



JOSEPH M. GOLDSTEIN
PARTNER, BOARD CERTIFIED IN BUSINESS
LITIGATION
Shutts & Bowen LLP
201 East Las Olas Blvd.
Suite 2200
Fort Lauderdale, FL 33301
DIRECT (954) 847-3837
EMAIL JGoldstein@shutts.com

February 3, 2025

VIA E-MAIL

Glen Marcos, CPPO, CPPB, FCPM, FCPA, GMarcos@fortlauderdale.gov
Chief Procurement Officer
City of Fort Lauderdale

**Re: Appeal of Denial of Formal Bid Protest of RFP No. 332, Automated School
Zone Speed Detection Camera System.**

Dear Mr. Marcos:

Shutts & Bowen LLP represents Blue Line Solutions LLC (“Blue Line Solutions”), the highest-ranked vendor for RFP No. 332, Automated School Zone Speed Detection Camera System (“RFP”) and timely files this appeal to the City Commission of the Chief Procurement Officer’s denial of the bid protest pursuant to Section 2-182, City Code of Ordinances, which is attached hereto as Exhibit 1. The City Commission should grant this appeal because the CPO erred in denying the protest, which is attached hereto as Exhibit 2. Blue Line Solutions timely submitted its SOC2 Report, and even if it did not, such should be waived as a minor irregularity because such was not an evaluated item, Blue Line Solutions provided its SOC2 Report by the date requested by the Purchasing Department, and in any event Blue Line Solutions had received its SOC2 Report at the time that the CPO now says it was due, despite the later date as requested by the CPO’s staff.

First, the CPO erred as a matter of law in that he failed to fully address the issue as a matter of law that Blue Line Solutions, who was the highest ranked vendor by the subject matter experts on the evaluation committee, timely submitted its SOC2. Second, even if untimely, the CPO has erred as a matter of law and fact in not determining that it is in the best interest of the City of Fort Lauderdale to waive such a minor irregularity to receive the benefits of highest ranked vendor.

We request that the City not schedule this matter for the City Council meeting during the week of March 3, 2025 as undersigned counsel is on a pre-scheduled vacation with his family that week for Spring Break.

I. EXECUTIVE SUMMARY

The following facts are undisputed:

- **Blue Line is the highest ranked vendor.**
- **The SOC2 submission was not an evaluated item, and the SOC2 submission was to be submitted after evaluations as a condition to commence negotiations.**

Change To:

Negotiations will occur with the highest ranked, responsive, and responsible firm contingent upon receipt of ~~The Contractor should provide a current SSAE, SOC 2, Type I report with their proposal to be provided within 60 days after proposal due date. Awarded Contractor will be required to provide an SSAE 18, SOC 2, Type II report annually during the term of his contract. If the Contractor cannot provide the SSAE 18, SOC2, Type I report at the required time of proposal submittal, a current SOC 3 report will be accepted.~~

- **Blue Line received its SOC2, effective as of September 13, 2024, on October 16, 2024**



Opinion

In our opinion, in all material respects,

- a. The description presents Blue Line Solutions, LLC's New Guard Platform (system) that was designed and implemented as of September 13, 2024, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed as of September 13, 2024, to provide reasonable assurance that Blue Line Solutions, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of that date.

- **The City of Fort Lauderdale requested Blue Line submit its SOC2 by November 15, 2024, and Blue Line complied.**

From: Kirk McDonald <KMcDonald@fortlauderdale.gov>
Sent: Wednesday, November 13, 2024 6:17:36 PM
To: Jason Friedberg <jfriedberg@bluelinesolutions.org>
Cc: Jonmichael Mullins <jmullins@bluelinesolutions.org>
Subject: RE: Evaluation Committee Meeting Agenda for Event 332: Automated School Zone Speed Detection Camera System: Reference check

Dear Jason,

The Evaluation Committee (EC) shortlist meeting was held today, November 13, 2024, for RFP No. 332, Automated School Zone Speed Detection Camera System. In the meeting, the EC determined that Blue Line Solutions, LLC is the highest ranked, responsive, and responsible firm. As a result of the EC's decision, the Procurement Services Division must move forward with ensuring compliance with the RFP requirement pursuant to Addendum No. 3 of the RFP, whereby it states:

"Negotiations will occur with the highest ranked, responsive, and responsible firm contingent upon receipt of a current SSAE, SOC 2, Type I report to be provided within 60 days after proposal due date. Awarded Contractor will be required to provide an SSAE 18, SOC, Type II report annually during the term of [t]his contract. If the Contractor cannot provide the SSAE, SOC2, Type I report at the required time, a current SOC 3 report will be accepted."

Subsequently, Competitive Negotiations is the next phase of this competitive process. Blue Line Solutions, LLC is to submit its SOC Report as required by the above-mentioned Addendum No. 3 language by no later than **Friday, November 15th, 2024, at 5:00p.m.** Feel free to contact me with any questions you may have.

Respectfully,

Kirk McDonald
Senior Procurement Specialist
City of Fort Lauderdale | Procurement Services Division
101 NE 3rd Avenue, Suite 1650 | Fort Lauderdale, FL 33301
P 954-828-5073 | F 954-828-5576 | kmcdonald@fortlauderdale.gov
Integrity – Compassion – Accountability – Respect – Excellence

February 3, 2025

Page 4

From: Jonmichael Mullins <jmullins@bluelinesolutions.org>
Sent: Wednesday, November 13, 2024 5:56 PM
To: Kirk McDonald <KMcDonald@fortlauderdale.gov>; Jason Friedberg <jfriedberg@bluelinesolutions.org>
Subject: Blue Line Solutions SOC 2 Report

Good Evening. Please see the BLS SOC 2 report attached. If you have my questions, or need anything else at all, feel free to reach out.

-JM Mullins
938-207-9197

II. BACKGROUND

The City posted the RFP, incorporated by reference as Exhibit B to the Bid Protest (attached as Exhibit 2), on Thursday, July 11, 2024, seeking qualified, experienced, and licensed firm(s) to provide Automated School Zone Speed Detection Camera System Equipment with both LiDAR (Light Detection and Ranging) and RADAR options to the City. Vendor proposals were due on Friday, August 23, 2024.

On Friday, August 30, 2024, the City issued Addendum No. 3 to the RFP, attached hereto as Exhibit C to Bid Protest (attached as Exhibit 2). Addendum No. 3 states in pertinent part, the following:

Negotiations will occur with the highest ranked, responsive, and responsible firm contingent upon receipt of a current SSAE, SOC 2, Type I report to be provided within **60 days** after proposal due date. Awarded Contractor will be required to provide an SSAE 18, SOC 2, Type II report annually during the term of [t]his contract. If the Contractor cannot provide the SSAE 18, SOC2, Type I report at the required time, a current SOC 3 report will be accepted.

(Emphasis added.)

The Evaluation Committee's ("EC") shortlist meeting for the RFP was held on Wednesday, November 13, 2024. At that meeting, the EC determined that Blue Line Solutions, LLC is the highest-ranked, responsive, and responsible firm.

On November 13, 2024, at 5:56 PM, Blue Line Solutions submitted its SOC Report to the City via email correspondence, attached hereto as Exhibit D to the Bid Protest (attached as Exhibit 2).

On November 13, 2024, at 6:17 PM, the City's Procurement Division contacted Blue Line Solutions via email correspondence regarding the submission of its SOC Report pursuant to Addendum No. 3, setting a submission deadline for Friday, November 15, 2024. The email correspondence is attached hereto as Exhibit E to the Bid Protest (attached as Exhibit 2). At the time of the City's correspondence to Blue Line Solutions, Blue Line Solutions had already timely submitted its SOC Report.

On January 16, 2025, the City posted its Award Recommendation/Intent to Award the RFP, recommending RedSpeed Florida LLC for award because “[t]he highest ranked firm, Blue Line Solutions, LLC did not meet the time deadline requirements to submit its SOC2.”

As discussed further below, Blue Line Solutions timely provided its SOC2 report, and even if the submission was untimely such is a minor irregularity that the City Commission should waive as being in its best interest.

III. SUMMARY OF ARGUMENT

The denial of the bid protest challenging the award recommendation is improper as a matter of law, and otherwise improper, arbitrary, and capricious because the City failed to follow its Procurement Ordinance and the instructions of the RFP. This led to the inappropriate recommendation of award to second-ranked vendor RedSpeed Florida LLC when Blue Line Solutions is the highest-ranked, responsive, and responsible vendor. Therefore, the City Commission should grant this bid protest appeal and find accept the ranking of the Evaluation Committee finding Blue Line Solutions to be the highest ranked vendor deserving of an award.

IV. ARGUMENT

A. The CPO’s Decision to Deny the Bid Protest and Recommend Award to the Second Ranked Vendor is Incorrect as a Matter of Law, and Arbitrary and Capricious.

1. *The RFP intended days to mean business days unless it specifically used calendar days. Therefore, awarding the second-ranked vendor when the first-ranked vendor timely submitted its SOC Report and is responsible and responsive is improper.*

“While a public authority has wide discretion in award of contracts for public works on competitive bids, such discretion must be exercised based upon clearly defined criteria, and may not be exercised arbitrarily or capriciously.” *City of Sweetwater v. Solo Const. Corp.*, 823 So. 2d 798, 802 (Fla. 3d DCA 2002).

On November 13, 2024, the EC, at the shortlist meeting for the RFP determined that Blue Line Solutions was the highest-ranked, responsive, and responsible firm per the terms of the solicitation. Subsequent to this determination, the City via its Procurement Division contacted Blue Line Solutions by email regarding the submission of its SOC Report pursuant to Addendum No. 3, representing that the SOC Report was due by Friday, November 15, 2024. *See Ex. E to Bid Protest*, attached as Exhibit 2. On this same day, Blue Line Solutions submitted its SOC Report to the City via email correspondence. *See Ex. D to Bid Protest*, attached as Exhibit 2.

Addendum No. 3 states in pertinent part, the following:

Negotiations will occur with the highest ranked, responsive, and responsible firm contingent upon receipt of a current SSAE, SOC 2, Type I report to be provided within **60 days** after proposal due date. Awarded Contractor will be required to provide an SSAE 18, SOC 2, Type II report annually during the term of [t]his contract. If the Contractor cannot provide the SSAE 18, SOC2, Type I report at the required time, a current SOC 3 report will be accepted. (Emphasis added.) *See* Ex. C to Bid Protest, attached as Exhibit 2.

Addendum No. 3 did not specify “calendar days.” However, the solicitation specifies “calendar days” three separate times, indicating a distinction between deadlines in calendars days versus business days. The respective references to calendar days are as follows:

“Upon formal request of the City, based on the application of a Local Business Preference the Proposer **shall** within **ten (10) calendar days** submit the following documentation” Sec. 2.19.2 RFP, at 6. (Emphasis added.)

“Upon formal request of the City, based on the application of a Disadvantaged Business Preference the Proposer **shall** within **ten (10) calendar days** submit the following documentation” Sec. 2.20.2 RFP, at 7. (Emphasis added.)

“The delivery time **shall** be stated in **calendar days** from the date of City notification of award or notice to proceed with delivery.” Sec. 4.2. RFP, at 26. (Emphasis added.)

The absence of the phrase “calendar days” when otherwise referencing days was evident in over ten (10) different provisions throughout the solicitation. For example, in section 2.26.4, referencing insurance certificate requirements, the RFP explicitly provided the following:

“The Contractor shall provide the City with valid Certificates of Insurance (binders are unacceptable) no later than **ten (10) days** prior to the start of work contemplated in this Agreement.” Sec. 2.26.4(a), RFP, at 10.

“The Contractor shall provide to the City a Certificate of Insurance having a thirty (30) day notice of cancellation; **ten (10) days**’ notice if cancellation is for nonpayment of premium.” Sec. 2.26.4(b), RFP, at 10.

“In the event the Agreement term or any surviving obligation of the Contractor following expiration or early termination of the Agreement goes beyond the expiration date of the insurance policy, the Contractor shall provide the City with an updated Certificate of Insurance no later than **ten (10) days** prior to the expiration of the insurance currently in effect. The City reserves the right to suspend the Agreement until this requirement is met.” Sec. 2.26.4(d), RFP, at 10-11.

The CPO failed to address the above facts that this Solicitation specifically used the term “calendar days” when it required a task done within a certain time.

Furthermore, the Procurement Division’s contemporaneous interpretation, as demonstrated by its email correspondence evidencing its calculation of the deadline for the SOC Report submission, also establishes that days are interpreted as business days and not calendar days. On November 13, 2024, following the evaluation meeting where the EC determined that Blue Line Solutions was the highest ranked, responsive, and responsible firm, Mr. McDonald advised Blue Line Solutions that it had until November 15 to provide its SOC Report. The deadline for the submission of the SOC Report coincides with 60 business days after the August 30, 2024, proposal due date rather than 60 calendar days after the proposal due date.¹

As detailed above, the intent of the RFP is clear by the use of “calendar days” in specific instances and not others. Additionally, it is important to highlight the use of the word “shall” preceding all uses of the phrase “calendar days.” In all three (3) references to calendar days the RFP is restrictive rather than permissive, using mandatory language to indicate the requirement for those specific instances to be calculated in “calendar days.” See *Pecchia v. Wayside Ests. Home Owners Ass’n, Inc.*, 388 So. 3d 1136, 1142 (Fla. 5th DCA 2024) (“In Florida, it has long been the law that “shall” is mandatory). In other provisions of the RFP, like the three (3) examples provided above under the insurance certificate requirements, where there is no use of the phrase “calendar days” more lenient and permissive language is used, suggesting that there is no specific intent for the calculation of days for these provisions to be in calendar days. From the overall construction of the RFP document and subsequent communications from the procurement division, it is evident that “days,” in the absence of a specific identification of calendar days, is construed to mean business days.

Therefore, the CPO erred by failing to reasonably interpret that the SOC Report was due 60 business days after the proposal due date and not calendar days. With the clear intent for the SOC Report to be due 60 business days after the proposal due date instead of 60 calendar days, the City Commission should grant this bid protest appeal and award this contract to Blue Line Solutions, as the responsive and responsible highest ranked vendor.

2. *Even if Blue Line Solutions did untimely submit its SOC Report, the City Commission Must Determine that the Submission of SOC Report is a merely a Minor Irregularity, and it is in the City’s Best Interest to Accept the Proposal from the Highest Ranked Vendor*

Moreover, even if Blue Line Solutions’ SOC report was submitted late, such is a minor regularity that must be waived. In issuing Addendum No. 3, the City amended the RFP to make it clear that the SOC Report was not to be used for determining responsiveness or ranking. Initially, the RFP

¹ Technically, due to an intervening holiday (Labor Day on September 2) and a closure date due to Hurricane Milton (on October 10), the 60th business day was actually November 19, 2024.

required vendors to submit the SOC Report with its proposal. By changing the timing to 60 days after the submission of the proposal, the City contemplated that such would play no role in determining responsiveness, responsibility (at least prior to negotiations or award), and ranking. Instead, the RFP made submission of such merely a condition to begin negotiations if you were previously found responsive, responsible, and the highest ranked by the EC, which Blue Line Solutions was on November 13, 2024, the same day it submitted its SOC Report.

Not only did Blue Line Solutions timely submit its SOC Report after being found responsive, responsible, and the highest ranked, but it had the SOC Report, effective as of September 13, 2024, dated from its auditors on October 16, 2024. See the SOC Report submitted by Blue Line (attached as Exhibit 3). There was no need for Blue Line Solutions to submit its SOC Report until the EC found it responsive, responsible, and highest ranked, which is exactly what Blue Line Solutions did on the same day the EC made its determination that Blue Line Solutions, LLC is the highest-ranked, responsive, and responsible firm.

Under Florida Law, minor irregularities, such as the late submission of a document that does not affect the competitive advantage or the interests of the City, can be waived, allowing the vendor to proceed to the negotiation phase. See *Robinson Elec. Co., Inc. v. Dade County*, 417 So. 2d 1032, 1034 (Fla. 3d DCA 1982), where the court set forth the analysis for determining what constitutes a material variance or irregularity:

In determining whether a specific noncompliance constitutes a substantial and hence nonwaivable irregularity, the courts have applied two criteria—first, whether the effect of a waiver would be to deprive the municipality of its assurance that the contract will be entered into, performed and guaranteed according to its specified requirements, and second, whether it is of such a nature that its waiver would adversely affect competitive bidding by placing a bidder in a position of advantage over other bidders or by otherwise undermining the necessary common standard of competition.

As previously mentioned, the Procurement Division provided a SOC Report submission deadline of November 15, 2024. Blue Line Solutions timely submitted its SOC Report two (2) days before the deadline on November 13, 2024. At that time, Blue Line Solutions was already selected as the highest-ranked, responsive, and responsible firm. As Ex. E to the Bid Protest, attached as Exhibit 2, demonstrates, the submission of the SOC Report is procedural in nature to move the vendor forward to the competitive negotiation phase. Thus, even if late, such submission of this SOC Report, especially where its effective date preceded the RFP timeliness requirement, is a minor irregularity that the City should waive because it does not adversely affect competitive bidding by placing Blue Line Solutions, which was already determined to be the highest-ranked firm, in a position of advantage over other bidders nor does it deprive the City of its assurance that the contract will be entered into, performed and guaranteed according to its specified requirements.

Moreover, if anything, for this RFP, at most, the SOC report goes to the responsibility of a vendor, and the law is clear that the City may consider information regarding a vendor's responsibility up to the time of award. It is also important to highlight that the language in Addendum No. 3 intended the report to be produced after the evaluation and ranking meeting and to merely be a condition for the commencement of negotiations rather than play a role in the determination of responsiveness, which is determined at the time of proposal submission, or ranking, which was to occur before the submission of the SOC Report.

Where material, which goes to the responsibility of a vendor, is required by the City to be produced *after* the initial due date for the bid or proposal, the Chief Procurement Officer *shall* consider such submitted materials. *Cf.* Procurement Manual, at 37-38, § M.11.c.2), 3) & 4). Further, the City's Procurement Code specifically permits such matters a technicality or irregularity that may be waived by the Chief Procurement Officer. Where, as here, the matter to be waived is to the highest ranked vendor, it is arbitrary and capricious not to waive such a minor irregularity. The CPO appears to recognize such as a minor irregularity, but gives insufficient consideration as to waiving such where, as here, Blue Line Solutions is otherwise the highest ranked vendor by the EC.

V. CONCLUSION & REQUEST FOR RELIEF

Local governmental agencies must evaluate proposals consistent with the solicitation's terms, and exercise its discretion based upon clearly defined criteria. *City of Sweetwater v. Solo Const. Corp.*, 823 So. 2d 798, 802 (Fla. 3d DCA 2002). To award this contract to RedSpeed Florida, LLC is contrary to the terms of this solicitation and the representations made by the government agency when Blue Lines Solution is the first ranked, responsive, and responsible vendor, which timely submitted its SOC Report consistent with the interpretation of days as evidenced in the RFP.

Therefore, as a matter of law, fact, and public policy, the City Commission should grant this bid protest appeal, reject the Award Recommendation to RedSpeed Florida LLC, and award to Blue Line Solutions LLC as the highest ranked, responsible, and responsive vendor.

Sincerely,

Shutts & Bowen LLP



Joseph M. Goldstein

EXHIBIT 1



**CITY OF FORT LAUDERDALE
PROCUREMENT SERVICE DIVISION
101 N.E. 1 STREET, SUITE 1650
FORT LAUDERDALE, FLORIDA 33301**

January 30, 2025

Via Email

JGoldstein@shutts.com

Joseph M. Goldstein
Shutts & Bowen LLP
201 East Las Olas Blvd.
Suite 2200
Ft. Lauderdale, FL 33301

RE: Response to Protest of the Award- Request For Proposals (RFP) No. 332, Automated School Zone Speed Detection Camera System Filed on 1/21/25

Dear Mr. Goldstein:

The City of Fort Lauderdale ("City") is in receipt of your timely protest on behalf of your client, Blue Line Solutions LLC ("Blue Line ") regarding RFP No. 332, Automated School Zone Speed Detection Camera System.

Blue Line in its written protest omits some important facts from its Executive Summary. On August 21, 2024, Blue Line had already protested the specifications of RFP No. 332, claiming Section 2.45, Service Organization Controls of the RFP, was unduly restrictive, overstated the City's needs, and limited competition as it originally required the following:

"THE CONTRACTOR SHOULD PROVIDE A CURRENT SSAE 18, SOC 2, TYPE I REPORT WITH THEIR PROPOSAL. AWARDED CONTRACTOR WILL BE REQUIRED TO PROVIDE AN SSAE 18, SOC 2, TYPE II REPORT ANNUALLY DURING THE TERM OF THIS CONTRACT. IF THE CONTRACTOR CANNOT PROVIDE THE SSAE 18, SOC 2, TYPE I REPORT AT TIME OF PROPOSAL SUBMITTAL, A CURRENT SOC 3 REPORT WILL BE ACCEPTED."

You further contended the City should delete the SOC 2 Type I or SOC3 Reports as a requirement and allow for the Nlets Audit because it was more appropriate for the services sought in RFP No. 332, Automated School Zone Speed Detection Camera System and substantially similar to the SOC 2 Report (**See Exhibit A**).

I denied Blue Line's protest of the specifications and petition for relief to eliminate the above-mentioned SOC 2 requirement and allow for alternatives, such as the Nlets audit process due to the fact the City's Information Technology Department provided the following response and position (**See Exhibit B**).

"...The City's policy, specifically Policy 2.45 Service Organizational Controls, clearly outlines the requirement for a current SSAE 18 SOC 2 Type I report with proposals. This requirement is in place to ensure that vendors possess the necessary security controls and safeguards to protect sensitive city data.

A SOC 2 report is a rigorous, independent assessment conducted by a qualified third-party auditor. This audit examines a service organization's systems and

controls in relation to security, availability, processing integrity, confidentiality, or privacy. The SOC 2 report provides assurance to the City that the vendor has implemented robust security measures to protect our data and systems.

While we appreciate [Blue Line's] perspective on the Nlets audit, it is important to clarify that it does not meet the rigorous standards and comprehensive scope required by an SOC 2 report. An SOC 2 audit provides a thorough evaluation of an organization's overall systems and controls, encompassing a broad range of security measures. Conversely, an Nlets audit is specifically designed for law enforcement agencies and addresses a more limited set of framework and compliance requirements. Given the critical nature of the data handled by the City of Fort Lauderdale as a whole, we must adhere to the highest security standards to safeguard the information of our residents and personnel.

Furthermore, it is essential to clarify that an SOC 2 Type II report, requires annually audits and reporting is not a one-time event but rather an ongoing process of monitoring and improvement. This continuous assessment ensures that the vendor maintains strong security controls throughout the contract term.

Given the critical nature of the services being procured and the sensitive data involved, the City cannot deviate from the established SOC 2 requirement. We believe this standard is essential to protect the interests of our citizens and ensure the integrity of our operations...."

Despite my denial of Blue Line's protest on August 30, 2024, the Procurement Services Division issued an Addendum No. 3 to the RFP changing the deadline response from August 30, 2024 at 2 p.m. to September 6, 2024 at 2 p.m. as well as the SOC 2 timeframe submission requirement allowing for negotiations to occur with the highest ranked, responsive, and responsible firm contingent upon receipt of a current SSAE, SOC 2, Type I report within 60 days after proposal due date.

Blue Line submitted its RFP response on the same day that Addendum No. 3 was issued on August 30, 2024. As part of its proposal response, "Exhibit 1: The Road to SOC2 Compliance", Blue Line admitted that it would not have the SOC2 Type 1 Report until March 2025 and the SOC2 Type 2 report sometime into the later part of 2025 as shown below. In addition, included below is Blue Line's Exhibit 2, which is an engagement letter from the Johanson Group to execute a SOC 2 Type I and SOC 2 Type II **dated on the same date Blue Line submitted its proposal to the City on August 30th, 2024.**

SOC2 CONTROLS TIMELINE

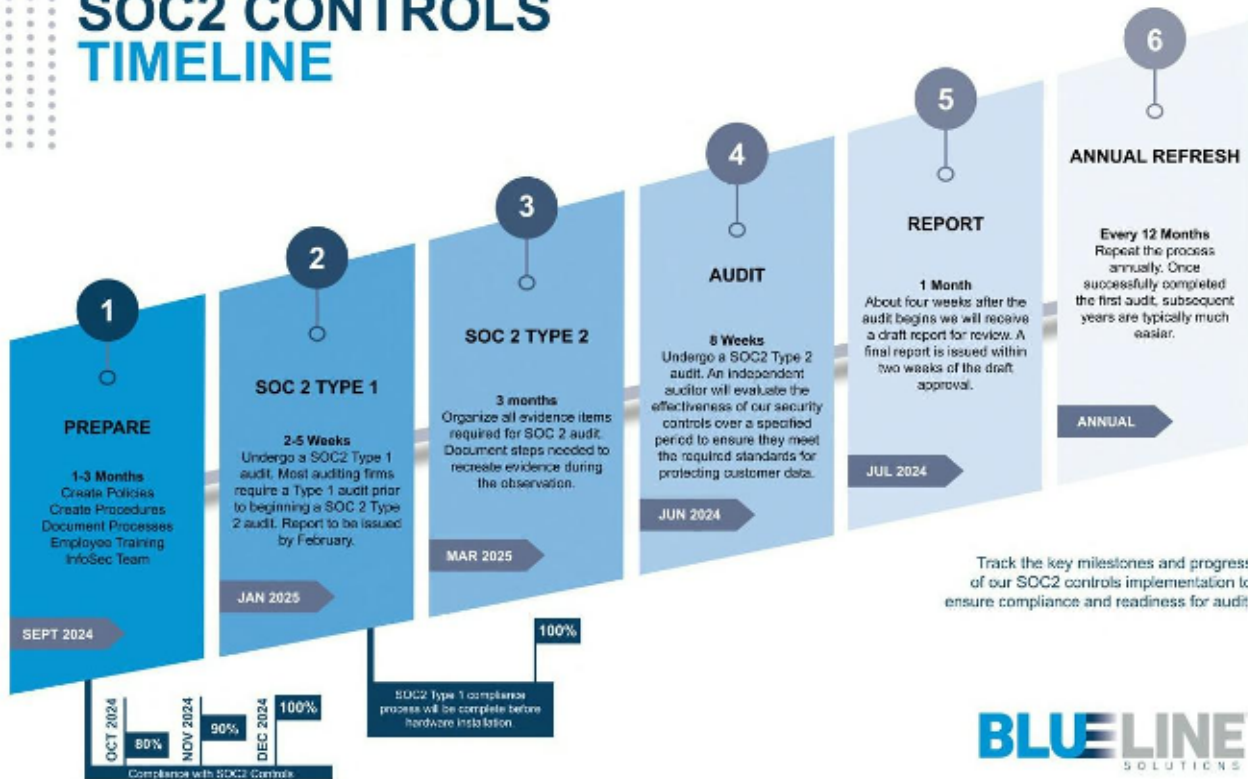


Exhibit 1: The Road to SOC2 Compliance



BLUELINE™

IN RESPONSE TO:
Fort Lauderdale RFP 332
SUBMITTED ON:
8/30/2024



August 30, 2024

Blue Line Solutions, LLC

Dear Blue Line Solutions, LLC,

We are pleased to confirm our understanding of the terms and objectives of our engagement and the nature and limitations of the services we will provide to Blue Line Solutions, LLC.

We confirm that we have been engaged by Blue Line Solutions, LLC to execute a SOC 2 Type I and SOC 2 Type II attestation engagement on the relevant AICPA Trust Services Criteria categories. The expected testing period for the SOC 2 Type I and SOC 2 Type II examination will be determined based upon assessment of readiness.

We will issue a written report upon completion of our examination of management's description and the suitability of the design and operating effectiveness of controls (Type I) to achieve the related control objectives stated in the description (Type II) commonly known as a SOC 2 Type I and SOC 2 Type II report. As the engagement is in process as of the date of this letter, we cannot provide assurance that an unmodified opinion will be expressed until we have completed our required procedures. Circumstances may arise in which it is necessary for us to modify our opinion, add an emphasis-of-matter or other-matter paragraph(s), or withdraw from the engagement.

We appreciate the opportunity to be of service to you and believe this accurately summarizes the significant terms of our engagement. If you have any additional questions, please do not hesitate to contact us.

Very truly yours,

Johanson Group LLP

Exhibit 2: Letter of Engagement (SOC 2)

Now as part of its protest and contrary to its original representations made to the City of not being able to produce the reports within the required timeframe, Blue Line is now claiming that it received its SOC 2 Type I Report, effective as of September 13, 2024, on October 16, 2024. Yet, for whatever reason, Blue Line failed to forward the report to the City on the same day the Johanson Group provided it to Blue Line despite the deadline articulated in Addendum No. 3, , which is 60 days after the proposal due date, November 5, 2024. It is evident from your own facts that this was an avoidable issue by Blue Line.

While the circumstances concerning your matter are quite unfortunate, Blue Line must take responsibility for its own actions or inactions.

Blue Line further alleges that:

- 1) The City intended to say 60 business and not calendar days in order to comply with the submission requirements of the SOC 2 Type I report;
- 2) The decision to post the intended award to the second ranked firm, RedSpeed Florida LLC is arbitrary and capricious;
- 3) The Chief Procurement Officer should grant Blue Line relief by deeming the failure to timely submit the SOC 2 Type I report as a minor irregularity and waive the timing requirement to allow for the late submission of the SOC 2 Type I report; and
- 4) Mr. McDonald's email to provide the report by November 15th indicates that the Procurement Services Division established a new submission deadline of November 15, 2024 and proof that 60 business days and not calendar days was the City's intent.

These assertions are not accurate. Mr. McDonald does not possess the authority to unilaterally change the submission timeline requirements in the RFP solicitation document nor any subsequent issuance of an addendum or addenda. Conversely, when the SOC 2 Type 1 report was requested by Mr. McDonald on November 13th to be provided by Blue Line on November 15th, the Procurement staff were under the impression that it was still within 60 calendar days. This was a miscalculation and error on our part.

With this being said, Blue Line should not construe this to mean or argue that it should now be afforded the opportunity to submit the report after the deadline, and even if it were a minor irregularity as you argue, City's authority to waive a minor irregularity is discretionary.

Consequently, your request for relief to grant this protest is not supported by the applicable facts or law. Therefore, I hereby deny your protest and will be moving forward with the Notice of Intent to Award to RedSpeed Florida LLC.

Respectfully,

Glenn Marcos Digitally signed by Glenn Marcos
Date: 2025.01.30 12:59:28 -05'00'

Glenn Marcos, CPPO, CPPB, FCPM, FCPA
Chief Procurement Officer
Assistant Finance Director – Procurement and Contracts

cc: Susan Grant, Acting City Manager
D'Wayne Spence, Acting City Attorney
Laura Reece, Acting Assistant City Manager

Linda Short, Director, Finance Department
William Shultz, Chief of Police
Rhonda Montoya Hasan, Senior Assistant City Attorney
Eric Abend, Senior Assistant City Attorney
Julie Steinhardt, Assistant City Attorney
Tamecka McKay, Director, Information Technology Services
Angela Marinas, Assistant Director, Information Technology Services
Charles Everette, Security Manager/HIPPA Security Officer, Information Technology Services
Kirk McDonald, Senior Procurement Specialist
File

EXHIBIT 2



CITY OF FORT LAUDERDALE
2025 JAN 21
9:53
PROCUREMENT SERVICES

JOSEPH M. GOLDSTEIN
PARTNER, BOARD CERTIFIED IN BUSINESS
LITIGATION
Shutts & Bowen LLP
201 East Las Olas Blvd.
Suite 2200
Fort Lauderdale, FL 33301
DIRECT (954) 847-3837
EMAIL JGoldstein@shutts.com

January 21, 2025

VIA E-MAIL

Glen Marcos, CPPO, CPPB, FCPM, FCPA, GMarcos@fortlauderdale.gov
Chief Procurement Officer
City of Fort Lauderdale

Re: Formal Bid Protest of RFP No. 332, Automated School Zone Speed Detection Camera System.

Dear Mr. Marcos:

Shutts & Bowen LLP represents Blue Line Solutions LLC (“Blue Line Solutions”), the first-ranked vendor of RFP No. 332, Automated School Zone Speed Detection Camera System (“RFP”). Blue Line Solutions submits this timely formal bid protest of the City of Fort Lauderdale’s (“City”) January 16, 2025, Award Recommendation/Intent to Award (“Award Recommendation”), attached hereto as **Exhibit A**. This protest is being filed within five (5) days after a notice of intent to award was posted on the City of Fort Lauderdale's world wide web site. Accompanied with the protest is an application fee of \$ 5,000. As grounds for its protest, Blue Line Solutions states as follows:

I. EXECUTIVE SUMMARY

The following facts are undisputed:

- **Blue Line is the highest ranked vendor.**
- **The SOC2 submission was not an evaluated item, and the SOC2 submission was to be submitted after evaluations as a condition to commence negotiations.**

Change To:

Negotiations will occur with the highest ranked, responsive and responsible firm contingent upon receipt of ~~The Contractor should provide~~ a current SSAE, SOC 2, Type I report ~~with their proposal~~ to be provided within 60 days after proposal due date. Awarded Contractor will be required to provide an SSAE 18, SOC 2, Type II report annually during the term of his contract. If the Contractor cannot provide the SSAE 18, SOC2, Type I report at the required time of proposal submittal, a current SOC 3 report will be accepted.

- **Blue Line received its SOC2, effective as of September 13, 2024, on October 16, 2024**



Opinion

In our opinion, in all material respects,

- a. The description presents Blue Line Solutions, LLC's New Guard Platform (system) that was designed and implemented as of September 13, 2024, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed as of September 13, 2024, to provide reasonable assurance that Blue Line Solutions, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of that date.

- **The City of Fort Lauderdale requested Blue Line submit its submit its SOC2 by November 15, 2024, and Blue Line complied.**

From: Kirk McDonald <KMcDonald@fortlauderdale.gov>
Sent: Wednesday, November 13, 2024 6:17:36 PM
To: Jason Friedberg <jfriedberg@bluelinesolutions.org>
Cc: Jonmichael Mullins <jmullins@bluelinesolutions.org>
Subject: RE: Evaluation Committee Meeting Agenda for Event 332: Automated School Zone Speed Detection Camera System: Reference check

Dear Jason,

The Evaluation Committee (EC) shortlist meeting was held today, November 13, 2024, for RFP No. 332, Automated School Zone Speed Detection Camera System. In the meeting, the EC determined that Blue Line Solutions, LLC is the highest ranked, responsive, and responsible firm. As a result of the EC's decision, the Procurement Services Division must move forward with ensuring compliance with the RFP requirement pursuant to Addendum No. 3 of the RFP, whereby it states:

"Negotiations will occur with the highest ranked, responsive, and responsible firm contingent upon receipt of a current SSAE, SOC 2, Type I report to be provided within 60 days after proposal due date. Awarded Contractor will be required to provide an SSAE 18, SOC, Type II report annually during the term of [t]his contract. If the Contractor cannot provide the SSAE, SOC2, Type I report at the required time, a current SOC 3 report will be accepted."

Subsequently, Competitive Negotiations is the next phase of this competitive process. Blue Line Solutions, LLC is to submit its SOC Report as required by the above-mentioned Addendum No. 3 language by no later than **Friday, November 15th, 2024, at 5:00p.m.** Feel free to contact me with any questions you may have.

Respectfully,

Kirk McDonald
Senior Procurement Specialist
City of Fort Lauderdale | Procurement Services Division
101 NE 3rd Avenue, Suite 1650 | Fort Lauderdale, FL 33301
P 954-828-5073 | F 954-828-5576 | kmcdonald@fortlauderdale.gov
Integrity – Compassion – Accountability – Respect – Excellence

From: Jonmichael Mullins <jmullins@bluelinesolutions.org>
Sent: Wednesday, November 13, 2024 5:56 PM
To: Kirk McDonald <KMcDonald@fortlauderdale.gov>; Jason Friedberg <jfriedberg@bluelinesolutions.org>
Subject: Blue Line Solutions SOC 2 Report

Good Evening. Please see the BLS SOC 2 report attached. If you have my questions, or need anything else at all, feel free to reach out.

-JM Mullins
938-207-9197

II. BACKGROUND

The City posted the RFP, incorporated by reference as **Exhibit B**, on Thursday, July 11, 2024, seeking qualified, experienced, and licensed firm(s) to provide Automated School Zone Speed Detection Camera System Equipment with both LiDAR (Light Detection and Ranging) and RADAR options to the City. Vendor proposals were due on Friday, August 23, 2024.

On Friday, August 30, 2024, the City issued Addendum No. 3 to the RFP, attached hereto as **Exhibit C**. Addendum No. 3 states in pertinent part, the following:

Negotiations will occur with the highest ranked, responsive, and responsible firm contingent upon receipt of a current SSAE, SOC 2, Type I report to be provided within **60 days** after proposal due date. Awarded Contractor will be required to provide an SSAE 18, SOC 2, Type II report annually during the term of [t]his contract. If the Contractor cannot provide the SSAE 18, SOC2, Type I report at the required time, a current SOC 3 report will be accepted.

(Emphasis added.)

The Evaluation Committee's ("EC") shortlist meeting for the RFP was held on Wednesday, November 13, 2024. At that meeting, the EC determined that Blue Line Solutions, LLC is the highest-ranked, responsive, and responsible firm.

On November 13, 2024, at 5:56 PM, Blue Line Solutions submitted its SOC Report to the City via email correspondence, attached hereto as **Exhibit D**.

On November 13, 2024, at 6:17 PM, the City's Procurement Division contacted Blue Line Solutions via email correspondence regarding the submission of its SOC Report pursuant to Addendum No. 3, setting a submission deadline for Friday, November 15, 2024. The email correspondence is attached hereto as **Exhibit E**. At the time of the City's correspondence to Blue Line Solutions, Blue Line Solutions had already timely submitted its SOC Report.

On January 16, 2025, the City posted its Award Recommendation/Intent to Award the RFP, recommending RedSpeed Florida LLC for award because "[t]he highest ranked firm, Blue Line Solutions, LLC did not meet the time deadline requirements to submit its SOC2."

As discussed further below, Blue Line Solutions timely provided its SOC2 report, and even if the submission was untimely such is a minor irregularity that should have been waived.

III. SUMMARY OF ARGUMENT

The Award Recommendation is improper, arbitrary, and capricious because the City failed to follow its Procurement Ordinance and the instructions of the RFP. This led to the inappropriate recommendation of award to second-ranked vendor RedSpeed Florida LLC when Blue Line

Solutions is the highest-ranked, responsive, and responsible vendor. Therefore, Blue Line Solutions should be the vendor recommended for award for this RFP.

IV. ARGUMENT

A. The City's Decision to Award the Second Rank Vendor is Arbitrary and Capricious.

1. *The RFP intended days to mean business days unless it specifically used calendar days. Therefore, awarding the second-ranked vendor when the first-ranked vendor timely submitted its SOC Report and is responsible and responsive is improper.*

“While a public authority has wide discretion in award of contracts for public works on competitive bids, such discretion must be exercised based upon clearly defined criteria, and may not be exercised arbitrarily or capriciously.” *City of Sweetwater v. Solo Const. Corp.*, 823 So. 2d 798, 802 (Fla. 3d DCA 2002).

On November 13, 2024, the EC, at the shortlist meeting for the RFP determined that Blue Line Solutions, LLC is the highest-ranked, responsive, and responsible firm per the terms of the solicitation. Subsequent to this determination, the City via its Procurement Division contacted Blue Line Solutions via email correspondence regarding the submission of its SOC Report pursuant to Addendum No. 3, representing that the SOC Report was due by Friday, November 15, 2024. *See Ex. E.* On this same day, Blue Line Solutions submitted its SOC Report to the City via email correspondence. *See Ex. D.*

Addendum No. 3 states in pertinent part, the following:

Negotiations will occur with the highest ranked, responsive, and responsible firm contingent upon receipt of a current SSAE, SOC 2, Type I report to be provided within **60 days** after proposal due date. Awarded Contractor will be required to provide an SSAE 18, SOC 2, Type II report annually during the term of [t]his contract. If the Contractor cannot provide the SSAE 18, SOC2, Type I report at the required time, a current SOC 3 report will be accepted.

(Emphasis added.) *See Ex. C.*

Addendum No. 3 did not specify “calendar days.” However, the solicitation specifies “calendar days” three separate times, indicating a distinction between deadlines in calendars days versus business days. The respective references to calendar days are as follows:

“Upon formal request of the City, based on the application of a Local Business Preference the Proposer **shall within ten (10) calendar days** submit the following documentation” Sec. 2.19.2 RFP, at 6. (Emphasis added.)

“Upon formal request of the City, based on the application of a Disadvantaged Business Preference the Proposer **shall** within **ten (10) calendar days** submit the following documentation” Sec. 2.20.2 RFP, at 7. (Emphasis added.)

“The delivery time **shall** be stated in **calendar days** from the date of City notification of award or notice to proceed with delivery.” Sec. 4.2. RFP, at 26. (Emphasis added.)

The absence of the phrase “calendar days” when otherwise referencing days was evident in over ten (10) different provisions throughout the solicitation. For example, in section 2.26.4, referencing insurance certificate requirements, the RFP explicitly provided the following:

“The Contractor shall provide the City with valid Certificates of Insurance (binders are unacceptable) no later than **ten (10) days** prior to the start of work contemplated in this Agreement.” Sec. 2.26.4(a), RFP, at 10.

“The Contractor shall provide to the City a Certificate of Insurance having a thirty (30) day notice of cancellation; **ten (10) days**’ notice if cancellation is for nonpayment of premium.” Sec. 2.26.4(b), RFP, at 10.

“In the event the Agreement term or any surviving obligation of the Contractor following expiration or early termination of the Agreement goes beyond the expiration date of the insurance policy, the Contractor shall provide the City with an updated Certificate of Insurance no later than **ten (10) days** prior to the expiration of the insurance currently in effect. The City reserves the right to suspend the Agreement until this requirement is met.” Sec. 2.26.4(d), RFP, at 10-11.

Furthermore, the Procurement Division’s contemporaneous interpretation, as demonstrated by its email correspondence evidencing its calculation of the deadline for the SOC Report submission, also establishes that days are interpreted as business days and not calendar days. On November 13, 2024, following the evaluation meeting where the EC determined that Blue Line Solutions was the highest ranked, responsive, and responsible firm, Mr. McDonald advised Blue Line Solutions that it had until November 15 to provide its SOC Report. The deadline for the submission of the SOC Report coincides with 60 business days after the August 30, 2024, proposal due date rather than 60 calendar days after the proposal due date.¹

As detailed above, the intent of the RFP is clear by the use of “calendar days” in specific instances and not others. Additionally, it is important to highlight the use of the word “shall” preceding all uses of the phrase “calendar days.” In all three (3) references to calendar days the RFP is restrictive rather than permissive, using mandatory language to indicate the requirement for those specific

¹ Technically, due to an intervening holiday (Labor Day on September 2) and a closure date due to Hurricane Milton (on October 10), the 60th business day was actually November 19, 2024.

instances to be calculated in “calendar days.” See *Pecchia v. Wayside Ests. Home Owners Ass’n, Inc.*, 388 So. 3d 1136, 1142 (Fla. 5th DCA 2024) (“In Florida, it has long been the law that “shall” is mandatory). In other provisions of the RFP, like the three (3) examples provided above under the insurance certificate requirements, where there is no use of the phrase “calendar days” more lenient and permissive language is used, suggesting that there is no specific intent for the calculation of days for these provisions to be in calendar days. From the overall construction of the RFP document and subsequent communications from the procurement division, it is evident that “days,” in the absence of a specific identification of calendar days, is construed to mean business days.

Therefore, it is reasonably interpreted that the SOC Report was due 60 business days after the proposal due date and not calendar days. With the clear intent for the SOC Report to be due 60 business days after the proposal due date instead of 60 calendar days, the City’s decision to award the second-ranked vendor, when the first-ranked vendor is responsible and responsive is improper, arbitrary and capricious.

2. *Even if Blue Line Solutions did untimely submit its SOC Report, the Submission of SOC Report is a merely a Minor Irregularity.*

Moreover, even if Blue Line Solutions’ SOC report was submitted late, such is a minor regularity that must be waived. In issuing Addendum No. 3, the City amended the RFP to make it clear that the SOC Report was not to be used for determining responsiveness or ranking. Initially, the RFP required vendors to submit the SOC Report with its proposal. By changing the timing to 60 days after the submission of the proposal, the City contemplated that such would play no role in determining responsiveness, responsibility (at least prior to negotiations or award), and ranking. Instead, the RFP made submission of such merely a condition to begin negotiations if you were previously found responsive, responsible, and the highest ranked by the EC, which Blue Line Solutions was on November 13, 2024, the same day it submitted its SOC Report.

Not only did Blue Line Solutions timely submit its SOC Report after being found responsive, responsible, and the highest ranked, but it had the SOC Report, effective as of September 13, 2024, dated from its auditors on October 16, 2024. There was no need for Blue Line Solutions to submit its SOC Report until the EC found it responsive, responsible, and highest ranked, which is exactly what Blue Line Solutions did on the same day the EC made its determination that Blue Line Solutions, LLC is the highest-ranked, responsive, and responsible firm.

Under Florida Law, minor irregularities, such as the late submission of a document that does not affect the competitive advantage or the interests of the City, can be waived, allowing the vendor to proceed to the negotiation phase. See *Robinson Elec. Co., Inc. v. Dade County*, 417 So. 2d 1032, 1034 (Fla. 3d DCA 1982), where the court set forth the analysis for determining what constitutes a material variance or irregularity:

In determining whether a specific noncompliance constitutes a substantial and hence nonwaivable irregularity, the courts have applied two criteria—first, whether the effect of a waiver would be to deprive the municipality of its assurance that the contract will be entered into, performed and guaranteed according to its specified requirements, and second, whether it is of such a nature that its waiver would adversely affect competitive bidding by placing a bidder in a position of advantage over other bidders or by otherwise undermining the necessary common standard of competition.

As previously mentioned, the Procurement Division provided a SOC Report submission deadline of November 15, 2024. Blue Line Solutions timely submitted its SOC Report two (2) days before the deadline on November 13, 2024. At that time, Blue Line Solutions was already selected as the highest-ranked, responsive, and responsible firm. As **Ex. E** demonstrates, the submission of the SOC Report is procedural in nature to move the vendor forward to the competitive negotiation phase. Thus, even if late, such submission of this SOC Report, especially where its effective date preceded the RFP timeliness requirement, is a minor irregularity that the City should waive because it does not adversely affect competitive bidding by placing Blue Line Solutions, which was already determined to be the highest-ranked firm, in a position of advantage over other bidders nor does it deprive the City of its assurance that the contract will be entered into, performed and guaranteed according to its specified requirements.

Moreover, if anything, for this RFP, at most, the SOC report goes to the responsibility of a vendor, and the law is clear that the City may consider information regarding a vendor's responsibility up to the time of award. It is also important to highlight that the language in Addendum No. 3 intended the report to be produced after the evaluation and ranking meeting and to merely be a condition for the commencement of negotiations rather than play a role in the determination of responsiveness, which is determined at the time of proposal submission, or ranking, which was to occur before the submission of the SOC Report.

Where material, which goes to the responsibility of a vendor, is required by the City to be produced **after** the initial due date for the bid or proposal, the Chief Procurement Officer **shall** consider such submitted materials. *Cf.* Procurement Manual, at 37-38, § M.11.c.2), 3) & 4). Further, the City's Procurement Code specifically permits such matters a technicality or irregularity that may be waived by the Chief Procurement Officer. Where as here, the matter to be waived is to the highest ranked vendor, it is arbitrary and capricious not to waive such a minor irregularity.

V. CONCLUSION & REQUEST FOR RELIEF

Local governmental agencies must evaluate proposals consistent with the solicitation's terms, and exercise its discretion based upon clearly defined criteria. *City of Sweetwater v. Solo Const. Corp.*, 823 So. 2d 798, 802 (Fla. 3d DCA 2002). To award this contract to RedSpeed Florida, LLC is contrary to the terms of this solicitation and the representations made by the government agency

January 21, 2025

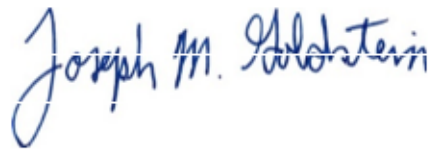
Page 9

when Blue Lines Solution is the first ranked, responsive, and responsible vendor, which timely submitted its SOC Report consistent with the interpretation of days as evidenced in the RFP.

Therefore, as a matter of law and public policy, the City should rescind the Award Recommendation to RedSpeed Florida LLC and award Blue Line Solutions LLC.

Sincerely,

Shutts & Bowen LLP

A handwritten signature in blue ink that reads "Joseph M. Goldstein". The signature is written in a cursive, flowing style.

Joseph M. Goldstein

Attachments

FTLDOCS 9507939 2

ITB AWARD RECOMMENDATION / INTENT TO AWARD

PROCUREMENT SPECIALIST: Kirk McDonald

DATE: 01/16/25

ITB#: 332 **ITEM / SERVICE:** Automated School Zone Speed Detection Camera System

Attached are apparent low bid(s) and a tabulation for subject items/services requisitioned by the department.

RECOMMENDATION:

A. Which vendor is recommended for Award? RedSpeed Florida

B. Does this meet specifications as per the department's request and as advertised? YES NO

If NO, is the variance considered: MINOR MAJOR

Explain:

C. Is the recommendation the lowest bid received? YES NO

D. List the Bids that are low but DO NOT meet specifications and list reasons why each does not meet specifications:
attach a memorandum of explanation to this form if necessary.

The highest ranked firm, Blue Line Solutions, LLC did not meet the time deadline requirements to submit its SOC2. The City is moving to the next highest ranked firm, RedSpeed Florida LLC.

(Attach an additional sheet if further comment or explanation is required.)

Glenn Marcos Digitally signed by Glenn Marcos
Date: 2025.01.16 11:40:59 -05'00'
SIGNATURE: _____
Chief Procurement Officer or designee

Date: 1/16/25

THIS FORM MUST BE COMPLETED FOR ALL AWARD RECOMMENDATIONS OF \$25,000 AND ABOVE.

Over \$25,000 YES NO



ADDENDUM NO. 3

RFP No. 332

TITLE: Automated School Zone Speed Detection Camera System

ISSUED: August 30, 2024

This addendum is being issued to make the following change(s). The **underline** denotes addition and ~~strikethrough~~ denotes deletion.

1. Event Dates

Change From:

Close: 08/30/2024 02:00:00 PM.

Change To:

Close: 09/06/2024 02:00:00 PM.

2. Section 2.45, Service Organization Controls

Change From:

The Contactor should provide a current SSAE 18, SOC 2, Type I report with their proposal. Awarded Contractor will be required to provide an SSAE 18, SOC 2, Type II report annually during the term of this contract. If the Contractor cannot provide the SSAE 18, SOC 2, Type I report at time of proposal submittal, a current SOC 3 report will be accepted.

Change To:

Negotiations will occur with the highest ranked, responsive, and responsible firm contingent upon receipt of ~~The Contractor should provide~~ a current SSAE, SOC 2, Type I report ~~with their proposal~~ to be provided within 60 days after proposal due date. Awarded Contractor will be required to provide an SSAE 18, SOC 2, Type II report annually during the term of his contract. If the Contractor cannot provide the SSAE 18, SOC2, Type I report at the required time of proposal submittal, a current SOC 3 report will be accepted.

***Note- All changes to the above and any other section regarding same, if applicable, shall be in effect.**

All other terms, conditions, and specifications remain unchanged.



City of Fort Lauderdale Procurement Services Division
101 NE 3rd Avenue Fort Lauderdale, Florida 33301
954-828-5933 Fax 954-828-5576
purchase@fortlauderdale.gov

Kirk McDonald
Senior Procurement Specialist:

Company Name: _____
(please print)

Bidder's Signature: _____

Date: _____

On Nov 20, 2024, at 1:03 PM, Jason Friedberg <jfriedberg@bluelinesolutions.org> wrote:

Regards,
Jason

[Jason Friedberg](#)
Vice President of Sales & Marketing
<Image.jpeg>

M: 267-671-2613
4409 Oakwood Dr.
Chattanooga, TN 37416

Confidentiality Message | This e-mail message is confidential, may be privileged and is intended for the exclusive use of the addressee. Any other person is strictly prohibited from disclosing, distributing or reproducing it. If the addressee cannot be reached or is unknown to you, please inform the sender by return email immediately and delete this e-mail message and destroy all copies.

From: Jonmichael Mullins <jmullins@bluelinesolutions.org>
Sent: Wednesday, November 20, 2024 1:00:13 PM
To: Jason Friedberg <jfriedberg@bluelinesolutions.org>
Subject: Fw: Blue Line Solutions SOC 2 Report

From: Jonmichael Mullins <jmullins@bluelinesolutions.org>
Sent: Wednesday, November 13, 2024 5:56 PM
To: Kirk McDonald <KMcDonald@fortlauderdale.gov>; Jason Friedberg <jfriedberg@bluelinesolutions.org>
Subject: Blue Line Solutions SOC 2 Report

Good Evening. Please see the BLS SOC 2 report attached. If you have my questions, or need anything else at all, feel free to reach out.

-JM Mullins
938-207-9197

Get [Outlook for iOS](#)
<Blue Line Solutions LLC SOC2 Type I Report - Final.pdf>



[Draft] Fw: Evaluation Committee Meeting Agenda for Event 332: Automated School Zone Speed Detection Camera System: Reference check

From
Draft saved Thu 11/21/2024 15:36

From: Kirk McDonald <KMcDonald@fortlauderdale.gov>
Sent: Wednesday, November 13, 2024 6:17:36 PM
To: Jason Friedberg <jfriedberg@bluelinesolutions.org>
Cc: Jonmichael Mullins <jmullins@bluelinesolutions.org>
Subject: RE: Evaluation Committee Meeting Agenda for Event 332: Automated School Zone Speed Detection Camera System: Reference check

Dear Jason,

The Evaluation Committee (EC) shortlist meeting was held today, November 13, 2024, for RFP No. 332, Automated School Zone Speed Detection Camera System. In the meeting, the EC determined that Blue Line Solutions, LLC is the highest ranked, responsive, and responsible firm. As a result of the EC’s decision, the Procurement Services Division must move forward with ensuring compliance with the RFP requirement pursuant to Addendum No. 3 of the RFP, whereby it states:

“Negotiations will occur with the highest ranked, responsive, and responsible firm contingent upon receipt of a current SSAE, SOC 2, Type I report to be provided within 60 days after proposal due date. Awarded Contractor will be required to provide an SSAE 18, SOC, Type II report annually during the term of [t]his contract. If the Contractor cannot provide the SSAE, SOC2, Type I report at the required time, a current SOC 3 report will be accepted.”

Subsequently, Competitive Negotiations is the next phase of this competitive process. Blue Line Solutions, LLC is to submit its SOC Report as required by the above-mentioned Addendum No. 3 language by no later than **Friday, November 15th, 2024, at 5:00p.m.** Feel free to contact me with any questions you may have.

Respectfully,

Kirk McDonald
Senior Procurement Specialist

City of Fort Lauderdale | Procurement Services Division
101 NE 3rd Avenue, Suite 1650 | Fort Lauderdale, FL 33301
P 954-828-5073 | F 954-828-5576 | kmcdonald@fortlauderdale.gov
Integrity – Compassion – Accountability – Respect – Excellence



Integrity – Compassion – Accountability – Respect – Excellence

EXHIBIT 3

System and Organization Controls (SOC) 2 Type I Report

And the Suitability of Design of Controls Relevant to the Trust
Services Criteria for Security Category

As of September 13, 2024

Together with Independent Service
Auditor's Report

Report on Management's Description of

BLUELINE

CAM #25-0379
SOLE Exhibit 4 NS
Page 32 of 64

TABLE OF CONTENTS

I. Independent Service Auditor's Report	3
II. Assertion of Blue Line Solutions, LLC Management	6
III. Description of the New Guard Platform	8
IV. Description of Design of Controls and Results Thereof	20



Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

Blue Line Solutions, LLC

Scope

We have examined Blue Line Solutions, LLC's accompanying description of its New Guard Platform (system) titled "Description of the New Guard Platform" as of September 13, 2024 (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design of controls stated in the description as of September 13, 2024, to provide reasonable assurance that Blue Line Solutions, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

Service Organization's Responsibilities

Blue Line Solutions, LLC is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Blue Line Solutions, LLC's service commitments and system requirements were achieved. Blue Line Solutions, LLC has provided the accompanying assertion titled "Assertion of Blue Line Solutions, LLC's Management" (assertion) about the description and the suitability of the design of controls stated therein. Blue Line Solutions, LLC is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

- a. The description presents Blue Line Solutions, LLC's New Guard Platform (system) that was designed and implemented as of September 13, 2024, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed as of September 13, 2024, to provide reasonable assurance that Blue Line Solutions, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of that date.

Restricted Use

This report is intended solely for the information and use of Blue Line Solutions, LLC, user entities of Blue Line Solutions, LLC's New Guard Platform (system) as of September 13, 2024, business partners of Blue Line Solutions, LLC subject to risks arising from interactions with the New Guard Platform (system), practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Johanson Group LLP

Colorado Springs, Colorado
October 16, 2024



Section II

ASSERTION OF BLUE LINE SOLUTIONS, LLC
MANAGEMENT

We have prepared the accompanying description of Blue Line Solutions, LLC's New Guard Platform (system) titled "Description of the New Guard Platform as of September 13, 2024," (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria*, (description criteria). The description is intended to provide report users with information about the New Guard Platform (system) that may be useful when assessing the risks arising from interactions with Blue Line Solutions, LLC's system, particularly information about system controls that Blue Line Solutions, LLC has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

We confirm, to the best of our knowledge and belief, that:

- a. The description presents Blue Line Solutions, LLC's New Guard Platform (system) that was designed and implemented as of September 13, 2024, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed as of September 13, 2024, to provide reasonable assurance that Blue Line Solutions, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of that date.

Blue Line Solutions, LLC Management
October 16, 2024



Section III

DESCRIPTION OF THE NEW GUARD PLATFORM

COMPANY BACKGROUND

Blue Line Solutions, headquartered in Chattanooga, TN, with offices in Shreveport, LA, and Hollywood, FL, specializes in reducing vehicle speeds and increasing safety through photo speed enforcement and advanced technology. We partner with communities to enhance safety and equip police agencies with intelligence to proactively prevent crimes.

DESCRIPTION OF SERVICES OVERVIEW OR SERVICES PROVIDED

New Guard provides law enforcement agencies with an end-to-end solution for reviewing, approving, and managing citations. It also offers violators a platform to review past citations and pay their current citations. This system description covers the New Guard platform and its capabilities. Other Blue Line Solutions services are not within the scope of this report.

The New Guard platform by Blue Line Solutions focuses on the following activities: citation review and approval for law enforcement, citation management, citation payment processing for violators, and Automatic License Plate Recognition (ALPR). Law enforcement agencies can efficiently review and approve citations using New Guard's streamlined interface, while violators have access to a secure platform where they can view past citations and pay their current ones. Additionally, the system incorporates ALPR technology, enabling law enforcement to automate license plate recognition for the identification of wanted vehicles.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Blue Line Solutions LLC designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Blue Line Solutions LLC makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Blue Line Solutions LLC has established for the services. The system services are subject to the Security commitments established internally for its services.

Blue Line Solutions communicates its system and service commitments to customers through Service Level Agreements (SLAs).

Security Commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Uptime availability of production systems

COMPONENTS OF THE SYSTEM

The System description is comprised of the following components:

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).

- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, as well as reports and other information prepared.

Infrastructure

Blue Line Solutions LLC maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents the device name, inventory type, description, and owner. To outline the topology of its network, the organization maintains the following network diagram(s).

Primary Infrastructure		
Hardware	Type	Purpose
Azure Platform	Azure	Managed cloud platform where services are hosted
Nova Datacenter	Co-Datacenter	Private data center for services that include CJL.

Software

Blue Line Solutions LLC is responsible for managing the development and operation of the New Guard Platform system including infrastructure components such as servers, databases, and storage systems. The in-scope Blue Line Solutions LLC infrastructure and software components are shown in the table provided below:

Primary Software		
System/Application	Type	Purpose
Papertrail	Logging and Monitoring	Real-time logging and event monitoring
Azure DevOps	Development Platform	Continuous integration and delivery, version control, and project management
GitHub	Version Control	Repository hosting and version control for code collaboration
Microsoft Defender for Endpoint	Security Tool	Endpoint protection and threat detection
Insightly	CRM and Ticketing System	Customer relationship management and project tracking
Atlassian Status page	Incident Communication	Communication tool for system status and incidents
Elastic	Reporting Tool	Full-text search and analytics engine
RabbitMQ	Messaging Queue	Message broker for handling asynchronous communication between services
JSReport	Reporting Tool	Generates dynamic PDFs
Foldermill	Workflow Automation	Automates document printing
NServiceBus	Messaging System	Service bus for managing asynchronous messaging between distributed systems
Microsoft IIS	Web Server	Web server for hosting websites and web applications
Send Grid	Email Service	To send automated emails for onboarding and password resets.
Azure Virtual Machine	Azure	Virtual machine service for web hosting and backend service offerings
Azure Kubernetes	Azure	Container orchestration for deployment, scaling, and management
Azure Database	Azure	Transactional database with backups and redundancy

Azure Cosmos DB	Azure	Globally distributed NoSQL database for high availability and scalability
Azure Storage	Azure	Cloud storage for data, backups, and file sharing
Microsoft SQL Server	Database	Relational database management system

People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Blue Line Solutions LLC has a staff of approximately 100 organized in the following functional areas:

- **Management:** Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

This includes:

- CEO - Mark Hutchinson
 - CFO - Jeff Oxner
 - CTO - Zach Watts
 - COO - Doug Deihl
- **Processing:** Responsible for managing citation processing and ensuring compliance with laws and regulations. This team handles the verification, validation, and follow-up of citations to ensure proper enforcement.
 - **Permitting:** Oversees the issuance and management of permits related to various enforcement programs. Ensures compliance with state and local regulations regarding permits.
 - **Information Technology:** Responsible for managing laptops, software, and other technology involved in employee productivity and business operations. Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure.
 - **Product Development:** Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.
 - **Production and Service:** Responsible for the installation of equipment, project management, and monitoring the availability of equipment. This team ensures that equipment is deployed and maintained correctly and oversees the successful execution of service projects.
 - **Sales:** Focused on generating revenue by engaging potential customers, maintaining customer relationships, and promoting the products and services offered by the company.
 - **Finance:** Responsible for managing the financial operations of the company, including budgeting, payroll, financial reporting, and ensuring financial compliance with regulations.

Data

Data as defined by Blue Line Solutions LLC, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant

third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized into the following major types of data used by Blue Line Solutions LLC.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Blue Line Solutions LLC.	<ul style="list-style-type: none"> • Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	<ul style="list-style-type: none"> • Internal memos • Design documents • Product specifications • Correspondences
Customer Data	Information received from customers for processing or storage by Blue Line Solutions LLC. Blue Line Solutions LLC must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	<ul style="list-style-type: none"> • Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company Data	Information collected and used by Blue Line Solutions LLC to operate the business. Blue Line Solutions LLC must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	<ul style="list-style-type: none"> • Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Blue Line Solutions LLC has policies and procedures in place for the proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

PROCESSES AND PROCEDURES

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security

Blue Line Solutions LLC's production servers are maintained by Microsoft Azure, Wasabi, and Nova. The physical and environmental security protections are the responsibility of Microsoft Azure, Wasabi, and Nova. Blue Line Solutions LLC reviews the attestation reports and performs a risk analysis of Microsoft Azure, Wasabi, and Nova on at least an annual basis.

Logical Access

Blue Line Solutions LLC provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privileged access to identified users and to maintain simple and repeatable user provisioning and de-provisioning processes.

Access to these systems is split into admin roles, user roles, and no-access roles. User access and roles are reviewed on an annual basis to ensure the least privileged access.

Information Technology is responsible for providing access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Blue Line Solutions LLC's policies and completing security training. These steps must be completed within 30 days of hire.

When an employee is terminated, Information Technology is responsible for de-provisioning access to all in-scope systems within 3 business days of that employee's termination.

Computer Operations - Backups

Customer data is backed up and monitored by the IT Team for completion and exceptions. If there is an exception, the IT Team will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in Microsoft Azure, Wasabi, and Nova with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations - Availability

Blue Line Solutions LLC maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

Blue Line Solutions LLC internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Blue Line Solutions LLC utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

Change Management

Blue Line Solutions LLC maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Blue Line Solutions LLC has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Blue Line Solutions LLC application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and de-provisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on the underlying hardware.

Blue Line Solutions uses an automated monitoring service for regular vulnerability scans and engages an external firm to perform annual penetration testing to identify any undiscovered vulnerabilities. Our product engineering team addresses any identified issues through our standard incident response and change management processes, ensuring the ongoing security and integrity of the New Guard platform.

BOUNDARIES OF THE SYSTEM

The boundaries of the New Guard Platform are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the New Guard Platform.

This report does not include the Cloud Hosting Services provided by Azure at multiple facilities.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

Common Criteria (to the Security Category)
<p>Security refers to the protection of</p> <ul style="list-style-type: none"> i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Blue Line Solutions LLC's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Blue Line Solutions LLC's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Blue Line Solutions LLC's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

The Blue Line Solutions LLC management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Blue Line Solutions LLC can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally, any regulatory changes that may require Blue Line Solutions LLC to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

Blue Line Solutions LLC's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Blue Line Solutions LLC's assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Blue Line Solutions LLC's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensure the service organization is operating at maximum efficiency. Blue Line Solutions LLC's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Personnel termination procedures are in place to guide the termination process and are documented in a termination checklist.

RISK ASSESSMENT PROCESS

Blue Line Solutions LLC's risk assessment process identifies and manages risks that could potentially affect Blue Line Solutions LLC's ability to provide reliable and secure services to our customers. As part of this process, Blue Line Solutions LLC maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Blue Line Solutions LLC product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Blue Line Solutions LLC's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Blue Line Solutions LLC addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Blue Line Solutions LLC's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

INFORMATION AND COMMUNICATION SYSTEMS

Information and communication are an integral component of Blue Line Solutions LLC's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Blue Line Solutions LLC uses several information and communication channels internally to share information with management, employees, contractors, and customers. Blue Line Solutions LLC uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Blue Line Solutions LLC uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Blue Line Solutions LLC's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Blue Line Solutions LLC's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Blue Line Solutions LLC's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Blue Line Solutions LLC's personnel.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

CHANGES TO THE SYSTEM

No significant changes have occurred to the services provided to user entities in the last 3 months preceding the end of the review date.

INCIDENTS

No significant incidents have occurred to the services provided to user entities in the last 3 months preceding the end of the review date.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All Common Security Criteria were applicable to Blue Line Solutions LLC's New Guard Platform system.

SUBSERVICE ORGANIZATIONS

This report does not include the Cloud Hosting Services provided by Azure at multiple facilities.

Subservice Description of Services

The Cloud Hosting Services provided by Azure support the physical infrastructure of the entity's services.

Complementary Subservice Organization Controls

Blue Line Solutions LLC's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Blue Line Solutions LLC's services to be solely achieved by Blue Line Solutions LLC control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Blue Line Solutions LLC.

The following subservice organization controls have been implemented by Microsoft Azure, Wasabi, and Nova and included in this report to provide additional assurance that the trust services criteria are met.

Subservice Organization - Azure		
Category	Criteria	Control
Security	CC 6.4	Procedures to restrict physical access to the data center to authorized employees, vendors, contractors, and visitors, have been established.
Security	CC 6.4	Security verification and check-in for personnel requiring temporary access to the interior of the data center facility, including tour groups or visitors, are required.
Security	CC 6.4	Physical access to the data center is reviewed quarterly and verified by the Datacenter Management team.
Security	CC 6.4	Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
Security	CC 6.4	The data center facility is monitored 24x7 by security personnel.

Blue Line Solutions LLC management, along with the subservice provider, defines the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Blue Line Solutions LLC performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Making regular site visits to vendor and subservice organization(s') facilities
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Blue Line Solutions LLC's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Blue Line Solutions LLC's services to be solely achieved by Blue Line Solutions LLC control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Blue Line Solutions LLC.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Blue Line Solutions LLC.
2. User entities are responsible for notifying Blue Line Solutions LLC of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Blue Line Solutions LLC services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Blue Line Solutions LLC services.
6. User entities are responsible for providing Blue Line Solutions LLC with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Blue Line Solutions LLC of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.



Section IV

DESCRIPTION OF DESIGN OF CONTROLS AND
RESULTS THEREOF

Relevant trust services criteria and Blue Line Solutions, LLC-related controls are an integral part of management's system description and are included in this section. Johanson Group LLP assessed if Blue Line Solutions, LLC's controls were suitably designed to meet the specified criteria for the security category set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*, as of September 13, 2024.

Assessment of control design included inquiry of appropriate management, supervisory, and staff personnel and the inspection of Blue Line Solutions, LLC's policy and procedure documentation. The results of those assessments were considered in the planning, the nature, timing, and extent of Johanson LLP's review of the controls designed to address the relevant trust services criteria. Being a Type I SOC 2 report, there were no tests performed to determine the operational effectiveness of each designed control.

Criteria Number	Trust Services Criteria	Description of Blue Line Solutions, LLC's Controls	Result
CONTROL ENVIRONMENT			
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.	Control determined to be suitably designed.
		The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Control determined to be suitably designed.
		The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Control determined to be suitably designed.
		The company requires contractors to sign a confidentiality agreement at the time of engagement.	Control determined to be suitably designed.
		The company requires employees to sign a confidentiality agreement during onboarding.	Control determined to be suitably designed.
		The company managers are required to complete performance evaluations for direct reports at least annually.	Control determined to be suitably designed.
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company management demonstrates a commitment to integrity and ethical values.	Control determined to be suitably designed.
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Control determined to be suitably designed.
		The company maintains an organizational chart that describes the organizational structure and reporting lines.	Control determined to be suitably designed.
		Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Control determined to be suitably designed.
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Blue Line Solutions, LLC's Controls	Result
		The company performs background checks on new employees.	Control determined to be suitably designed.
		The company managers are required to complete performance evaluations for direct reports at least annually.	Control determined to be suitably designed.
		The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Control determined to be suitably designed.
CC 1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Control determined to be suitably designed.
		The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Control determined to be suitably designed.
		The company managers are required to complete performance evaluations for direct reports at least annually.	Control determined to be suitably designed.
COMMUNICATION AND INFORMATION			
CC 2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Control determined to be suitably designed.
		The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Control determined to be suitably designed.
		Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Control determined to be suitably designed.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Control determined to be suitably designed.
		The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Control determined to be suitably designed.
		Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Control determined to be suitably designed.
		The company's information security policies and procedures are documented and reviewed at least annually.	Control determined to be suitably designed.
		The company communicates system changes to authorized internal users.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Blue Line Solutions, LLC's Controls	Result
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Control determined to be suitably designed.
		The company provides a description of its products and services to internal and external users.	Control determined to be suitably designed.
		The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Control determined to be suitably designed.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company notifies customers of critical system changes that may affect their processing.	Control determined to be suitably designed.
		The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Control determined to be suitably designed.
		The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Control determined to be suitably designed.
		The company provides guidelines and technical support resources relating to system operations to customers.	Control determined to be suitably designed.
		The company provides a description of its products and services to internal and external users.	Control determined to be suitably designed.
		The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Control determined to be suitably designed.
RISK ASSESSMENT			
CC 3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Control determined to be suitably designed.
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.
CC 3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Control determined to be suitably designed.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Blue Line Solutions, LLC's Controls	Result
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.
		The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Control determined to be suitably designed.
CC 3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Control determined to be suitably designed.
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Control determined to be suitably designed.
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Control determined to be suitably designed.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Control determined to be suitably designed.
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.
MONITORING ACTIVITIES			
CC 4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Blue Line Solutions, LLC's Controls	Result
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Control determined to be suitably designed.
		The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Control determined to be suitably designed.
		Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Control determined to be suitably designed.
CC 4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Control determined to be suitably designed.
		The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Control determined to be suitably designed.
CONTROL ACTIVITIES			
CC 5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company's information security policies and procedures are documented and reviewed at least annually.	Control determined to be suitably designed.
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Control determined to be suitably designed.
		The company's information security policies and procedures are documented and reviewed at least annually.	Control determined to be suitably designed.
		The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Control determined to be suitably designed.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Blue Line Solutions, LLC's Controls	Result
		The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Control determined to be suitably designed.
		The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Control determined to be suitably designed.
		The company's data backup policy documents requirements for the backup and recovery of customer data.	Control determined to be suitably designed.
		Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Control determined to be suitably designed.
		The company's information security policies and procedures are documented and reviewed at least annually.	Control determined to be suitably designed.
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Control determined to be suitably designed.
		The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Control determined to be suitably designed.
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.
		The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Control determined to be suitably designed.
LOGICAL AND PHYSICAL ACCESS			
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company maintains a formal inventory of production system assets.	Control determined to be suitably designed.
		The company restricts access to migrate changes to production to authorized personnel.	Control determined to be suitably designed.
		The company requires authentication to production data stores to use authorized secure authentication mechanisms, such as a unique SSH key.	Control determined to be suitably designed.
		The company restricts privileged access to encryption keys to authorized users with a business need.	Control determined to be suitably designed.
		The company's data stores housing sensitive customer data are encrypted at rest.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Blue Line Solutions, LLC's Controls	Result
		The company requires authentication to systems and applications to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Control determined to be suitably designed.
		The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Control determined to be suitably designed.
		System access is restricted to authorized access only.	Control determined to be suitably designed.
		The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Control determined to be suitably designed.
		The company restricts privileged access to databases to authorized users with a business need.	Control determined to be suitably designed.
		The company restricts privileged access to the firewall to authorized users with a business need.	Control determined to be suitably designed.
		The company restricts privileged access to the operating system to authorized users with a business need.	Control determined to be suitably designed.
		The company restricts privileged access to the production network to authorized users with a business need.	Control determined to be suitably designed.
		The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Control determined to be suitably designed.
		The company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Control determined to be suitably designed.
		The company requires passwords for in-scope system components to be configured according to the company's policy.	Control determined to be suitably designed.
		The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Control determined to be suitably designed.
		The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Control determined to be suitably designed.
		The company's network is segmented to prevent unauthorized access to customer data.	Control determined to be suitably designed.
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Control determined to be suitably designed.
		The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Blue Line Solutions, LLC's Controls	Result
		The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Control determined to be suitably designed.
		The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Control determined to be suitably designed.
		The company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Control determined to be suitably designed.
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Control determined to be suitably designed.
		The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Control determined to be suitably designed.
		The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Control determined to be suitably designed.
		The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Control determined to be suitably designed.
		The company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Control determined to be suitably designed.
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The entity does not operate any physical hardware such as servers and network devices but rather uses subservice organizations and relies on its own controls for physical access.	Control determined to be suitably designed.
		The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Control determined to be suitably designed.
		The company requires visitors to sign in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Blue Line Solutions, LLC's Controls	Result
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Control determined to be suitably designed.
		The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Control determined to be suitably designed.
		The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Control determined to be suitably designed.
		The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Control determined to be suitably designed.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the production network to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Control determined to be suitably designed.
		The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Control determined to be suitably designed.
		The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Control determined to be suitably designed.
		The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Control determined to be suitably designed.
		The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Control determined to be suitably designed.
		The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Control determined to be suitably designed.
		The company uses firewalls and configures them to prevent unauthorized access.	Control determined to be suitably designed.
		The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Control determined to be suitably designed.
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Control determined to be suitably designed.
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company encrypts portable and removable media devices when used.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Blue Line Solutions, LLC's Controls	Result
		The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Control determined to be suitably designed.
		The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Control determined to be suitably designed.
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Control determined to be suitably designed.
		The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Control determined to be suitably designed.
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Control determined to be suitably designed.
SYSTEM OPERATIONS			
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Control determined to be suitably designed.
		The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Control determined to be suitably designed.
		The company's formal policies outline the requirements for the following functions related to IT / Engineering: vulnerability management and system monitoring.	Control determined to be suitably designed.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Control determined to be suitably designed.
		Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Blue Line Solutions, LLC's Controls	Result
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Control determined to be suitably designed.
		The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Control determined to be suitably designed.
		The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Control determined to be suitably designed.
		An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Control determined to be suitably designed.
		The company's formal policies outline the requirements for the following functions related to IT / Engineering: vulnerability management and system monitoring.	Control determined to be suitably designed.
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Control determined to be suitably designed.
		Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Control determined to be suitably designed.
CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Control determined to be suitably designed.
		The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Control determined to be suitably designed.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company tests its incident response plan at least annually.	Control determined to be suitably designed.
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Blue Line Solutions, LLC's Controls	Result
		The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Control determined to be suitably designed.
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Control determined to be suitably designed.
		Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Control determined to be suitably designed.
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Control determined to be suitably designed.
		The company tests its incident response plan at least annually.	Control determined to be suitably designed.
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Control determined to be suitably designed.
		The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Control determined to be suitably designed.
CHANGE MANAGEMENT			
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Control determined to be suitably designed.
		The company restricts access to migrate changes to production to authorized personnel.	Control determined to be suitably designed.
		The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Control determined to be suitably designed.
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Control determined to be suitably designed.
		The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Blue Line Solutions, LLC's Controls	Result
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Control determined to be suitably designed.
		Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Control determined to be suitably designed.
RISK MITIGATION			
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Control determined to be suitably designed.
		The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Control determined to be suitably designed.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Control determined to be suitably designed.
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Control determined to be suitably designed.
		The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Control determined to be suitably designed.