation, monitoring, maintenance and alerting of all hosting systems.

6. Describe access requests and procedures, tools and applications that are required so DCSD resources can configure application and data changes using either the offeror's service portal or a request ticket.

7. The offeror shall provide a single point of contact for all incident, problem issues on a 7/24/365 basis.

8. The offeror shall be solely responsible for managing any incident, problem and changes that occur to the DRaaS infrastructure. The offeror should also provide root cause analysis on any incidents that arise and are remediated.

9. Provide the process for how requests, approvals and validation processes are communicated and managed.

10. Provide details on the offeror's role in managing operations failback from the cloud data center back to DCSD's production data center.

11. Provide details on how relevant infrastructure and/or tool set changes will be communicated to DCSD (sufficient time for DCSD to review and to provide input needs to be made available prior to implementation).

12. The offeror shall provide the processes and management for notification of both scheduled and emergency maintenance and/or down time to DCSD.

13. DCSD would expect at least two weeks to assess potential impacts and implement mitigating measures in the event of an emergency during an offeror outage.

14. Detail the fault tolerance, monitoring, alerting and notification processes for any hardware and power solutions that may affect DCSD (e.g., UPS, battery and server clustering). Detail how DCSD can access said monitoring.

15. The proposal response should express the time limit (if any) for DCSD to use the provided cloud based infrastructure once a disaster is declared; as well the incremental costs for recurring use.

16. Provide details on the extent which the offeror trains the customer's support staff in the use and management of the service.

17. Offeror to provide details of all financial institution/government regulations they must adhere to such as SOX, GLBA, FFIEC. DCSD is required to adhere to FERPA and HIPAA regulations.

C.4 Security (also see Security Questionnaire in Attachment K)

(Please label your response to this section as C.4 in the technical proposal)

1. Describe the provisions made for secure transfer of data from DCSD's primary site to the DRaaS site (with any associated costs/schedules).
2. Describe the offeror's policy with regard to data breach notification and follow-on mitigation.
3. Describe how personally identifying information for students and staff is protected and secured in transit and at rest.

C.5 Storage - (**Please label your response to this section as C.5 in the technical proposal**)

1. Detail tiered pricing and availability for data storage solution between DCSD's primary site and the DRaaS location with intermittent write access and transaction logging.
2. Describe how the offeror's solution will make sufficient storage continually available for incremental data replication from the primary site to the DR site; including the offeror's storage backup (DR) strategy.
3. Describe data recovery and certification of destruction process and procedures.

C.6 Network - (**Please label your response to this section as C.6 in the technical proposal**)

1. Offeror to describe how circuits between sites are fail safe and of sufficient bandwidth to handle 100% of DCSD peak demand.
2. Circuits into and out of the offeror cloud based location should support DCSD's existing environment and be described in detail (type, bandwidth, etc.). The offeror should include details on how they are managed, monitored and how alerts are communicated to DCSD when appropriate.
3. Describe bandwidth scalability as it pertains to potential DCSD future growth.
4. Describe how the offeror's solution will allow for coordinated configuration changes between DCSD and the offeror.
5. Provide details of the availability schema for DCSD to have network access assurance - the offeror solution should provide continuous availability of the network and DR site at all times.

C.7 Infrastructure – ((Please label your response to this section as C.7 in the technical proposal)

1. Provide a complete description of the proposed cloud based infrastructure including; quantities, configuration and models of equipment, applications, types of data storage, memory, CPU/servers, network, storage used to support the DRaaS solution.
2. The offeror must provide a sufficient cloud based infrastructure environment that will allow DCSD to build a suitable DR environment to support business processes.

3. The offeror shall describe their excess cloud based infrastructure capacity.
4. Provide details of expected performance and any degradation DCSD would experience should the offerors customers stress their environment to 100% of server capacity, storage capacity, and/or network capacity.
5. The offeror must provide details of the location of all DR cloud-based infrastructure.

C.8 Tools/Applications - **(Please label your response to this section as C.8 in the technical proposal)**

1. Provide details of any hardware/software tools required by DCSD to fully integrate to the offeror's hosting environment including; name, version, quantity, pricing.
2. Offeror to provide details of any offeror application or toolsets required to allow DCSD access to the DRaaS site to configure the servers, applications, memory and networks. Include versions/configuration details and associated costs. Also, the proposal must state if the they will be provided by the offeror or if DCSD must furnish and install.
3. Provide details of the virtual environment deployed and the tools/applications used.
4. Describe the options for conversion or accommodating DCSDs tools if the offeror does not utilize DCSD's VMware tools.

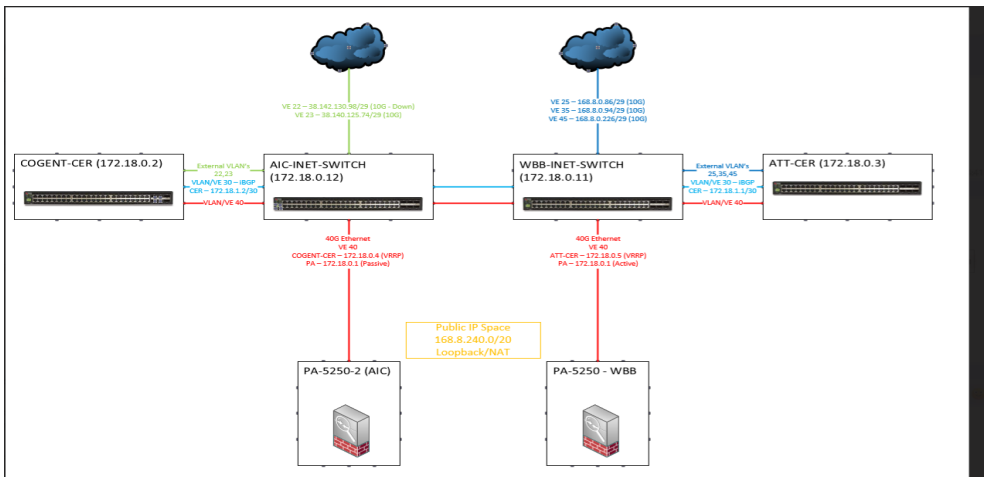
D. Existing Data Center / Discovery

D.1 Data Center Overview

Below is a summary of the current data center environment.

The Primary data center environment is (comprised of) managed VMware infrastructure with adequate storage for production data. The current infrastructure is detailed below; however, it is subject to change.

Data Center Environment	Notes
NETWORK	
Two ISPs, with circuits coming in at WBBC Data Center and AIC Core Site COGENT circuits at AIC 3x 10Gbps circuits (CER is named ATT) at WBB 2x40Gbps LAG between sites (80Gbps total)	WBB circuit (presumably AT&T) is the preferred default route. See Diagram below (or on the next page)



Cogent Circuit is DCSD owned fiber direct to 56 Marietta PeachNet Circuits are AT&T fiber with OSPF routing to PeachNet. OSPF is configured on ATT-CER which is sharing internal routes to provider	Utilization at 3:00 was 35-40% on most interfaces.
CPU/SERVERS	
3 Physical Domain Controllers	
1 Veeam backup server; 2 Exagrid appliances	
57 Physical ESX hosts Core Locations (9) (each has two 8 core CPUs) Head-End Locations (48) (each has single 6 core CPU's)	3 ESX hosts per each site
239 Virtual servers in production	Core Site resource utilization Average CPU/Memory – 26%/57% Head End Site resource utilization Average CPU/Memory – 26%/57%
5 Physical SQL servers	
1 IBM Power7 Model 8205 (OS400 V7R1) Native Applications: • CrossPointe/GUI • DB2 for i (RDBMS)	Partition 1 2 Processors (25% Typ), 36 GB RAM, 11.7 TB Storage (72%) Partition 2 1 Processor (5% Typ), 20 GB RAM, 5.7 TB Storage (43%) Partition 3 1 Processor (3% Typ), 6 GB RAM, 19.3 TB Storage (76.6%)
Approximately 269 total servers in production	
STORAGE	

Approximately 175 TB usable storage (virtual storage) Approximately 75 TB (Exagrid) Approximately 150 TB (Veeam Backup) Approximately 46TB (SQL, Local Storage, etc.)	Growth rate approximately 5% per year
MEMORY	
2,390 GB pre-allocated RAM	Reservation of RAM for the virtual servers is not uniform
Each physical server has 16 – 128 GB of 1866MHz RAM	
Hosts RAM utilization - 62%	

D.2 Data Center Discovery

The chosen offeror and DCSD will complete discovery of the DCSD Data Center and satellite sites. Discovery should include but not be limited to:

- Application Process Analysis
- Logical Data Connections Analysis
- Data Center Configuration Analysis
- Data Network Analysis
- Data Storage and Replication Analysis

E. Service Level Agreements (SLA)

The offeror should express their standard Service Levels Agreement (SLA) as part of this proposal and how it will be measured and reported with an example. Final SLA's will be determined as part of Contract negotiations. The offeror should detail customer compensation for unmet SLAs.

F. Cost and Contract Information

Expectations for pricing and contract options of this proposal are outlined below (explain in detail within proposal, provide in or attach to Attachment A – Cost Proposal Form):

1. The contract period is one year with four 1-year renewal options.
2. The offeror should clearly document contract termination options and charges. (**Please provide in Technical Proposal**)
3. Storage costs must be clearly articulated. (**Attachment A – Cost Proposal Form**)

4. Standard DRaaS pricing for base services must be clearly documented. (**Attachment A – Cost Proposal Form**)

5. Provide tiered pricing for the various services offered in a DRaaS model where available. (**Please attach to Attachment A – Cost Proposal)**

6. Separate pricing for DR testing on a "per test" basis should also be provided. (**Please attach to Attachment A – Cost Proposal)**

7. Complete network access and use pricing should be detailed in the proposal response, including any costs associated with variable bandwidth (burst) usage with minimum/maximum bandwidth pricing tiers.

G. Company Profile

Offerors to this Request for Proposal are required to demonstrate, and include with their submissions to this RFP, a full and complete company profile, to include, but not be limited to: the date of establishment, mission statement, type and confirmation of company's legal entity form, company's organizational structure/chart, principals' names and titles, company size in relation to industry, number of employees, company history, financial position, and all relevant current and past experience on similar projects, including the company's overall experience in providing **Disaster Recovery as a Service (DRaaS)**.

Compliance Information:

Companies must meet minimum criteria as specified to receive further consideration. Proposals shall include the following:

The submitting company must be licensed by the State of Georgia to provide all services specified in this RFP and all documents must be in the name of the submitting company.

Litigation Information (Y/N):

Identify and briefly discuss any instances in the past five (5) years where your contract was terminated, with or without cause. Provide Owner name, project name and Owner Project Representative Name and Number. For joint ventures responding to this RFP, provide the above information as it pertains to the joint venture and for each partner or entity creating said joint venture. **If there is no failure or failures to complete a contract, please include a statement that the Firm has never failed to complete a contract or contracts or have defaulted or have been declared in default on any contract.**

Identify any legal actions that have been filed against your company for services rendered in connection with in the past (5) years. Provide a brief explanation for each occurrence and the outcome/disposition. **If there have been no legal actions filed against your company, please include a statement that the Company has not had any legal actions filed against them in the past five (5) years.**

H. References

Upload this document under the Response Attachment tab via IonWave titled "References".

Offeror must provide the names and contact phone numbers of at least two **(2)** current references, preferably references comparable to DCSD, for whom the offeror is providing or has provided comparable services. Offeror's Reference Form (**Attachment E**), **References will be contacted.**

I. Brochures, Catalogs, Manuals, Websites, Literature

In addition to the formal response to this RFP, all offerors are encouraged to submit brochures, catalogs, manuals, website materials, industry literature, and any other marketing and informational media which will support and enhance their submission value.

J. Added Value

Offerors are encouraged to describe in detail all added value or additional services or benefits available and offered at no cost to DCSD in their RFP responses. Attach and label as **"ADDED VALUE."**

K. Evaluation Criteria

DCSD advertises this RFP as an opportunity for interested and qualified firms specializing in **Disaster Recovery as a Service (DRaaS)** to submit responses consistent with the scope of work stated herein. Respondents to this RFP are encouraged to submit their most comprehensive, innovative and creative proposals for services for DCSD.

DCSD may, at its sole discretion, select or reject all or portions of the service(s) proposed from responsive offerors. As a part of the evaluation process, DCSD may find it necessary to evaluate the addition or deletion of components of an offeror's proposal in order to make equivalent comparisons to other proposals. DCSD will select the offeror whose proposal DCSD determines best meets the needs of DCSD, based on the requirements and evaluation criteria set forth herein.

The determination of the successful proposal will be based upon information supplied by the offeror in the RFP response and upon other information that will be obtained by DCSD as it deems necessary. Proposal conformance to RFP instructions, terms, conditions, and requirements is critical to offeror responsiveness.

The lowest-cost proposal submitted may not necessarily be determined to be the most responsive and responsible proposal when all factors have been considered. However, the quoted price is an important factor in the determination of the selected proposal.

An Evaluation Committee will evaluate the proposals using the following criteria:

1. Firm's Overview (15 Points)

a. Provide a full and complete company profile to include, but not limited to Firm's name, address, headquarters and or branch office handling this project, as well as primary contact name, title, related telephone/fax numbers and email address.
b. State how many years licensed to do business under the name stated above. Describe firm ownership structure and history.
c. List the number of permanent employees and provide an organizational chart of the firm.
d. Provide a professional biographical summary (resume) including certifications and detailed outline of the role and responsibility of executive/management staff, and any staff or subcontractors that will be assigned to manage the **DRaaS** environment.
e. Provide the total number of current clients/owners and industries served.

2. **Scope of Services (35 points)**

   a. Please provide your company's detailed methodology and proposed strategy for providing **Disaster Recovery as a Service (DRaaS)** for DCSD as stated in Part III Scope of Work items B-E of this RFP.
   b. Provide the name and telephone number of the individual(s) that can be contacted in case of an emergency or for services needed after hours, holidays or weekends.
   c. Public or private cloud offerings and related security.

3. **Firm's Relevant Experience and Expertise (20 points)**

   a. Please list past experience providing **Disaster Recovery as a Service (DRaaS)** for other K-12 school districts that are comparable in size to DCSD. Experience with other comparable K-12 school districts is preferred however, experience with other public/governmental agencies comparable in size to DCSD is allowed. List no more than 10 projects and do list projects not completed by your company or completed more than 10 years ago. Please include the following for each project:

      1. Owner/Client Name and location.
      2. Nature of services provided.
      3. Owner/Client representative name, title, email address, and phone number
      4. Dates of Service (Start mm/yy and end mm/yy)
      5. Owner/Client size (number of facilities, employees/students, number of WAN core sites, etc.)
      6. Staff involved in providing the services who will also be assigned to DCSD.

4. **Professional References (10 points)**

   a. The company shall submit a minimum of three (3) written recommendations from current or previous clients/owners.
   b. The company shall provide their strategy to provide a positive working relationship with DCSD. This strategy must include actual examples of how the company has demonstrated their cooperation with other clients/owners.
   c. DCSD reserves the option of contacting any of the references provided to confirm information provided.

5. **Cost Proposal (20 points)**

   a. Indicate your proposed price to provide the services as stated in this RFP using **Attachment A – Cost Proposal Form** provided as part of this RFP.
   b. Please provide any and all pricing breakdown as requested on the **Attachment A-Cost Proposal Form**.
   c. The **Attachment A-Cost Proposal Form** shall not be altered in any way. Any alterations to the provided cost proposal form may cause your company to be deemed non-responsive and disqualified from further consideration.

Relative Weight	Evaluation Criteria	Score
15	Firm's Overview	
35	Scope of Services	
20	Firm's Relevant Experience and Expertise	
10	Professional References	
20	Cost Proposal	
100 points	**TOTAL SCORE**	

L. Transition Plan/Transition on Commencement of Contract

The awarded offeror shall assume full services in accordance with the award of the RFP. The awarded offeror shall coordinate and cooperate with DCSD's existing provider(s) to ensure a smooth and orderly transition with uninterrupted services.

Transition and Continuity of Service upon Expiration of Contract

Continuity of services is necessary to DCSD. The awarded offeror agrees to this philosophy and upon expiration of contract, agrees to:

a. Exercise best efforts and cooperation for an orderly and efficient transition to another provider or to DCSD.
b. Negotiate a plan in good faith with successor to determine the nature and extent of the phase-in, phase-out services required. The plan shall specify a date for services described in the plan and shall be subject to approval by DCSD. The existing provider shall provide sufficiently experienced personnel during the phase-in and phase-out periods to ensure that the imperious services in the contract are maintained at the required level of need and proficiency.
c. All DCSD property (including but not limited to, students and DCSD records, parts, equipment, facilities, keys, and materials) shall be returned to DCSD upon expiration of contract.
d. Offeror shall include in their response any DCSD or any subsequent contractor requirements if offeror is awarded this contract and does not retain this contract upon its expiration.

M. REQUIRED CONTENT / DOCUMENT CHECKLIST

All potential respondents must register as a vendor at https://dekalbschoolsga.ionwave.net/Login.aspx.

IMPORTANT NOTICE: Submittals to this solicitation will be received electronically on the DeKalb County School District website at **https://dekalbschoolsga.ionwave.net/Login.aspx.**

IonWave will not accept a bid submission without the required documents listed below. Failure to upload the required information and/or documentation required in this solicitation may cause the submission to be declared non-responsive and rejected.

Offerors are required to upload **one (1) pdf. copy electronically via https://dekalbschoolsga.ionwave.net/Login.aspx** of their response. Responses must be submitted on 8 ½" x 11" single-sided stock. Offerors must reply in a narrative to each requirement and question. "Understand and comply" responses are not acceptable. All RFP submissions must include the following items and attachments.

The Request for Proposals document, RFP 24- 577 Disaster Recovery as a Service (DRaaS) (MUST BE the first document in the submission); this document is located at http://www.dekalbschoolsga.org/solicitations

Table of Contents for your submission

- Addenda – Each individual Addendum must be printed, signed, and inserted immediately following the Table of Contents **(Upload Required)**
- Audited Company Financial Statements/Company Annual Reports for 2021 and 2022 (**Upload Required)**
- Business License **(Upload Required)**
- Certificate of Insurance **(Upload Required)**
- Attachment A – Cost Proposal Form/Fee Schedule **(Upload Required)**
- Attachment B – Non-Collusion **(Upload Required)**
- Attachment C - Conflict of Interest **(Upload Required)**
- Attachment D – Critical Paragraphs **(Upload Required)**
- Attachment E – Offeror's Client Reference Form **(Upload Required)**
- Attachment F – Statement of Confidentiality and Non-Disclosure **(Upload Required)**
- Attachment G – Suspension and Debarment Certification **(Upload Required)**
- Attachment H – Immigration & Security Certification **(Upload Required)**
- Attachment I – Sample Service Agreement
- Attachment J– Mandatory Service and Support Requirements **(Upload Required)**
- Attachment K- Security Audit Questionnaire **(Upload Required)**
- Attachment L- Signature Page **(Upload Required)**
- Technical Proposal **(Upload Required)**
- Brochures, Catalogs, Manuals, Websites, Literature, and other marketing media
- Added Value

3. Executive Summary

Layer 3 Communications, a wholly owned subsidiary of MGT Consulting (MGT), is a premier managed service, project service, and staffing firm. We are headquartered in Norcross, GA, and service customers globally with a heavy focus in the southeast United States. Layer 3 Communications was acquired in May of 2022 by MGT Consulting. MGT was founded in 1975 and is a purpose-driven, market-shaping leader committed to providing highly specialized solutions to solve complex, mission-critical problems that live at the top of the client leadership agenda. We partner with school districts, cities and counties, higher education institutions, and state agencies to help them achieve high-value, transformational change through our capabilities and industry knowledge, all powered by technology.

Our mission is to be the social impact and performance leader in our industry. Social impact is our "North Star." To achieve this goal, MGT has expanded its technology, education, and operational performance solutions to deliver performance improvement that lifts people's lives and impacts communities. By uniting passionate, like-minded people, we are helping drive greater social impact every day for the clients and communities we serve.

DeKalb County School District (DCSD) has published a Request for Proposal which outlines the requirements for their preferred disaster recovery solution. Our proposal provides details for a modern datacenter solution with high performance, resiliency, and visibility, offered as a service to ensure the environment is managed and maintained at the highest level.

Services will be hosted out of our datacenter space in QTS Dallas which offers DCSD a disaster recovery site in a different geographic region, as requested. We are proposing a private-cloud solution utilizing VMware licensing and dedicated infrastructure for DCSD.

All professional and managed services are provided by our US-based field and 24x7 Operations Center (OC) engineering teams. Layer 3 Communications will perform managed services in conjunction with DCSD staff. Layer 3 Communications will also meet on a periodic basis with the DCSD staff to report on the health, posture, and viability of managed assets.

A detailed explanation of the Layer 3 Communications, our services, and their associated costs is included throughout this document. We are prepared to begin within two weeks of written authorization to proceed. Thank you for your continued interest in Layer 3 Communications and our products and services. We are pleased to have the opportunity to present this proposal to DeKalb County School District for your review.

C. Minimum Requirements

C.1 Considerations

1.DCSD utilizes VMWare for virtualization and wishes to find a DRaaS service that utilizes this toolset.

Layer 3 Communications will leverage a complete solution utilizing Veeam's Data Platform to provide DRaaS for all virtual workloads.

2.Document how non-VMWare servers will be replicated and restored.

Utilizing Veeam, Layer 3 Communications will provide a target Cloud Connect repository in our Dallas, TX data center for replicas. Non-VMware servers will utilize Veeam agents (Windows, Linux) to create backup jobs and backups copy jobs. These backup copy jobs will be transmitted securely via Veeam Cloud Connect to a dedicated private cloud for DCSD backed by VMware.

Restoration of the backup jobs can be performed in two methodologies:
If local access to the DCSD Veeam Backup and Recovery console is available, an Instant Recovery or Restore can be initiated to the dedicated Dallas environment. If the local DCSD environment is unavailable, the repository will be rescanned from the provider side and backup jobs will be loaded in Dallas. Using the Dallas Veeam Backup and Replication console, an Instant Recovery or Restore job will be performed to convert the physical machine to a virtual machine. In the event of clustered disks or special instances, Layer 3 Communications will manually restore the server via a "bare metal" restore.

If awarded, Layer 3 Communications will work with DCSD IT staff to test and verify each physical server and create an action plan per server.

3.The offeror should clearly document how their cloud based DRaaS solution functions.

Utilizing Veeam, Layer 3 Communications will provide a target Cloud Connect repository in our Dallas, TX data center for replicas. Virtual Machines (VMs) local to DeKalb environments will be replicated to a dedicated private cloud for DCSD backed by VMware. DCSD virtual networks will be mapped and associated with corresponding dedicated virtual networks in Dallas for DRaaS. Veeam's Backup and Recovery console will provide access for Partial Failovers.

A Partial Failover occurs when the local network remains unaffected, and all connectivity is available for the target VM(s). One or more VMs may be tested during an arranged time window. To begin the initiation of a partial failover, DCSD or Layer 3 Communications will initiate the failover process from the customer Veeam Backup and Replication console. Upon entering a partial failover, the Network Extension Appliances power on both locally and at the failover/DR environment. Once both appliances are functioning and communicating, the target VM(s) power on as well. Veeam performs a network service check as part of the process to ensure full connectivity. If successful, The VM runs without issue and appears to be in the local network retaining the local IP information. For the initial Partial Failover testing, Layer 3 Communications will work with DCSD to identify VMs in each network

segment for testing purposes. During the testing period, any failures or issues will be remediated during the testing window or immediately following testing.

A partial failover is ended in two ways: Failover Undo and Failback. Failover Undo is generally reserved for testing purposes only. It allows failover from the Replica VM to the original production VM without saving any changes made during the testing window. Failback allows for any changed data to be written to the original VM in production. Depending on the size of changes, this could account for significant times to failback.

A Full Site Failover occurs when the local network is either unavailable or compromised. In this scenario, all VMs for a target environment are powered on based on preconfigured failover plans established in collaboration with DCSD via Layer 3 Communications engineers. During the Full Failover testing process, Layer 3 Communications will refine and finalize semi-automated processes for network and virtual machine changes. In addition, the following changes are made:

- Network gateways are relocated via scripting to Dallas and deprecated in DCSD environments.
- DCSD will change external DNS records based on preexisting documentation.
    - Should DCSD provide access to external DNS management, Layer 3 Communications will assist with DNS changes for failover.
- FW/Network/Access policies are validated to reflect Dallas production environment.
    - Dallas FortiGate FWs will be configured to match DCSD non-ADOM policies.
- DCSD VMs will be powered on via scripting based on predefined DR Tiers
- DCSD is asked to change any OS dependencies to reflect new environment.

Once a full site failover has been completed, DCSD and Layer 3 Communications will communicate expectations and timelines for resolution of original production environment. In the event of a prolonged DR scenario (greater than 48 hours), Layer 3 Communications will begin creation of a new Veeam environment to create local backups and replicas to the original Production environment or another data center for additional protection. When failing back to the original Production environment, an outage window will need to be identified. VMs will follow the same process as a full failover and be examined and verified for functionality with DCSD and Layer 3 Communications.

4.The offeror should clearly document how data is replicated to the DRaaS service.

Veeam utilizes its component Cloud Connect feature to provide secure, encrypted data transfer between local DCSD sites and the target Dallas, TX environment. There are two options for secure data transfer:

DCSD can use Veeam Cloud Connect directly to submit via ISP access (ports 6180 and 443) where job data is encrypted at rest and in flight.

DCSD can use a dedicated Point to Point connection (Dallas data center to 56 Marietta to DCSD local networks) to securely transmit data without sending via Internet connection. Layer 3 Communications would work with DCSD IT staff to establish direct connectivity between environments if this option is requested.

5.The offeror should clearly document the type of connectivity offered as part of their solution.

Layer 3 Communications will provide blended Tier 1 ISP connectivity in our Dallas, TX data center. Current ISP connectivity is offered through Cogent and Hurricane Electric. Optional Point to Point connectivity will be provided via Packet Fabric between the Dallas, TX environment to 56 Marietta via existing connectivity.

All above connectivity methodologies have an existing 10Gbps port connectivity per provider. Multiple connections can be made to increase capacity or larger than 10Gbps port connectivity can be made available upon request and additional fees.

6.The offeror should clearly document how additional connectivity/bandwidth usage is managed/handled when DCSD needs to utilize the DRaaS solution.

Connectivity at the DR site in Dallas, TX is in an "always available" state. Since Veeam and other services leverage continuous connectivity, Layer 3 Communications will provide a dedicated quota of bandwidth for DCSD. In the event of a DRaaS event, the connectivity would be readily available. If needed, bursting of ISP connectivity could be available. If awarded, Layer 3 Communications would perform an assessment of ISP usage at the current DCSD datacenter for in scope devices and VMs.

7.The offeror should clearly document how their own Disaster Recovery procedures and solution operates and what, if any, are the potential impacts to DCSD's DRaaS service.

Layer 3 Communications has a defined Business Continuity plan that can be made available upon award and request. Layer 3 Communications maintains survivability via our data centers in Suwanee, GA and Dallas, TX. The proposed environment for DCSD is a dedicated, private environment that will have defined Service Level Agreements (SLAs) and expectations for Recovery Time Objectives (RTOs)and Recovery Point Objectives (RPOs). This is separate from the provider's DRaaS environment. As a result, our 24/7/365 NOC/SOC/Data Center Operations Team will always be available to deliver all contracted services.

8.The offer should document all service tiers, along with associated Recovery Time Objective (RTO)and Recovery Point Objective (RPO) targets, tier pricing and daily resource usage charges.

Layer 3 Communications is proposing a dedicated environment for the DCSD DRaaS solution. This solution will encompass all workloads named within the Request for Proposal at the time of proposal. If additional workloads are requested, Layer 3 Communications will work with DCSD IT staff to identify solutions and resources.

As a result of a dedicated environment, Recovery Time Objectives (RTOs)and Recovery Point Objectives (RPOs) can be defined by DCSD and Layer 3 Communications to achieve optimal outcomes for recovery. As a result, tiered pricing and daily resource usage charges are nonapplicable.

9.Offeror must prove scalability of their services and that they can support any changing and growing needs DCSD may have.

Layer 3 Communications can scale as DCSD needs within a timely fashion. For example, this contract calls for dedicated 125TB of storage as outlined in the Request. If additional storage is needed, we have existing storage available that can be dedicated if purchased. If a significant increase in storage is needed, Layer 3 Communications has current relationships with vendors where 500TB and beyond storage can be acquired and provisioned within

45 days. Proof of scalability can be provided via publishing of current proposed solution and/or quotes with expected timelines of possible needed extension of subservices.

10.The offeror should be forthright about the size of their existing production customer base and the number of actual declarations that the offeror has supported over the past year.

Layer 3 Communications can be forthright about the fact we have a robust datacenter practice in which we host or support a large number and variety of customer. We are happy to provide a redacted list of customers and offerings per customer, if required. If needed, Layer 3 Communications can also provide additional customer references pertinent to this proposal where Layer 3 Communications provides similar DRaaS offerings. However, we cannot publish information regarding size and declarations in a public bid document.

11.It is preferable that the offeror provides a private cloud (non-shared infrastructure) solution rather than public cloud solution.

Layer 3 Communications is proposing a private cloud (non-shared infrastructure) solution for most services. Certain services such as ISP connectivity will use a shared resource but will be securely provisioned and allocated via quotas to provide assurance of services and data integrity.

C.2 Meeting Requirements and Minimum Expectations

The RFP response must address all DCSD's requirements and expectations documented in this section. Please provide quantifiable details of your proposed solution along with any associated processes, procedures, and protocols. Copies of these documents should be provided if available.

If a requirement cannot be met, please indicate the performance level offered or an alternative option.

The solutions proposed will be evaluated across all responding offerors and will be subject to scoring.

Layer 3 Communications' proposed solution meets and, in some cases, exceeds the requirements and expectations detailed throughout the RFP document. We have addressed each requirement with a response and welcome any questions that may arise.

C.3 Support/Procedures

1.The offeror's proposal shall allow for support up to four DR tests per year at the discretion of DCSD (please provide supporting processes and procedures). DCSD would expect that testing should last no longer than 12 hours.

DR testing for up to four tests per year will be available for DCSD. DR Testing and validation can be verified through several methodologies via both synthetic testing and full site failover testing, if needed. Layer 3 Communications can provide guidelines for testing windows to achieve a 12-hour testing window.

2.The offeror must describe the timing and processes in place that describes the procedures for DCSD to create additional resources.

Per section C2, Layer 3 Communications can scale the environment to accommodate additional resources. Layer 3 Communications would ask that communications be initiated by DCSD through their L3C assigned Account Manager. Depending on the scale and need of resources, resources might be available same day and up to 45 days for storage and server needs. Layer 3 Communications will work with DCSD IT staff to review requests and provide a timeline for resource allocation on a case-by-case basis.

3.The offeror will need to express their own DR procedures and capabilities in the event the offeror's cloud platform encounters a disaster.

Layer 3 Communications infrastructure is replicated between our datacenters in Suwannee, GA and Dallas, TX. Client site connectivity is maintained to both locations. In the event of a loss of service at either location, the full production environment can be run at the other site by simply moving services to the active location. Network connectivity automatically fails over via the use of dynamic routing protocols. Secure remote access enables our engineer to work in the environment remotely. Our DR plan is fully documented and tested on an ongoing basis. The plan and the results of our most recent test are available on request.

In the event of a disaster in our Dallas, TX data center, DCSD would be notified of an event and provided with timelines for remediation. As a stopgap, services would be provided, on demand, in our Suwanee, GA data center until services in Dallas are restored or moved to another data center that meets the geographic requirement.

4.The offeror should describe the procedures for DCSD to unilaterally execute fail over into the DRaaS location.

DCSD would unilaterally execute a failover via a Full Site Failover. Full Site Failover occurs when the local network is either unavailable or compromised. In this scenario, all VMs for a target environment are powered on based on preconfigured failover plans established in collaboration with DCSD via Layer 3 Communications engineers. During the Full Failover testing process, Layer 3 Communications will refine and finalize semi-automated processes for network and virtual machine changes. In addition, the following changes are made:

- Network gateways are relocated via scripting to Dallas and deprecated in DCSD environments.
- DCSD will change external DNS records based on preexisting documentation.
    - Should DCSD provide access to external DNS management, Layer 3 Communications will assist with DNS changes for failover.
- FW/Network/Access policies are validated to reflect Dallas production environment.
    - Dallas FortiGate FWs will be configured to match DCSD non-ADOM policies.
- DCSD VMs will be powered on via scripting based on predefined DR Tiers
- DCSD is asked to change any OS dependencies to reflect new environment.

Once a full site failover has been completed, DCSD and Layer 3 Communications will communicate expectations and timelines for resolution of original production environment. In the event of a prolonged DR scenario (greater than 48 hours), Layer 3 Communications will begin creation of a new Veeam environment to create local backups and replicas to the original Production environment or another data center for additional protection. When failing back to the original Production environment, an outage window will need to be identified. VMs will follow the

same process as a full failover and be examined and verified for functionality with DCSD and Layer 3 Communications.

5. The offeror should provide details if they are not solely responsible for elements of the solution including procurement, configuration, management, operation, monitoring, maintenance and alerting of all hosting systems.

Layer 3 Communications is solely responsible for all elements of the solution being proposed.

6. Describe access requests and procedures, tools and applications that are required so DCSD resources can configure application and data changes using either the offeror's service portal or a request ticket.

Upon award, access requests and procedures will be initiated via a support ticket as outlined via the single point of contact. Layer 3 Communications will work with DCSD IT staff to provide both physical and virtual access to systems as needed with secure end to end management.

For physical access for vendors and staff, communications should be sent ideally 24 hours in advance to ensure the highest quality of service. All vendors and staff are required to provide a legal State issued ID for access to the data center environment.

Access to the dedicated virtual environment will be approved on a per case basis. It is the preference of Layer 3 Communications to limit administrative access to the environment. Additionally, RBAC will be enforced via domain-based credentials. For security reasons, we will not provide local accounts to the virtual environments.

Access to firewalls, network switches, and Out of Band systems will be maintained and limited to Layer 3 Communication employees. Health checks or status updates of these systems will be provided to DCSD IT staff.

Moves/Adds/Changes/Deletions (MACDs) to the environment should be documented via a support ticket.

7. The offeror shall provide a single point of contact for all incident, problem issues on a 7/24/365 basis.

Layer 3 Communications' Network Operations Center is staffed 24 hours a day. It can be reached via email at support@layer3com.com or via phone at (770) 225-5279. We ask that the NOC is considered the single point of contact for all incident and problem issues.

In addition, Layer 3 Communications primary point of contact for DCSD regarding anything related to sales or account management is Alex Chitty. Layer 3 Communications can be reached for sales assistance by:

a. Calling Alex Chitty (Sr. Account Manager) cell phone at (404) 441-8151
b. Emailing Ryan Greene at achitty@layer3com.com
c. Calling our main office line at (770) 225-5300

If DCSD cannot reach Alex for sales or account management activities and requests, the escalation process is to contact:

a. Scott Faxon (Vice President of Sales)
    i. Cell (404) 992-5100

   ii. Email sfaxon@layer3com.com
b. Rodney Turner (President)
   i. Cell (404) 307-5803
   ii. Email rturner@layer3com.com

We aim to provide DCSD with the highest level of customer service, therefore we feel it's important to always make multiple points of contact available to DCSD.

8. The offeror shall be solely responsible for managing any incident, problem and changes that occur to the DRaaS infrastructure. The offeror should also provide root cause analysis on any incidents that arise and are remediated.

Layer 3 Communications is proposing a fully managed solution for DRaaS infrastructure. As part of our standard approach, incidents that result in trouble tickets are investigated, analyzed, and remediated by our Network Operation Center and engineering resources. A root cause analysis (RCA) report will be provided to DCSD IT when these issues arise.

9. Provide the process for how requests, approvals and validation processes are communicated and managed.

Support/Managed Service requests may be submitted by phone, email, or via an online support portal. New support requests immediately notify our 24x7x365 NOC, email local engineering resources, the Support Manager and local on call engineer. All requests are centrally tracked and managed using the Layer 3 Communications case management system.

Layer 3 Communications can be reached for support by:

a. Emailing support at support@layer3com.com

b. Calling (844) 352-9373 or (770) 225-5279

c. Opening a ticket via the Layer 3 Communications support portal at https://layer3.force.com/support

Initial Response Escalation:

Cases open by email or through the support portal are expected to receive an initial response within 30 minutes. After 30 minutes have passed, the first escalation is automatically triggered by the case management system to the NOC Manager.

Support Technical Escalation Process:

a. Contact the NOC by calling or emailing support (see above)

b. Account Engineers – escalated by NOC Engineer or NOC Manager

c. Subject Matter Expert – escalated by Account Manager, Account Engineer, or NOC Engineers

d. Specific Vendor Support – escalated by the NOC or Account Engineers

Support Management Escalation Process:

a. Support / NOC Manager – Jack Maxfield

    a. Cell - (770) 329-3761 / Work – (770) 613-4015 / Email – jmaxfield@layer3com.com

b. Director of Engineering (Eastern Region) – Andrew Kozlowitz

    a. Cell (731) 234-1195 / Email – akozlowitz@layer3com.com

c. Director Managed / Advanced Services – Brad Goodman

    a. Cell (912) 659-2732 / Email – bgoodman@layer3com.com

d. Director Security Services – Alan Jones

    a. Cell (205) 223-8004 / Email – ajones@layer3com.com

General Ticketing Resolution Process:

When a support request is received, the NOC Engineer working with the request will perform the following steps:

- Ensure that a ticket is generated for the request. The ticket should minimally include the following information:

    a. Customer Name

    b. Customer Contact information

    c. Description of the support request

    d. Priority of the support request

    e. Initial Manufacturer (if applicable)

If the Customer is not already established in the ticket system, the NOC Engineer should create the required company object, including the base domain name, and ensure the customer contact is linked to company object.

- Triage the request directly with the customer to validate the request matches the actual description of the request. The initial customer contact is required within 30 min from the time that the request was made

(assumes the request was electronically made). If the original request varies from the actual issue, the NOC engineer should update the case notes with the correct data.

- If the support request can be remediated within the NOC, then the case should be closed immediately upon completion of the ticket. Case notes describing the remediation are recommended in cases not resulting in a return merchandise authorization (RMA).
- Where required, NOC engineers will utilize one of the following escalation paths:
    f. Daytime (M-F 8am-5PM EST) – first call escalation will go to the account SE. If the account SE is unavailable, then one of the subject matter expert (SME) engineers defined in the ticketing system should be used.
    g. Afterhours – first call escalation will go to the appropriate regional on-call engineer. If the on-call engineer for that regional account is unavailable, then the opposite regional on-call engineer should be used. If both on-call resources are unavailable, the escalation path defined in 4A should be used.

        *The NOC engineer will still maintain the case through escalation. Case notes describing the remediation are recommended.

- Where manufacturer technical assistance center support (TAC) is required, the NOC engineer will include the manufacturer case number and case notes regarding remediation.
- Where the Manufacturer TAC is engaged and the ticket is marked urgent (defined as all systems down) or the manufacturer SLAs has been exceeded, the NOC will engage the account manager and the support manager to intervene with TAC. If engineering resources outside of the NOC are utilized, the regional SE manger should be included in this process.
- Where the customer requires executive engagement in the support request, the support manager or account manager will engage with the Regional Engineering Director(s) and the Executive Director of Sales for the appropriate region.
- Follow up for support tickets that fall into step 5 or 6 of this process will be facilitated at the quarterly business review (QBR).

10.Provide details on the offeror's role in managing operations failback from the cloud data center back to DCSD's production data center.

Upon a full site failover to the DR site, DCSD and Layer 3 Communications will communicate expectations and timelines for resolution of original production environment. In the event of a prolonged DR scenario (greater than 48 hours), Layer 3 Communications will begin creation of a new Veeam environment to create local backups and replicas to the original Production environment or another data center for additional protection. When failing back to the original Production environment, an outage window will need to be identified. VMs will follow the same process as a full failover and be examined and verified for functionality with DCSD and Layer 3 Communications.

11.Provide details on how relevant infrastructure and/or tool set changes will be communicated to DCSD (sufficient time for DCSD to review and to provide input needs to be made available prior to implementation).

As part of the solution onboarding, Layer 3 Communications will request contact information for the appropriate DCSD IT staff for provider tool changes, maintenance of DR environment, maintenance of services, etc. These changes are generally sent 1 business week in advance except for critical security alerts or similar high impact issues. Similarly, the expectation is that DCSD provide communications when changes are made to their primary environment that might impact DRaaS systems and services.

12.The offeror shall provide the processes and management for notification of both scheduled and emergency maintenance and/or down time to DCSD.

Scheduled and emergency maintenance will be coordinated with DCSD IT staff. All maintenance will be logged in a ticket for tracking purposes.

For maintenance requiring down time, Layer 3 Communications will request an approved outage window from DCSD. A rollback plan will be identified prior to the start of the outage window. DCSD IT will be notified once maintenance is complete and services are back up and running.

If, for whatever reason, the maintenance is not complete by the end of the approved outage window, Layer 3 Communications will rollback and reschedule the maintenance window.

For maintenance not requiring downtime, Layer 3 Communications will create a ticket and make DCSD IT aware of the reason for the maintenance. The ticket will be rolled up into our Quarterly Business Review report.

13.DCSD would expect at least two weeks to assess potential impacts and implement mitigating measures in the event of an emergency during an offeror outage.

Layer 3 Communications will always strive to provide a two-week assessment period for DCSD IT staff. If two weeks is unable to be maintained for any reason, Layer 3 Communications will communicate the reasons for the adjusted outline.

14.Detail the fault tolerance, monitoring, alerting and notification processes for any hardware and power solutions that may affect DCSD (e.g., UPS, battery and server clustering). Detail how DCSD can access said monitoring.

Layer 3 Communications has engineered a fault tolerant solution for the proposed solution. Physically, Layer 3 Communications is providing a single cabinet in our Dallas, TX with 30A (24A daily max) N+1 power, backup UPS, diesel power generation, and redundant underfloor cooling. Power to the building is provided via two separate substations.

The dedicated infrastructure will provide 5 servers for its DRaaS solution. Each server will have two 18C CPU for a total of 72 logical processors per server. Each server will have 448G of RAM. Storage will be allocated to the dedicated hosts via a minimum of 2 10Gbps redundant links.

For monitoring, Layer 3 Communications will leverage Veeam ONE for monitoring and alerting of the DRaaS solution. L3C will alert identified DCSD IT staff via Veeam One emails. Access to Veeam One will be provided to DCSD staff as requested. Veeam One access will be reachable via web access for defined internal DCSD networks. For this solution, we will create baseline monitoring of incoming replica jobs to the DR site, health status of the DRaaS environment (CPU, Memory, disk, etc.), and the health of the local Veeam environment (with the assistance

of DCSD IT staff). Layer 3 Communications will request a concise list of IT staff or distribution group (preferred) for notifications.

15.The proposal response should express the time limit (if any) for DCSD to use the provided cloud-based infrastructure once a disaster is declared; as well the incremental costs for recurring use.

Layer 3 Communications is providing a dedicated environment for DCSD's DRaaS solution. The environment can be used at any point in time, without a time limit, for the duration of the contract. The solution is designed for ease of management and overall cost reduction compared to other service providers. The solution does not account for "on demand" functionality for additional workloads or software licensing required by on demand. Additional "on demand" functionality can be achieved if needed but is not priced or provided in this response. Layer 3 Communications will continuously work with DCSD IT staff over the contract to identify current and projected impacts on the DRaaS environment based on Production needs. Layer 3 Communications will provide quarterly analysis of the environment and communications on the overall health.

If DCSD needs to exceed the dedicated environment and utilize on demand resources, Layer 3 Communications will indicate costs and timelines for usage of those environments. In this scenario, additional licensing may be needed to service the solution (i.e. Microsoft SPLA licensing). Layer 3 Communications will also strive to provide the best, streamlined, cost mindful solution for DCSD.

16.Provide details on the extent which the offeror trains the customer's support staff in the use and management of the service.

Layer 3 Communications will train DCSD IT staff on accessing and navigating the DRaaS environment, Veeam One monitoring, and any included tools we will be providing as part of this solution. This training will occur in a one-time engagement after implementation and prior to the first quarterly business review. Access and navigation instructions will be provided via PDF as well. This training will enable DCSD IT to confirm the health and performance of the disaster recovery environment.

17.Offeror to provide details of all financial institution/government regulations they must adhere to such as SOX, GLBA, FFIEC. DCSD is required to adhere to FERPA and HIPAA regulations.

Layer 3 Communications is not required to adhere to any financial institution/government regulations. Layer 3 Communications has a firm understanding of FERPA and HIPAA regulations. Layer 3 Communications' DRaaS solution will not expose any protected data within the DRaaS environment.

C.4 Security Questionnaire (Attachment K)

1.Describe the provisions made for secure transfer of data from DCSD's primary site to the DRaaS site (with any associated costs/schedules).

Veeam utilizes it's Cloud Connect feature to provide secure, encrypted data transfer between local DCSD sites and the target Dallas, TX environment. There are two options for secure data transfer:

DCSD can use Veeam Cloud Connect directly to submit via ISP access (ports 6180 and 443) where job data is encrypted at rest and in flight.

DCSD can use a dedicated Point to Point connection (Dallas data center to 56 Marietta to DCSD local networks) to securely transmit encapsulated data without sending via Internet connection. Layer 3 Communications would work with DCSD IT staff to establish direct connectivity between environments if this option is requested.

Both options are included in the scope of this response and have been evaluated by both Veeam and Layer 3 Communications.

2.Describe the offeror's policy with regard to data breach notification and follow-on mitigation.

It is Layer 3 Communications' standard policy is to notify a client of a data breach pertaining to client data immediately upon discovery. The DCSD IT contacts identified as points of contact during the early stages of the project will be notified with all known details of the breach. As discovery, response, and remediation procedures are completed, DCSD will be made aware of any details regarding DCSD breeched data.

3.Describe how personally identifying information for students and staff is protected and secured in transit and at rest.

Layer 3 Communications' solution does not expose student or staff information during transmittal or at rest. The solution provides protections in the following fashions:

- An immutable repository at the DRaaS site for backup jobs.
- Layer 3 Communications does not have administrative access to underlying VM's OS or applications.
- Due to the dedicated environment, DCSD controls end to end security of the environment.

Attachment K
RFP 24-577
Disaster Recovery as a Service (DRaaS)
Security Audit Questionnaire

Item No.	SECURITY AUDIT QUESTIONNAIRE	Comply (Yes)	Do Not Comply (No)	Other (explain in remarks)	Remarks/Comments
PS	**Personnel Security/Auditing**				
PS-1	Do you provide background/credit/education/drug screening of employees involved in the delivery of your service?	Yes			Layer 3 Communications performs background checks for criminal and educational screening purposes.
PS-2	Do your personnel sign non-disclosure and confidentiality agreements?	Yes			If requested, our employees sign non-disclosure and confidentiality agreements. Usually this is at the discretion of the customer on a per case basis
PS-3	Does an internal security awareness policy exist for employees?	Yes			L3C has an internal security awareness policy.
PS-4	Does the cloud provider have an information security program that includes policies on (please attached relevant polices):	Yes			Layer 3 Communications has an information security program that covers all relevant topics.
PS-4a	• Data encryption	Yes			
PS-4b	• Data handling (secure use, storage, and destruction of sensitive data)	Yes			
PS-4c	• Data classification	Yes			
PS-4d	• Physical access	Yes			
PS-4e	• Electronic access	Yes			
Item No.	**SECURITY AUDIT QUESTIONNAIRE**	**Comply (Yes)**	**Do Not Comply (No)**	**Other (explain in remarks)**	**Remarks/Comments**
PS-4f	• Data retention	Yes			
PS-4g	• Security configuration standards for networks and operating systems	Yes			

Item No.	SECURITY AUDIT QUESTIONNAIRE	Comply (Yes)	Do Not Comply (No)	Other (explain in remarks)	Remarks/Comments
PS-4h	• Security patching	Yes			
PS-4i	• Vulnerability management	Yes			
PS-4j	• Prevention of computer viruses	Yes			
PS-4k	• Alternate site plan	Yes			
PS-4l	• Disaster recovery plan	Yes			
PS-5	Are employees kept abreast of changes to the security policy?	Yes			Notifications are announced annually or via email.
PS-6	Are employees aware of the process for reporting security incidents (please attach relevant process description)?	Yes			Yes. Employees report incidents, as outlined, to our security team for analysis, processing and possible remediation.
PS-7	Is there an internal audit group responsible for reviewing the information security environment?		No		There is a defined group for reviewing information security environments and policies.
PS-8	Do contracts with your offerors require a minimum level of security from the offeror?	Yes			No. As a service provider we often meet our customers "as is" and from a secure position provide resources to provide services.
PS-9	When an employee leaves the company, are access privileges immediately revoked?	Yes			Yes. Privileged access is removed and active sessions are revoked after password changes and removal of roles.
PS-10	Are visitors required to sign-in, be issued an identification badge, and be escorted while on the premises?	Yes			For our data centers, visitors must be provided access in advance, provide identification, and must be escorted for the duration of the visit.
Item No.	**SECURITY AUDIT QUESTIONNAIRE**	**Comply (Yes)**	**Do Not Comply (No)**	**Other (explain in remarks)**	**Remarks/Comments**
PS-11	Are access logs for the facility maintained for 30 days? Are the logs accessible by Customer's?	Yes			Logs are maintained by the data center provider. Additional logs for cage and cabinet access are also logged.
PS-12	Does the company have policies on removable media in the data center?	Yes			Our data center practice prohibits the use of removal media except in instances of maintenance purposes.
PS-13	Do third parties have physical access to the data center space where your cloud infrastructure is located?		No		Our data center is secured by keyed access by roster to our cage. In our cage, each cabinet is secured by badge access. Third party access is prohibited.
PS-14	Are the facility's premises separated into different control areas such as data center floor, loading/delivery areas and others?	Yes			The data center is separated into different control areas with assignable permissions per rostered individual.

Item No.	SECURITY AUDIT QUESTIONNAIRE	Comply (Yes)	Do Not Comply (No)	Other (explain in remarks)	Remarks/Comments
PS-15	What are the hours of operation of the security facilities at the data center?				Our data center facility is available 24/7/365.
PS-16	Is there CCTV monitoring the data center floor?	Yes			The data center has CCTV coverage.
PS-17	Are loading dock or delivery areas monitored by CCTV?	Yes			
PS-18	What is the retention policy on CCTV feeds?				30 days
PS-19	How is your cloud environment separated from other entities within the same data center?	Yes			We have a secured cage by key access. Within the cage we have secured access by badge to cabinets.
PS-20	Describe the fire suppression solution used in the data center.				Dry pipe fire suppression system
PS-21	Are temperature and humidity controls in the data center restricted to authorized personnel only and separated from the rest of the facility?	Yes			Temperature and humidity controls to the data center are restricted to only authorized personnel.
PS-22	Are there procedures in place to control the removal of property from the facility?	Yes			Removal of property from the data center is restrcited to authorized personnel.
Item No.	**SECURITY AUDIT QUESTIONNAIRE**	**Comply (Yes)**	**Do Not Comply (No)**	**Other (explain in remarks)**	**Remarks/Comments**
PS-23	Is there a holding area for deliveries at the data center where internal doors can be secured while external doors are open?	Yes			Deliveries are secured from the rest of the data center and controlled by access to and from the floor.
PS-24	How are power and communications cables physically separate?	Yes			Power is delivered under the raised floor vs low voltage above
PS-25	Are there locked/alarmed conduit boxes?	Yes			UPS systems that supply power feeds are secured.
PS-26	Are inventory records maintained of all hardware?	Yes			We maintain an inventory of managed racks
PS-27	Do you sweep for unauthorized devices attached to cables?	Yes			The data center is reviewed for issues weekly.
PS-28	Does the facility include the following physical security elements?	Yes			The facility includes all physical security elements
PS-28a	• Electronic access control	Yes			
PS-28b	• CCTV monitoring	Yes			
PS-28c	• Alarm systems, windows, doors, server areas, etc.	Yes			

Item No.	SECURITY AUDIT QUESTIONNAIRE	Comply (Yes)	Do Not Comply (No)	Other (explain in remarks)	Remarks/Comments
PS-28d	• On-site security guards	Yes			
PS-28e	• Building specifications	Yes			
PS-28f	• Identity badge procedures	Yes			
PS-28g	• Logging of site access	Yes			
Item No.	**SECURITY AUDIT QUESTIONNAIRE**	**Comply (Yes)**	**Do Not Comply (No)**	**Other (explain in remarks)**	**Remarks/Comments**
PS-28h	• Power and network redundancy	Yes			
PS-28i	• Power surge protection	Yes			
PS-28j	• Fire suppression systems	Yes			
PS-28k	• Heating/air conditioning	Yes			
LS	**Logical Security/Auditing**				
LS-1	Please provide a copy of your information security policy.	Yes			
LS-2	Does a separation of duties exist between individuals who authorize access, personnel who enable access, and personnel who verity access to your infrastructure?			Other	In most cases, yes. In other cases where personnel with knowledge of systems are limited, no
LS-3	Are all critical system clocks and times synchronized, and do logs include a date and time stamp?	Yes			All critical system clocks and times are syncronized when possible
LS-4	Do access control logs contain successful/unsuccessful login attempts and access to audit logs?	Yes			Access control logs contain audits of successful and unsuccessful logins.
LS-5	Do audit trails include a record of individual or process identity, date, time, function performed, and the resource(s) accessed?	Yes			Logs contain these records.
LS-6	Does a formal log review process exist?	Yes			Logs are sent to our SIEM for analysis and review
LS-7	Are system logs unalterable (e.g., use write-once technology or equivalent protection)?			Other	Logs are immediately sent to SIEM rather than saved for possible alteration

Item No.	SECURITY AUDIT QUESTIONNAIRE	Comply (Yes)	Do Not Comply (No)	Other (explain in remarks)	Remarks/Comments
LS-8	Are all activities on the networking infrastructure performed by personnel with unique logins and are logged?	Yes			When available
Item No.	**SECURITY AUDIT QUESTIONNAIRE**	**Comply (Yes)**	**Do Not Comply (No)**	**Other (explain in remarks)**	**Remarks/Comments**
LS-9	Do you provide two-factor authentication?	Yes			For appropriate systems that have capability
LS-10	Are installation and offeror-default passwords provided with new hardware, system software, etc. reset before they go into production?	Yes			
LS-11	Do administrators and remote users have individually assigned user identities and passwords?	Yes			
LS-12	Do systems notify users of their last successful login to their account?			Other	For systems that provide this information, Users are able to see this information
LS-13	Are all activities on the virtualization layer performed by personnel with unique logins and are logged?	Yes			
LS-14	Are access scripts with embedded passwords prohibited?	Yes			
LS-15	Are system administrators the only people who have administrative privileges?	Yes			
LS-16	Are your support representatives able to access DCSD data?		No		L3C Employees do not have access to DCSD data
LS-17	Is an automatic computer screen locking facility enabled for system administrators? This would lock the screen when the computer is left unattended for a certain period.	Yes			Automatic logouts for systems are enabled
LS-18	Do you periodically check your network to ensure that no unauthorized equipment has been attached to it?	Yes			Weekly checks are performed
LS-19	Does the company have the appropriate controls in place to cooperate with investigations by law enforcement officials? Do collection of evidence policies and procedures exist?	Yes			

Item No.	SECURITY AUDIT QUESTIONNAIRE	Comply (Yes)	Do Not Comply (No)	Other (explain in remarks)	Remarks/Comments
Item No.	SECURITY AUDIT QUESTIONNAIRE	Comply (Yes)	Do Not Comply (No)	Other (explain in remarks)	Remarks/Comments
LS-20	Once there has been a successful full backup, would you then have access to the DCSD's VM OS admin passwords?		No		L3C employees do not have privileged access to VMs and is not a requirement.
LS-21	Do your underlying portal management systems ensure that DCSDs cannot access networks and systems owned by other DCSDs, and does it present no ability to bypass the management interface to the underlying infrastructure?	Yes			Networks are clearly documented and seperated
MR	**Monitoring/Request Management**				
MR-1	What controls does your company have in place to monitor the cloud infrastructure capacity?	Yes			VeeamOne, Nagios, vCenter
MR-2	Do your clients have access to a monitoring portal?	Yes			On a per case and per service basis
MR-3	Is there an option to receive alerts directly from your monitoring solution?	Yes			This is a standard practice
MR-4	Can you monitor logs for specific event codes or error codes?	Yes			Logs off all devices can be ingested into our SIEM if needed
MR-5	Do you have a process we would follow to request support assistance? Please indicate in the ***Remarks/Comments*** section.	Yes			Submit a ticket to support@layer3com.com or via phone at 770-225-5279
MR-6	Can your ticketing system integrate with DCSD's? (Incident IQ)	Yes			Some integrations can be made
MR-7	Do you provide trending reports on capacity and performance?	Yes			Via Veeam ONE reporting
DR	**Data backup/business continuity/disaster recovery**				
DR-1	Does your company have a formal written business continuity policy?	Yes			Can be available upon request

Item No.	SECURITY AUDIT QUESTIONNAIRE	Comply (Yes)	Do Not Comply (No)	Other (explain in remarks)	Remarks/Comments
DR-2	Does your company provide business continuity plan writing services?			Other	L3C can assist with the creation of a business continuity plan. Customer would be required to provide input and specifications.
Item No.	**SECURITY AUDIT QUESTIONNAIRE**	**Comply (Yes)**	**Do Not Comply (No)**	**Other (explain in remarks)**	**Remarks/Comments**
DR-3	Is the distance between the backup recovery facility and the primary location adequate to ensure that one incident does not affect both facilities?	Yes			Primary site is in GA. DR site is in TX.
DR-4	Does the recovery location use different power and telecommunications grids from those used by the primary site?	Yes			Primary site is in GA. DR site is in TX.
DR-5	Do you have insurance coverage for business interruptions or general service interruptions, regardless of the reason?	Yes			Insurance coverage is for Layer 3 Communications. Policies do not include customer equipment or environments including service environments.
DR-6	Does your company carry cyber-insurance? Does this cover identity theft, cyber-extortion, cyber-terrorism, information asset network security and network business interruptions?	Yes			Layer 3 Communications maintains cyber-insurance.
DR-7	Is there a communication plan in place for notifying DCSDs that a major event has occurred and could potentially impact service delivery?	Yes			Communication methodologies and templates are prepared.
DR-8	Do you have an established recovery time objectives in the event of a disaster?	Yes			Layer 3 Communications has RTOs and RPOs for it's environments.
DR-9	Do you have a retention standard for standard server backups? Please indicate in the ***Remarks/Comments*** section.	Yes			Minimum of 7 days with immutable backups. Depending on system importance, there are established ranges from 14 to 90 days of retention
DR-10	Do you have an auto or self- provisioned backup solution for your public cloud? If so, please describe the features it offers based on previous questions asked about backups.		No		Layer 3 Communications restricts access by customer Public IP and has defined access rights and quotas to services.
DR-11	Would the recovery location use different power and telco grids from those at the primary site?	Yes			Primary site is in GA. DR site is in TX.

Item No.	SECURITY AUDIT QUESTIONNAIRE	Comply (Yes)	Do Not Comply (No)	Other (explain in remarks)	Remarks/Comments
VI	**Vulnerability/intrusion detection**				
VI-1	Please describe your general network security and intrusion detection system/intrusion protection system (IDS/IPS)?	Yes			Security honey pots, SIEM logs analysis and near real-time correlation of data.
Item No.	**SECURITY AUDIT QUESTIONNAIRE**	**Comply (Yes)**	**Do Not Comply (No)**	**Other (explain in remarks)**	**Remarks/Comments**
VI-2	How does your company prevent Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks? Please indicate in the ***Remarks/Comments*** section.	Yes			Dedicated hardware for DDoS scrubbing and mitigation and/or strategies to direct traffic.
VI-3	Are third party vulnerability assessments conducted?	Yes			Assessments are conducted annually by rotating providers
VI-4	Are penetration tests conducted?	Yes			Annual penetration testing of extenal and internal resources
VI-5	Describe your incident response procedures. Please indicate in the ***Remarks/Comments*** section.				Primarily incidents are received by our NOC or SOC. Incidents from our SIEM have enriched data with initial analysis. Incidents can then be escalated.
VI-6	Are tools in place to monitor and manage file integrity?	Yes			
VI-7	Is vulnerability assessment management in place?	Yes			Annual penetration testing of extenal and internal resources
	Compliance/Certifications				
CC-1	Does the company comply with existing US Department of Commerce Safe Harbor registrations and certifications and EU Data Privacy regulations?			Other	Layer 3 Communications complies with Safe Harbor regristrations but is not applicable for EU Data Privacy regulations as it does not apply toL3C and its current customer base.
CC-2	Does your company comply with FERPA?	Yes			
CC-3	Does your company comply with HIPAA?	Yes			
CC-4	Does your company comply with additional data privacy and security standards? Please indicate which ones.			Other	SOC 1, SOC 2, HITRUST, PCI DSS, FISMA, ISO 27001
CC-5	Are your facilities and/or environments PCI certified?	Yes			

Item No.	SECURITY AUDIT QUESTIONNAIRE	Comply (Yes)	Do Not Comply (No)	Other (explain in remarks)	Remarks/Comments
CC-6	When was the most recent SSAE 16 review performed? Please indicate in the ***Remarks/Comments*** section.	Yes			Q4 of 2023. SOC2 Reports available upon request.

Layer 3 Communications' Employee Security Policy

1. Overview

The following policy is designed to promote and enforce quality security practices for Layer 3 Communications. These polices shall be reviewed quarterly.

1.1 Purpose

The purpose of these policies is to outline the appropriate usage of information technology resources and confidential information at Layer 3 Communications. These policies are in place to protect the employee, clients as well as Layer 3 Communications.

1.2 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Layer 3 Communications, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Layer 3 Communications and all employee owned equipment used for Layer 3 Communications business purposes.

1.3 Enforcement

These policies should be read and interpreted by all Layer 3 Communications employees, contractors, consultants, temporaries, and other workers at Layer 3 Communications. Failure to comply with any of these policies can result disciplinary action up to and including termination of employment.

2. Acceptable Use

All systems issued to or purchased for employees, including all computer systems and software, media, facsimile and telephony equipment are the property of Layer 3 Communications. These items are to be used for business purposes in serving the interests of the Company and its clients in the course of normal operation. As a condition of providing access to these systems, Layer 3 Communications places certain restrictions on workplace use of the same for temporary and contract workers as well as for employees.

The telecommunication and computer systems, as well as the equipment and data stored or data in transit, are, and remain at all times, the property of Layer 3 Communications. Accordingly, all messages and files created, sent, received or stored within the system should be related to company business and are and will remain the property of the Company.

Though Layer 3 Communications strives to provide an atmosphere of openness and trust, employees should be aware that they have no legal expectations of privacy. Layer 3 Communications reserves the right to review any message or file composed, sent or received using Layer 3 Communications resources. As such, employees should use these resources with the assumption that someone other than the intended recipient may view information transmitted.

2.1 Policy

2.1.1 Voicemail

The content of voice-mail messages may not contain anything that would reasonably be considered offensive or disruptive to any employee. Offensive content would include, but is not limited to, sexual comments or images, racial slurs, gender-specific comments or any comments that would offend someone on the basis of their age, sex, sexual orientation, religious or political beliefs, national origin or disability.

2.1.2 Internet and Email

Using a reasonable amount of Layer 3 Communications resources for personal emails is acceptable, but non-work-related email should be saved in a separate folder from work related email. All email over 4 years old should be deleted when pertinent.

Layer 3 Communications employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Layer 3 Communications may monitor messages without prior notice.

Regarding Internet and e-mail access and usage, be advised that use of the Internet and e- mail provided by Layer 3 Communications expressly prohibits the following:

- Dissemination or printing of copyrighted materials, including articles and software, in violation of copyright laws.
- Sending, receiving, printing or otherwise disseminating proprietary data, trade secrets or other confidential information of Layer 3 Communications, clients of Layer 3 Communications and vendors, in violation of Company policy or proprietary agreements.
- Offensive or harassing statements or language, including disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious, or political beliefs.
- Sending, receiving, viewing, or soliciting sexually oriented messages, images, or videos.
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Installing, downloading or using file-sharing utilities (like Limewire, Bearshare, and illegal torrents) are not permitted under any circumstances on Layer 3 Communications' computer systems.
- Gambling or engaging in any other activity in violation of local, state or federal law.

2.1.3 Representation in Electronic Mediums

Personal Web sites, blogs, Facebook, Twitter, and other social media outlets have become prevalent methods of self-expression in our culture. Layer 3 Communications respects the right of employees to use these mediums, and any other, during their personal time. If an employee chooses to identify himself or herself as a Layer 3 Communications employee on any electronic medium, he or she must adhere to the following guidelines:

- Make it clear to the readers that the views expressed are the employee's alone and that they do not necessarily reflect the views of Layer 3 Communications.
- Do not disclose any information that is confidential or proprietary to Layer 3 Communications or to any third party that has disclosed information to the Company.
- Uphold Layer 3 Communications' value of respect for the individual, and avoid making defamatory statements about Layer 3 Communications' employees, clients, partners, affiliates and others, including competitors.
- Be careful not to let such communications and participation interfere with the employee's job or client commitments.

3. Password Security

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Layer 3 Communications' resources. All users, including contractors and vendors with access to Layer 3 Communications systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

3.2 Policy

3.2.1 General

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the InfoSec administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.

3.2.2 Guidelines

All users at Layer 3 Communications should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain at least ten character and are required to have:
  - Lower case characters
  - Upper case characters
  - “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc) and numbers are encouraged
- Weak passwords have the following characteristics:
  - The password contains less than nine characters
  - The password is a word found in a dictionary (English or foreign)
  - The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "Layer3", "layer321", "l3atl" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc. Any of the above spelled backwards.

- Passwords that increment or are in a series (passWord1, passWord2, junePass1, julyPass2, etc)

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. (NOTE: Do not use either of these examples as passwords!)

3.2.3 Password Protection Standards

- Always use different passwords for Layer 3 Communications accounts from other non-Layer 3 Communications access (e.g., personal ISP account, option trading, benefits, etc.).
- Always use different passwords for various Layer 3 Communications access needs whenever possible.
- For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.
- Do not share Layer 3 Communications passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Layer 3 Communications information.
- Passwords should never be written down or stored without encryption.
- Do not reveal a password in email, chat, or other electronic communication. Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name") Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the Information Security Department.
- Always decline the use of the "Remember Password" feature of applications (e.g., Internet explorer, Firefox, Chrome, etc).
- If an account or password compromise is suspected, report the incident to the Information Security Department.
- The Information Security Department or its delegates may perform password cracking or guessing on a periodic and/or random basis. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.

4. Device Security

The purpose of this policy is to provide guidance for workstations, laptop, and mobile device security for Layer 3 Communications to ensure the security of information on the workstations, laptops, and mobile devices and the information they may have access to. Any devices that is provided by Layer 3 Communications or is employee owned and used for Layer 3 Communications business purposes must comply with this policy.

4.1 Policy

4.1.1 General

Appropriate measures must be taken when using workstations, laptops, and mobile devices to ensure the confidentiality, integrity and availability of sensitive information, including personally identifiable information (PII) and that access to sensitive information is restricted to authorized users.

- Restricting physical access to workstations, laptops, and mobile devices to only authorized personnel.
- Securing workstations, laptops, and mobile devices (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations, laptops, and mobile devices that were left unsecured will be protected.
- Complying with all applicable password policies and procedures.
- Ensuring workstations, laptops, and mobile devices are used for authorized business purposes only.
- Never installing unauthorized software on workstations, laptops, and mobile devices.
- Storing all sensitive information, PII, and sensitive client information on network servers
- Keeping food and drink away from workstations, laptops, and mobile devices in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Ensuring the workstation or laptop has the Layer 3 Communications recommended antivirus software installed (Microsoft Security Essentials for Windows and Sophos for Mac).
- Ensuring that all workstations and laptops use the Layer 3 Communications recommended hard drive encryption software (windows bit locker or mac equivalent)

- Ensuring workstations, laptops, and mobile devices are current on all software updates (ie adobe, Windows, Mac OS, Firefox, Chrome, etc.).
- Ensuring that all workstations, laptops, and mobile devices use a surge protector (not just a power strip) or a UPS (battery backup).
- All hard drives shall be wiped or zeroed out before being repurposed or thrown away.
- No sensitive information should be stored on unencrypted removable storage devices.
- Installing pirated programs or otherwise installing programs not licensed to Layer 3 Communications without approval.

4.1.2 Mobile Devices

Appropriate measures must be taken when using mobile devices such as tablets and smart phones.

- All tablets and smart phones must have some form of authentication to log into the device (ie passcode, password, or pattern swipe lock, etc.).
- The loss or theft of any mobile device containing Layer 3 Communications data must be reported immediately.
- Layer 3 Communications shall also employ remote wipe technology to remotely disable and delete email stored on a tablet or smart phone which is reported lost or stolen.

5. Clean Desk

The purpose for this policy is to establish a culture of security and trust for all employees at Layer 3 Communications. An effective clean desk effort involving the participation and support of all Layer 3 Communications employees can greatly protect paper documents that contain sensitive information about Layer 3 Communications and our clients. All employees should familiarize themselves with the guidelines of this policy.

5.1 Policy

- At known extended periods away from your desk sensitive working papers are expected to be placed in locked drawers.
- At the end of the working day the employee is expected to tidy their desk and to put away all office papers containing sensitive information. Layer 3 Communications provides locking desks and filing cabinets for this purpose.
- If you are unsure of whether a sensitive documentation should be kept, lock it away or shred it.

- Consider scanning paper items and filing them electronically. Lock your desk and filing cabinets at the end of the day.
- Lock away portable devices such as laptops or tablet devices.
- Treat mass storage devices such as CDROM, DVD, hard drives, or flash media as sensitive and secure them in a locked drawer.
- All unnecessary sensitive information should be shredded.

C.5 Storage

1.Detail tiered pricing and availability for data storage solution between DCSD's primary site and the DRaaS location with intermittent write access and transaction logging.

DCSD will be provided with 125TB of dedicated storage as requested in the response. This provides an all-encompassing, cost-effective solution without additional fees associated with other providers. Additional storage can be made available for DCSD at any time.

2.Describe how the offeror's solution will make sufficient storage continually available for incremental data replication from the primary site to the DR site; including the offeror's storage backup (DR) strategy.

Storage is dedicated for DCSD and continuously available for replication. Additional storage can be made available, upon request, on a per TB basis. As previously stated, Layer 3 Communications has designed the solution to be cost-efficient and meet the needs of DCSD. Layer 3 Communications will work with DCSD to make accommodations to storage after analysis and communications with DCSD IT staff.

3.Describe data recovery and certification of destruction process and procedures.

Veeam provides management and reporting regarding data recovery and certification of data destruction. Layer 3 Communications, in correlation with DCSD IT staff, would review retention policies on a quarterly basis to maintain this process. This solution also utilizes Veeam Cloud Connect which safeguards the Dallas environment. In the event DCSD wants to terminate services in the Dallas DR site, the DCSD tenant would be removed, and all replicas and backup copy jobs would be automatically removed by the system.

In addition to this safeguard, Layer 3 Communications can provide evidence of the deletion of the environment via VMware and storage logs for complete end to end certification.

C.6 Network

1.Offeror to describe how circuits between sites are fail safe and of sufficient bandwidth to handle 100% of DCSD peak demand.

Layer 3 Communications will provide blended, multiple ISP providers with dedicated bandwidth for DCSD, based on the requirements within the RFP. In addition, analysis of current data center traffic can be performed to confirm sizing and predict future growth. Point to point traffic between sites will be dedicated between DCSD access at 56 Marietta and the Dallas, TX data center. Between the two connection options, Layer 3 Communications can provide secure options with failover capabilities for DRaaS traffic.

2.Circuits into and out of the offeror cloud-based location should support DCSD's existing environment and be described in detail (type, bandwidth, etc.). The offeror should include details on how they are managed, monitored and how alerts are communicated to DCSD when appropriate.

Layer 3 Communications has engineered the solution to be additive and supportive of DCSD's existing environment. Layer 3 Communications has great knowledge of the existing network environment due to previous engagements and meticulous documentation. In our Dallas, TX data center we have existing 10Gbps port, ISP connectivity with Cogent and Hurricane Electric. These circuits would be leveraged for DCSD ISP connectivity. For Point-to-Point connectivity, we have existing 10Gbps port connectivity via both Packet Fabric and Hurricane Electric. A new circuit, using one of these providers, would be established to 56 Marietta for cost-effective connectivity between GA production and TX DRaaS.

3.Describe bandwidth scalability as it pertains to potential DCSD future growth.

Our current agreements with providers allow for additional bandwidth scalability or additional circuits with preferential completion of circuits.

4.Describe how the offeror's solution will allow for coordinated configuration changes between DCSD and the offeror.

Layer 3 Communications has previously partnered with DCSD to architect, co-manage, and maintain its data network. As a result, there is awareness of the current DCSD data center sites, configuration knowledge to achieve optimal results, and knowledge of DCSD's personnel and change policy regarding networking.

In addition to institutional knowledge, there will be a meeting early on to build a "playbook" for alerting and coordinating with DCSD.

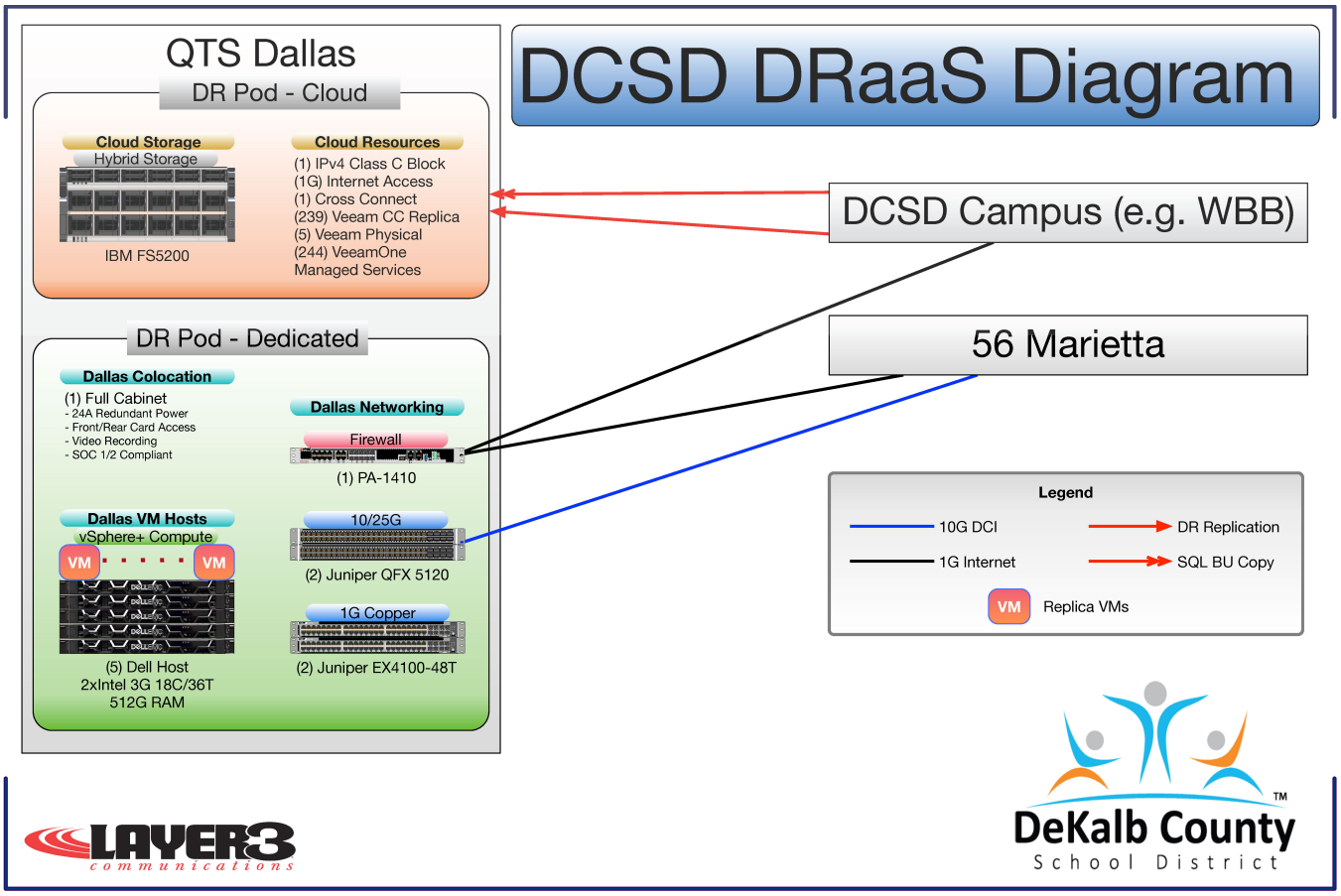
5.Provide details of the availability schema for DCSD to have network access assurance -the offeror solution should provide continuous availability of the network and DR site at all times.

Like the rest of the solution, Layer 3 Communications will provide dedicated firewalling and network switches for the DCSD DRaaS environment. Layer 3 Communications has engineered the DRaaS to be cost-effective while maintaining continuous availability of the network outside of communicated and agreed upon maintenance windows.

C.7 Infrastructure

1.Provide a complete description of the proposed cloud-based infrastructure including/quantities, configuration and models of equipment, applications, types of data storage, memory, CPU/servers, network, storage used to support the DRaaS solution.

Based on the requirements of the request, the proposed solution will be:



5 QTY Dell PowerEdge Servers (dual 18C, 3.0GHz CPU with 448GB RAM)

1 IBM FlashSystem (dual controller, 125TB dedicated volume, iSCSI protocol, NVMe FCM, HDD)

2 Juniper QFX switches (10/25Gbps)

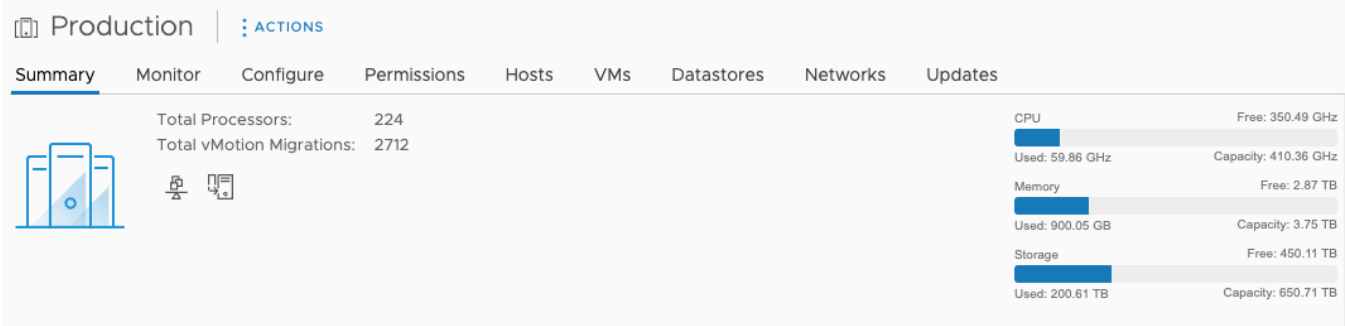
1 Palo Alto firewall

2.The offeror must provide a sufficient cloud-based infrastructure environment that will allow DCSD to build a suitable DR environment to support business processes.

Layer 3 Communications has proposed a dedicated solution that meets the technical requirements of this RFP. This solution will give DCSD a DRaaS solution that will be available to support business processes in a critical situation while meeting the geographical requirements.

3.The offeror shall describe their excess cloud-based infrastructure capacity.

Layer 3 Communications is a provider for public, shared, and private cloud engagements. While this solution is for a dedicated environment, there is a current, excess capacity of 350GHz of CPU, 2.8 TB of Memory, and 450TB of available storage within our shared, Dallas, TX environment:



This solution was built to not use shared resources as it will incur additional costs for licensing, compute, storage, and connectivity services that have not been included in this response. Layer 3 Communications is providing this information as requested to satisfy the response.

4.Provide details of expected performance and any degradation DCSD would experience should the offerors customers stress their environment to 100% of server capacity, storage capacity, and/or network capacity.

Layer 3 Communications provides monitoring and real-time analysis of customer's production and DR environments to avoid situations where customers stress the environments to total consumption. The environment is architected to provide resources for the environment provided in the request. As the tenant's environment requires more resources, Layer 3 Communications will work with DCSD to identify issues before they arise.

If a customer refuses to act and their dedicated environment is stressed to 100% capacity, storage would be primarily impacted first as machines would either experience data loss or service degradation. Server capacity would impact performance of all machines on a given host and/or cluster. Network capacity is unlikely to reach capacity outside of ISP connectivity.

5.The offeror must provide details of the location of all DR cloud-based infrastructure.

The proposed DR site is at:
6431 Longhorn Dr
Irving, TX 75063

The site is a QTS data center in which Layer 3 Communications has a secured cage with dedicated, individually secured cabinets.

C.8 Tools/Applications

1.Provide details of any hardware/software tools required by DCSD to fully integrate to the offeror's hosting environment including; name, version, quantity, pricing.

No additional tools are required to be purchased by DCSD to fully integrate into the proposed solution. We are utilizing Veeam, which is what DCSD uses today for integration with the proposed DRaaS solution.

2.Offeror to provide details of any offeror application or toolsets required to allow DCSD access to the DRaaS site to configure the servers, applications, memory, and networks. Include versions/configuration details and associated costs. Also, the proposal must state if they will be provided by the offeror or if DCSD must furnish and install.

No additional applications or toolsets will be needed to allow DCSD IT staff access to the environment. Management of the solution will be via Veeam, monitoring will be via Veeam ONE with email alerting, and management of the DRaaS infrastructure will be done with VMware. The proposed solution is complete without the need to purchase additional services.

3.Provide details of the virtual environment deployed and the tools/applications used.

Management of the DRaaS infrastructure will be done with VMware, management of the storage will be through IBM console, iDRAC will be utilized for server OOB access, network and firewall devices will be managed via web portals, SSH, or direct console.

4.Describe the options for conversion or accommodating DCSDs tools if the offeror does not utilize DCSD's VMware tools.

Layer 3 Communications will be utilizing VMware to meet the needs of the solution.

D.2 Data Center Discovery

D.2 Data Center Discovery

Layer 3 Communications and DCSD will complete discovery of the DCSD Data Center and satellite sites. Discovery will include but not be limited to:

- Application Process Analysis
- Logical Data Connections Analysis
- Data Center Configuration Analysis
- Data Network Analysis

•Data Storage and Replication Analysis

E. Service Level Agreements (SLA)

Layer 3 Communications' standard Service Level Agreements (SLA) are as follows. Final SLA's can be determined as part of Contract negotiations.

Layer 3 Communications will keep DCSD appraised of all trouble tickets. Layer 3 Communications uses the following service level definitions for ticket workflow:

- EMERGENCY – Service impacting outage notification – immediate notification upon identification of issue and root cause analysis report within 8 hours of remediation.
- CRITICAL – Services are available but critical services severely degraded – notification within 2 hours and root cause analysis report within 24 hours of remediation.
- MAJOR – Services are available, but a non-critical malfunction has occurred – notification within 24 hours identification of issue and root cause analysis report within 72 hours of remediation.
- MINOR - non-service impacting request (cosmetic or feature request) – notification within 48 hours identification of issue.

Layer 3 Communications Case Response and Escalation Times

Case Priority	Priority Classification	Troubleshooting Engagement	Update Frequency	Management Escalation
P1/ Critical	Critical system or service outage in a live environment that results in a severe degradation of overall network performance and/or significant reduction in capacity.	Continuous (24/7/365 until issue is resolved or workaround is in place, with customer agreement to downgrade priority)	Every 4 hours, or as jointly agreed	Immediate: Support Manager or On Call Duty Manager 1 Hour: Services Director and Regional Engineering Director 2 Hours: VP of Engineering 8 Hours: Principals (Owners): CEO/COOs
P2/ High	Intermittent degradation of system or service performance that impacts end-user service quality or impairs network operator control or operational effectiveness. Also, includes loss of redundancy or diagnostic capabilities.	Continuous (24/7/365 until issue is resolved or workaround is in place, with customer agreement to downgrade priority); unless otherwise jointly agreed.	Every 8 hours, or as jointly agreed	1 Hour: Support Manager or On Call Duty Manager 4 Hour: Services Director and Regional Engineering Director 8 Hours: VP of Engineering 48 Hours: Principals (Owners): CEO/COOs
P3/ Medium	Minor degradation of system or service performance that does not impact end-user service quality and minimal impact on network operations.	Normal business hours during normal business days	Every business day, or as jointly agreed	5 days: Support Manager or On Call Duty Manager 10 Days: Services Director and Regional Engineering Director
P4/ Low or Informational	No impact on system or network operation. Information requests or standard questions on configuration or functionality of equipment.	Normal business hours during normal business days	Every 5 business days, or as jointly agreed	10 days: Support Manager or On Call Duty Manager 30 Days: Services Director and Regional Engineering Director

F. Cost and Contract Information

Layer 3 Communications has proposed this DRaaS solution with the services above as a (1) one-year, (12) twelve-month contract with (4) four optional (1) one-year renewals.

Either party may cancel the contract with a 90-day written notice, subject to the below cancellation fees.

In the event DeKalb County School District wishes to terminate the contract prior to the end of the term, there will be an early termination fee of 75% of the remaining contract value.

G. Company Profile

Layer 3 Communications, a wholly owned subsidiary of MGT Consulting (MGT), is a premier managed service, project service, and staffing firm. We are headquartered in Norcross, GA, and service customers globally with a heavy focus in the southeast United States. Layer 3 Communications was acquired in May of 2022 by MGT Consulting. MGT was founded in 1975 and is a purpose-driven, market-shaping leader committed to providing highly specialized solutions to solve complex, mission-critical problems that live at the top of the client leadership agenda. We partner with school districts, cities and counties, higher education institutions, and state agencies to help them achieve high-value, transformational change through our capabilities and industry knowledge, all powered by technology.

Our mission is to be the social impact and performance leader in our industry. Social impact is our “North Star.” To achieve this goal, MGT has expanded its technology, education, and operational performance solutions to deliver performance improvement that lifts people’s lives and impacts communities. By uniting passionate, like-minded people, we are helping drive greater social impact every day for the clients and communities we serve.

With over 600 employees nationwide, our areas of expertise include consulting services, design and architecture of data and voice networks, detailed network documentation, implementation services, integration, and installation, the testing and verification of network solutions and issues, and post implementation support for troubleshooting for expedited mean time to repair during an outage.

Additionally, Layer 3 Communications provides a proactive approach by offering advanced services, such as, vulnerability assessments, penetration testing, disaster recovery, distributed denial of service mitigation (DDoS), cloud services (compute, store, networking, and security elements), and network and security managed services offerings.

We believe that our vast skill set in both our engineering talent and consultative approach to our account management philosophy provides our clients with the best solutions and services in the marketplace.

The benefits our customers experience by working with Layer 3 Communications include:

- Cost avoidance
- Guaranteed solutions

- Reliable point of contact
- Staff optimization
- Multiple vendor integration
- Experience in large scale projects

Additionally, Layer 3 Communications provides ongoing support, maintenance, and engineering services for the networks, as well as security devices we design and build for our customers.

Layer 3 Communications Headquarters

1450 Oakbrook Drive, Suite 900

Norcross, GA 30093

Primary Contact:

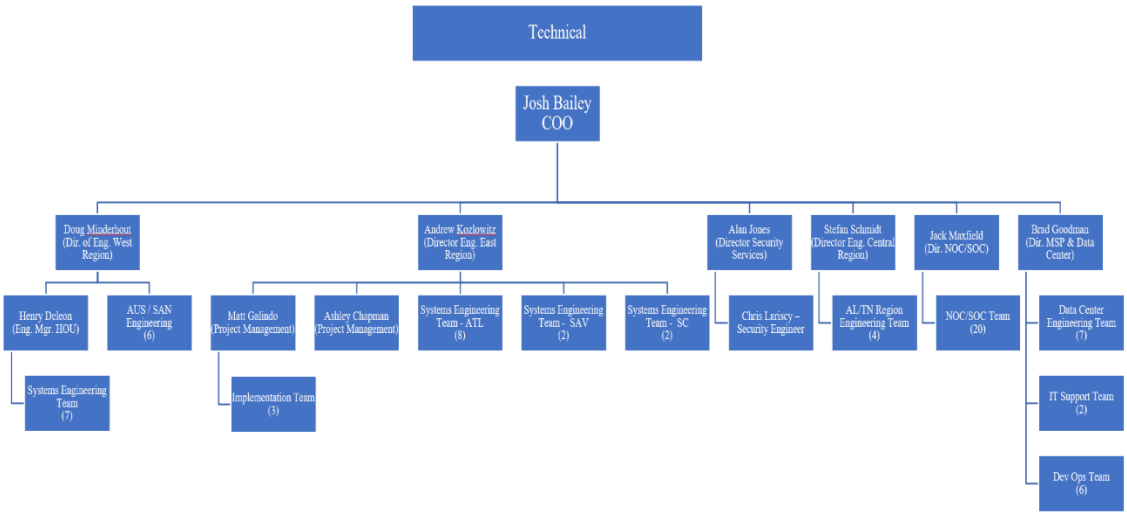
Alex Chitty, Senior Account Manager

Cell – (404) 441-8151

Office – (770) 613-4011

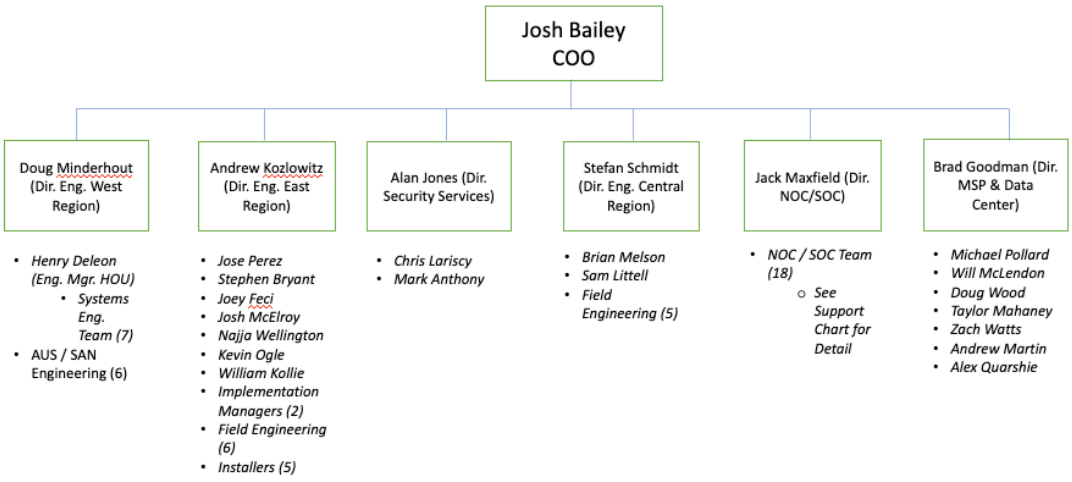
Email – achitty@layer3com.com

Below is the organizational chart for all key staff that will support DCSD including sales, engineering, support, and project management.

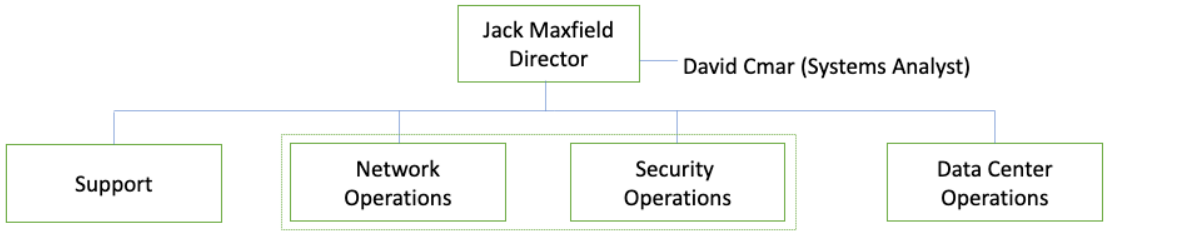

Technical
Josh Bailey
COO
Doug Minderhout
(Dir. of Eng. West Region)
Henry Deleon
(Eng. Mgr. HOU)
AUS / SAN Engineering
(6)
Systems Engineering Team
(7)
Andrew Kozlowitz
(Director Eng. East Region)
Matt Galindo
(Project Management)
Implementation Team
(3)
Ashley Chapman
(Project Management)
Systems Engineering Team - ATL
(8)
Systems Engineering Team - SAV
(2)
Systems Engineering Team - SC
(2)
Alan Jones
(Director Security Services)
Chris Lariscy – Security Engineer
Stefan Schmidt
(Director Eng. Central Region)
AL/TN Region Engineering Team
(4)
Jack Maxfield
(Dir. NOC/SOC)
NOC/SOC Team
(20)
Brad Goodman
(Dir. MSP & Data Center)
Data Center Engineering Team
(7)
IT Support Team
(2)
Dev Ops Team
(6)

Sales - FY2024

Engineering- FY2024



Support- FY2024



- *Ryan Cross - Manager*
- Hayden Young
- Rohit Shriyan
- Patrick Massey
- Andrew Mitchell
- Vaughn Vickers
- TBH - (Tier 2)
- Andrew Courtney (Tier 2)
- Sean Huff (Tier 2)

- Ade Ademakinwa
- Chris Harris
- Alain Kounga
- Ron Baker
- Michael Cross
- Jordan Bingham
- Shin Lor (Analyst)

- Nicole Neustadt (Analyst)
- Rhonda Bridges (Analyst)

- *Michael Pollard - Manager*
- Chuck Townsend
- Alex Quarshie
- Stephen Archie
- Javier Mendoza

Project Management- FY2024

Clients

Layer 3 Communications currently serves customers in the following industries:

Agriculture	Hospitals / Health Care
Banking	Insurance
Biotechnology	IT Services
Chemicals	Legal Services
Communications	Logistics / Transportation
Construction	Machinery
Consulting	Managed Service Providers
Consumer Products	Manufacturing
Education - Universities	Non-Profit
Education K-12	Oil & Gas
Electronics	Private K12
Energy / Utilities	Private (non-education)
Engineering	Professional Services
Environmental	Recreation
Federal	Restaurants
Finance	Retail
Food & Beverage	Services
Healthcare	State and Local Government
Hospitality	Technology

Being a premier SLED solutions integrator, Layer 3 Communications has completed datacenter projects for the following school districts:

DeKalb County School District	Eanes Independent School District
Fulton County Schools	Lamar Consolidated Independent School District
Fayette County Schools	Deer Park Independent School District
Gwinnett County Public Schools	Del Valle Independent School District
Richmond County Schools	Montgomery Independent School District

Contact information and project descriptions can be furnished upon request, however, given the confidential nature of datacenter environments this information cannot be published in a public bid document.

We have provided 2 customer reference forms in the attachment field in the online submission portal. The RFP verbiage asks for a minimum of 3. A 3rd reference form is available upon request.

Relevant Personnel

Layer 3 Communications employs qualified and manufacturer certified field engineers local to the areas surrounding our datacenters. Listed below are several of our field engineering resources, their names, titles, and contact information.

Key Project Management Support Staff				
Name	Position	Email	Mobile	Office
Matt Galindo	Project Manager	mgalindo@layer3com.com	770-570-2735	770-225-5291
Clayton Nugent	Project Manager	cnugent@layer3com.com	678-315-8074	770-225-5300
Ashley Chapman	Project Manager	achapman@layer3com.com	470-533-9554	770-225-5300

Key Network Architect Staff				
Name	Position	Email	Mobile	Office
Stephen Bryant	Network Architect	sbryant@layer3com.com	678-315-4663	770-225-5293
Jose Perez	Network Architect	jperez@layer3com.com	404-664-1169	770-225-5306
Chris Lariscy	Network Architect	clariscy@layer3com.com	678-687-0908	770-225-5284
Josh McElroy	Network Architect	jmcelroy@layer3com.com	770-329-3761	770-225-4009
Stefan Schmidt	Network Architect	sschmidt@layer3com.com	205-566-5606	770-903-6380
Will McLendon	Network Architect	wmclendon@layer3com.com	404-444-6042	770-225-5286
David Fraser	Network Architect	dfraser@layer3com.com	713-397-3540	281-310-9812
Joel McCotter	Network Architect	jmccotter@layer3com.com	832-248-7293	281-310-9815
Doug Wood	Network Architect	dwood@layer3com.com	321-480-8609	N/A
Doug Minderhout	Network Architect	dminderhout@layer3com.com	205-515-2780	N/A

Key Network Engineer Staff				
Name	Position	Email	Mobile	Office
Stephen Bryant	Network Engineer	sbryant@layer3com.com	678-315-4663	770-225-5293
Andrew Kozlowitz	Network Engineer	akozlowitz@layer3com.com	731-234-1195	615-679-9576

Jose Perez	Network Engineer	jperez@layer3com.com	404-664-1169	770-225-5306
Alan Jones	Network Engineer	ajones@layer3com.com	205-223-8004	770-903-6378
Joey Feci	Network Engineer	jfeci@layer3com.com	470-321-9800	N/A
Marc Anthony	Network Engineer	manthony@layer3com.com	205-999-0111	N/A
Jack Maxfield	Network Engineer	jmaxfield@layer3com.com	770-329-3761	770-225-5801
Chris Lariscy	Network Engineer	clariscy@layer3com.com	678-687-0908	770-225-5284
Josh McElroy	Network Engineer	jmcelroy@layer3com.com	770-329-3761	770-225-4009
Stefan Schmidt	Network Engineer	sschmidt@layer3com.com	205-566-5606	770-903-6380
Will McLendon	Network Engineer	wmclendon@layer3com.com	404-444-6042	770-225-5286
Erick Monterrosa	Network Engineer	emonterrosa@layer3com.com	770-330-7812	770-225-5308
Sean Huff	Network Engineer	shuff@layer3com.com	404-418-2602	770-225-5279
Rohit Shriyan	Network Engineer	rshriyan@layer3com.com	469-434-4521	770-225-5279
Cody Sartin	Network Engineer	csartin@layer3com.com	832-540-4111	N/A
Brian Melson	Network Engineer	bmelson@layer3com.com	470-398-2200	N/A
Doug Wood	Network Engineer	dwood@layer3com.com	321-480-8609	N/A
Hayden Young	Network Engineer	hyoung@layer3com.com	256-200-5667	770-225-5279
Ryan Cross	Network Engineer	rcross@layer3com.com	678-755-6544	770-225-5279
Hayden Young	Network Engineer	hyoung@layer3com.com	256-200-5667	770-225-5279
Kevin Ogle	Network Engineer	kogle@layer3com.com	678-437-7720	770-225-5287
Doug Wood	Network Engineer	dwood@layer3com.com	321-480-8609	N/A
Doug Minderhout	Network Engineer	dminderhout@layer3com.com	205-515-2780	N/A

Key Sr. Network Analyst Staff

Name	Position	Email	Mobile	Office
Jack Maxfield	Sr. Network Analyst	jmaxfield@layer3com.com	770-329-3761	770-613-4015
Andrew Courtney	Sr. Network Analyst	acourtney@layer3com.com	770-365-2327	770-225-5279
Ryan Cross	Sr. Network Analyst	rcross@layer3com.com	678-755-6544	770-225-5279
Patrick Massey	Sr. Network Analyst	pmassey@layer3com.com	770-630-7177	770-225-5279
Rohit Shriyan	Sr. Network Analyst	rshriyan@layer3com.com	469-434-4521	770-225-5279
Rhonda Bridges	Sr. Network Analyst	rbridges@layer3com.com	678-436-1203	770-225-5279
Phong (Shin) Lor	Sr. Network Analyst	slor@layer3com.com	404-789-7270	770-225-5279
Sean Huff	Sr. Network Analyst	shuff@layer3com.com	404-418-2602	770-225-5279
Hayden Young	Sr. Network Analyst	hyoung@layer3com.com	256-200-5667	770-225-5279
Nicole Neustadt	Sr. Network Analyst	nneustadt@layer3com.com	404-275-9789	770-225-5279
David Cmar	Sr. Network Analyst	dcmar@layer3com.com	770-331-1252	770-225-5279
Ade Ademakinwa	Sr. Network Analyst	aademakinwa@layer3com.com	404-704-2048	770-225-5279
Mitchell Glore	Sr. Network Analyst	mglore@layer3com.com	678-787-9734	770-225-5279
LaToria Williams	Sr. Network Analyst	lwilliams@layer3com.com	678-637-8415	770-225-5279
Andrew Mitchell	Sr. Network Analyst	amitchell@layer3com.com	678-386-5148	770-225-5279

Key VMware Engineer Staff				
Name	Position	Email	Mobile	Office
Will McLendon	VMware Engineer	wmclendon@layer3com.com	404-444-6042	770-225-5286
David Fraser	VMware Engineer	dfraser@layer3com.com	713-397-3540	281-310-9812
Brad Goodman	VMware Engineer	bgoodman@layer3com.com	912-659-2732	N/A
Michael Pollard	VMWare Engineer	mpollard@layer3com.com	770-653-0786	770-225-5315
Doug Wood	VMware Engineer	dwood@layer3com.com	321-480-8609	N/A

G.1 GA Business License

Only valid at this location and when location conforms to Gwinnett County Ordinance

Gwinnett County Licensing and Revenue
446 W. Crogan Street, Suite 300, Lawrenceville, GA 30046

DISPLAY THIS CERTIFICATE AT BUSINESS LOCATION FOR PUBLIC VIEW

Date Issued:	March 2, 2023	**Certificate Number:**	2023108599
Expires:	March 31, 2024	**Fee:**	$20,100.00
Business Name:	LAYER 3 COMMUNICATIONS LLC		
Description:	Custom Computer Programming Services		

2023
Not Transferable

Business Location
1450 OAKBROOK DR
STE 900
NORCROSS GA 30093-6239

MAIL TO:
LAYER 3 COMMUNICATIONS LLC
C/O LAYER 3 COMMUNICATIONS LLC
1450 OAKBROOK DR STE 900
NORCROSS GA 30093-6239

G.2 Litigation Information (Y/N)

Identify and briefly discuss any instances in the past five (5) years where your contract was terminated, with or without cause. Provide Owner name, project name and Owner Project Representative Name and Number. For joint ventures responding to this RFP, provide the above information as it pertains to the joint venture and for each partner or entity creating said joint venture. **If there is no failure or failures to complete a contract, please include a statement that the Firm has never failed to complete a contract or contracts or have defaulted or have been declared in default on any contract.**

Layer 3 Communications has never failed to complete a contract due to reasons within Layer 3 Communications' control. Nor has Layer 3 Communications defaulted or been declared in default on any contract.

Identify any legal actions that have been filed against your company for services rendered in connection within the past (5) years. Provide a brief explanation for each occurrence and the outcome/disposition. **If there have been no legal actions filed against your company, please include a statement that the Company has not had any legal actions filed against them in the past five (5) years.**

No legal actions have been filed against Layer 3 Communications in the past five (5) years.

L. Transition Plan on Commencement of Contract

Layer 3 Communications understands that continuity of services is necessary to DCSD. We agree to this philosophy and upon expiration of contract, agree to:

a. Exercise best efforts and cooperation for an orderly and efficient transition to another provider or to DCSD.

b. Negotiate a plan in good faith with successor to determine the nature and extent of the phase-in, phase-out services required. The plan shall specify a date for services described in the plan and shall be subject to approval by DCSD. The existing provider shall provide sufficiently experienced personnel during the phase-in and phase-out periods to ensure that the imperious services in the contract are maintained at the required level of need and proficiency.

c. All DCSD property (including but not limited to, students and DCSD records, parts, equipment, facilities, keys, and materials) shall be returned to DCSD upon expiration of contract.

d. Offeror shall include in their response any DCSD or any subsequent contractor requirements if offeror is awarded this contract and does not retain this contract upon its expiration.

M. Pricing

Q-34406

MGT Impact Solutions, LLC
1450 Oakbrook Drive Suite 900
Norcross, GA GA
Phone: (844) 552-9373
Fax: (866) 535-3925

Presented To:
DeKalb County School District
1780 Montreal Road
Tucker, Georgia 30084-6705

Date: 1/7/2025
Valid Until: 3/8/2025
Terms: NET 30

ATTN: Kermit Belcher
(678) 549-0787
kermit_belcher@dekalbschoolsga.org

Submitted By: Alex Chitty
achitty@layer3com.com

DRaaS RFP - Mar 1, 2025 - Feb 28, 2026

Description	Total
Software	$53,196.00
Infrastructure (Network, Compute, Memory, etc.)	$149,688.00
Storage at 25TB	$12,750.00
Additional Storage per 10 TB (up to 100TB) $5,100 per 10TB. 100TB quoted.	$51,000.00
Failover Testing	$36,000.00
Support and Maintenance	$62,640.00

Billing Terms	One Time	Total Cost	$365,274.00

* Total cost does not include shipping, handling, insurance and taxes where applicable. This Budgetary Quote is not a contract. It is subject to further Layer 3 Communications internal approvals and is not binding on either party.