Procurement
300 Turner Street NW
North End Center, Ste 2100
Blacksburg, Virginia 24061
P: (540) 231-6221 F: (540) 231-9628
www.procurement.vt.edu

July 16, 2024

Rileen Innovative Technologies Inc
Richard A Johnson
828 Brooke Rd
Virginia Beach, VA 23452

Dear Richard,

Subject: Contract Renewal Letter

Virginia Tech Contract #:	VTS-2097-2024
Commodity/Service:	Security Operations Consultant
Renewal Period:	8/1/24 - 7/31/25
Renewal #:	(1 of 4) one-year renewal

In accordance with the renewal provision of the original contract, the university would like to renew the contract for an additional term. Please advise concerning your intention by signing in the appropriate space below. A signed copy of this letter should be received in Procurement by ASAP.

If allowed by the contract, price adjustments must be requested at the time of renewal in accordance with the contract documents. Price adjustments are not automatic or retroactive and are only implemented upon request by the vendor at the time of renewal.

In addition, review the attached form which shows your company information as listed in the university's vendor database. If any of this information has changed, make corrections directly on the form, and return with this letter. It is essential this information be accurate for payments to be processed in a timely manner.

Virginia Tech recommends that our vendors utilize the Wells One AP Control Payment System for payment of all invoices and strongly encourages all vendors under contract with the university to participate in this program. If your firm is not enrolled in the program, refer to our website: http://www.procurement.vt.edu/Vendor/WellsOne.html or contact me directly for more information.

Sincerely,

Chad Dalton
Procurement Contract Support Specialist
(540) 231-9129

Rileen Innovative Technologies Inc **agrees** to renew the contract under the terms and conditions of the subject contract.

DocuSigned by:
Authorized Signature: Richard A Johnson
9B69A1E0297A4EC...
Date: 7/16/2024

Name: Richard A Johnson
(please print)
Title: President / CEO

We currently participate in the Wells One Program: _____

We would like to participate in the Wells One Program: X

DocuSigned by:
Approved: Reed Nagel
5EF51DA320D049B...
Reed Nagel
Associate Director for Goods and Services

Date: 7/16/2024

COMMONWEALTH OF VIRGINIA

STANDARD CONTRACT

Contract Number: VTS-2097-2024

This contract entered into this 1st day of August 2023 by RILEEN Innovative Technologies, Inc. hereinafter called the "Contractor" and Commonwealth of Virginia, Virginia Polytechnic Institute and State University called "Virginia Tech."

WITNESSETH that the Contractor and Virginia Tech, in consideration of the mutual covenants, promises and agreements herein contained, agree as follows:

SCOPE OF CONTRACT: The Contractor shall provide security operations consulting services to Virginia Tech as set forth in the Contract Documents.

PERIOD OF CONTRACT: From August 1st, 2023 through July 31st, 2024, with the option of four (4) one (1) year renewals.

COMPENSATION AND METHOD OF PAYMENT: The Contractor shall be paid by Virginia Tech in accordance with the Contract Documents.

CONTRACT DOCUMENTS: The Contract Documents shall consist of this signed contract, Request for Proposal (RFP) number 218672311 dated June 28th, 2023, together with Addendum Number 1 To RFP dated July 7th, 2023, the proposal submitted by the Contractor dated July 19th, 2023 and the Summary of Negotiations, all of which Contract Documents are incorporated herein.

ELECTRONIC TRANSACTIONS: If this paragraph is initialed by both parties, to the fullest extent permitted by Code of Virginia, Title 59.1, Chapter 42.1, the parties do hereby expressly authorize and consent to the use of electronic signatures as an additional method of signing and/or initialing this contract and agree electronic signatures (for example, the delivery of a PDF copy of the signature of either party via facsimile or electronic mail or signing electronically by utilizing an electronic signature service) are the same as manual executed handwritten signatures for the purposes of validity, enforceability and admissibility.

DS RN

(Initials)

In WITNESS WHEREOF, the parties have caused this Contract to be duly executed intending to be bound thereby.

Contractor
By: _____
(Signature)

Richard A. Johnson / President
Name and Title

Virginia Tech
By: DocuSigned by: Reed Nagel 5EF51DA320D049B...

Reed Nagel
Associate Director of Procurement

Request for Proposal #218672311

For

Security Operations Consultant for Virginia Tech

6/28/2023

Note: This public body does not discriminate against faith-based organizations in accordance with the *Code of Virginia*, § 2.2-4343.1 or against a bidder or offeror because of race, religion, color, sex, sexual orientation, gender identity, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment.

RFP # 218672311, Security Operations Consultant

INCLUDE THIS PAGE WITH YOUR PROPOSAL, SIGNATURE AT SUBMISSION IS REQUIRED

DUE DATE: Proposals will be received until Wednesday July 19th, 2023 at 3:00 PM. Failure to submit proposals to the correct location by the designated date and hour will result in disqualification.

INQUIRIES: All inquiries for information regarding this solicitation should be directed to Bryan Holloway, Phone: (540) 231- 8545 e-mail: bryanh91@vt.edu. All inquiries will be answered in the form of an addendum. Inquiries must be submitted by 12:00PM on Friday July 7th, 2023. Inquiries must be submitted to the procurement officer identified in this solicitation.

PROPOSAL SUBMISSION:

Please note, proposal submission procedures have changed effective March 2023.

Proposals may NOT be hand delivered to the Procurement Office.

Proposals should be submitted electronically through Virginia Tech's procurement portal. This portal allows you access to view business opportunities and submit bids and proposals to Virginia Tech digitally and securely.

Proposals must be submitted electronically at:
https://bids.sciquest.com/apps/Router/PublicEvent?CustomerOrg=VATech

Vendors will need to register through this procurement portal, hosted by Jaggaer. **It is encouraged for all vendors to register prior to the proposal submission deadline to avoid late submissions**. Registration is easy and free. If you have any challenges with the registration process, please contact Jaggaer Support at 1-800-233-1121 or procurement@vt.edu.

Click on the opportunity and log in to your vendor account to begin preparing your submission. Upon completion, you will receive a submission receipt email confirmation. Virginia Tech will not confirm receipt of proposals. It is the responsibility of the offeror to make sure their proposal is delivered on time.

Hard copy or email proposals will not be accepted. Late proposals will not be accepted, nor will additional time be granted to any individual Vendor.

Attachments must be smaller than 50MB in order to be received by the University.

In compliance with this Request For Proposal and to all the conditions imposed therein and hereby incorporated by reference, the undersigned offers and agrees to furnish the goods or services in accordance with the attached signed proposal and as mutually agreed upon by subsequent negotiation.

AUTHORIZED SIGNATURE: _____ Date: _____

[INCLUDE THIS PAGE]

I. PURPOSE:

This Request for Proposal (RFP) seeks to solicit proposals to establish a contract through competitive negotiations for Security Screening Equipment by Virginia Polytechnic Institute and State University (Virginia Tech), an agency of the Commonwealth of Virginia.

Virginia Polytechnic Institute and State University (Virginia Tech) is located in Blacksburg, Virginia, approximately 40 miles southwest of Roanoke, Virginia, the major commercial hub of the area. In addition to the university's main campus in Blacksburg, major off campus locations include twelve agriculture experiment research stations, the Marion duPont Scott Equine Medical Center and graduate centers in Roanoke and Fairfax, Virginia. Regularly scheduled air service is provided at the Roanoke Regional Airport.

Dedicated to its motto, Ut Prosim (That I May Serve), Virginia Tech takes a hands-on, engaging approach to education, preparing scholars to be leaders in their fields and communities. As the Commonwealth's most comprehensive university and its leading research institution, Virginia Tech offers 240 undergraduate degree programs to more than 31,000 students and manages a research portfolio of nearly $513 million. The university fulfills its land-grant mission of transforming knowledge to practice through technological leadership and by fueling economic growth and job creation locally, regionally, and across Virginia.

The purpose of this Request for Proposal (RFP) is to solicit sealed proposals to establish a term contract with one or more qualified vendors to provide security operations consulting to Virginia Tech across various campus locations. Virginia Tech is interested in seeking proposals from qualified vendors who have security operations consulting experience with an emphasis on major events and athletic venues. These consulting services may include, but are not limited to: overseeing the security screening process during sanctioned events, constructing crowd flow plans, ensuring that the University is purchasing the correct accessories needed in order to operate our screening equipment, coordinate with Emergency Management on campus to develop appropriate training procedures and guidelines, and to provide overall guidance to the University about our security screening process. Virginia Tech will be utilizing the CEIA Open Gate system for all of our security screening needs on campus, and the Consultant should be well versed with this system and its capabilities if proposing.

II. SMALL, WOMAN-OWNED AND MINORITY (SWAM) BUSINESS PARTICIPATION:

The mission of the Virginia Tech supplier opportunity program is to foster inclusion in the university supply chain and accelerate economic growth in our local communities through the engagement and empowerment of high quality and cost competitive small, minority-owned, women-owned, and local suppliers. Virginia Tech encourages prime suppliers, contractors, and service providers to facilitate the participation of small businesses, and businesses owned by women and minorities through partnerships, joint ventures, subcontracts, and other inclusive and innovative relationships.

For more information, please visit: https://www.sbsd.virginia.gov/

III. CONTRACT PERIOD:

The term of this contract is for one (1) year(s), or as negotiated. There will be an option for four (4) one (1) year renewals, or as negotiated.

IV. EVA BUSINESS-TO-GOVERNMENT ELECTRONIC PROCUREMENT SYSTEM:

The eVA Internet electronic procurement solution streamlines and automates government purchasing activities within the Commonwealth of Virginia. Virginia Tech, and other state agencies and institutions, have been directed by the Governor to maximize the use of this system in the procurement of goods and services. *We are, therefore, requesting that your firm register as a vendor within the eVA system.*

There are transaction fees involved with the use of eVA. These fees must be considered in the provision of quotes, bids and price proposals offered to Virginia Tech. Failure to register within the eVA system may result in the quote, bid or proposal from your firm being rejected and the award made to another vendor who is registered in the eVA system.

Registration in the eVA system is accomplished on-line. Your firm must provide the necessary information. Please visit the eVA website portal at http://www.eva.virginia.gov/pages/eva-registration-buyer-vendor.htm and **register both with eVA and Ariba**. *This process needs to be completed before Virginia Tech can issue your firm a Purchase Order or contract.* If your firm conducts business from multiple geographic locations, please register these locations in your initial registration.

For registration and technical assistance, reference the eVA website at: https://eva.virginia.gov/, or call 866-289-7367 or 804-371-2525.

V. CONTRACT PARTICIPATION:

It is the intent of this solicitation and resulting contract to allow for cooperative procurement. Accordingly, any public body, public or private health or educational institutions, or Virginia Tech's affiliated corporations and/or partnerships may access any resulting contract if authorized by the contractor.

Participation in this cooperative procurement is strictly voluntary. If authorized by the Contractor, the resultant contract may be extended to the entities indicated above to purchase at contract prices in accordance with contract terms. The Contractor shall notify Virginia Tech in writing of any such entities accessing the contract, if requested. No modification of this contract or execution of a separate contract is required to participate. The Contractor will provide semi-annual usage reports for all entities accessing the Contract, as requested. Participating entities shall place their own orders directly with the Contractor and shall fully and independently administer their use of the contract to include contractual disputes, invoicing and payments without direct administration from Virginia Tech. Virginia Tech shall not be held liable for any costs or damages incurred by any other participating entity as a result of any authorization by the Contractor to extend the contract. It is understood and agreed that Virginia Tech is not responsible for the acts or omissions of any entity, and will not be considered in default of the contract no matter the circumstances.

Use of this contract does not preclude any participating entity from using other contracts or competitive processes as the need may be.

VI. STATEMENT OF NEEDS/SCOPE OF WORK:

A. Consultant Requirements:

1. It is Virginia Tech's desire to contract with a vendor who can provide security operations consulting services, with an emphasis on major events and athletic venues. Some locations that may be of interest here on campus may include, but are not limited to: Lane Stadium, Cassell Coliseum, Burrus Hall, English Field at Atlantic Union Bank Park, etc.

2. The Contractor must have experience with the CEIA Open Gate Security Screening System.

3. The Contractor may be required to work with Virginia Tech's existing security services provider to ensure proper services and procedures are in place.

4. Security consulting services may include, but are not limited to:

    a) Providing an initial assessment of Virginia Tech's existing security infrastructure, policies, and procedures.

    b) Providing oversight during game day operations to ensure our security operations are running effectively and efficiently.

    c) To ensure Virginia Tech has purchased all of the required equipment and accessories, and advise if any additional equipment is recommended or necessary.

    d) Compile security operations data in order to provide informed recommendations based on industry best practices and compliance standards.

    e) Provide overall guidance to Virginia Tech on how to best utilize the CEIA Open Gate System and potential ways the University could improve upon its security screening process.

B. Training:

1. The selected offeror shall provide all applicable training materials necessary to operate the provided equipment. Upon request by Virginia Tech, the selected offeror shall provide onsite training as necessary. The cost associated with any training should be included in the offeror's pricing proposal based on an hourly rate.

C. Mandatory Requirement of Submittal References:

1. The contractor shall have previous experience with providing security operations consulting services. Two references from clients on such work will be required as a part of your submission.

VII. PROPOSAL PREPARATION AND SUBMISSION:

A. Specific Requirements

Proposals should be as thorough and detailed as possible so that Virginia Tech may properly evaluate your capabilities to provide the required goods or services. Offerors are required to submit the following information/items as a complete proposal:

1. Provide a detailed proposal that defines your consulting strategy and any costs associated. Discuss the advantages of your proposed plan and methodology, and how it will support the mission of Virginia Tech.

2. Provide a detailed pricing plan to include all of the consulting services, training materials, and any other associated costs. Pricing related to consulting services should be submitted in a Labor / Hour format.

3. Identify the individual(s) who will serve as the primary contact for the university, providing their qualifications and consulting experience relating to security operations and event management consulting.

4. A written statement to include, but not limited to the expertise, qualifications and experience of the firm and resumes of specific personnel to be assigned to perform the work. Include two (2) references from organizations similar to Virginia Tech where you have performed this type of work that is similar in scope.

5. Participation of Small, Women-owned and Minority-owned Business (SWAM) Business:

   If your business cannot be classified as SWaM, describe your plan for utilizing SWaM subcontractors if awarded a contract. Describe your ability to provide reporting on SWaM subcontracting spend when requested. If your firm or any business that you plan to subcontract with can be classified as SWaM, but has not been certified by the Virginia Department of Small Business and Supplier Diversity (SBSD), it is expected that the certification process will be initiated no later than the time of the award. If your firm is currently certified, you agree to maintain your certification for the life of the contract. For assistance with SWaM certification, visit the SBSD website at http://www.sbsd.virginia.gov/

6. The return of the Submission Instruction page and addenda, if any, signed and filled out as required.

D. General Requirements

1. RFP Response: In order to be considered for selection, Offerors shall submit a complete response to this RFP to include;

   a. **One (1) electronic document** in WORD format or searchable PDF of the entire proposal as one document, INCLUDING ALL ATTACHMENTS must be uploaded through the Virginia Tech online submission portal. Refer to page 2 for instructions.

      Any proprietary information should be clearly marked in accordance with 2.d. below.

   b. Should the proposal contain **proprietary information**, provide **one (1) redacted electronic copy** of the proposal and attachments **with proprietary portions removed or blacked out**. This redacted copy should follow the same upload procedures as described on Page 1 of this RFP. This redacted copy should be clearly marked *"Redacted Copy"* within the name of the document. The classification of an entire proposal document, line item prices and/or total proposal prices as proprietary or trade secrets is not acceptable. Virginia Tech shall not be

responsible for the Contractor's failure to exclude proprietary information from this redacted copy.

No other distribution of the proposals shall be made by the Offeror.

2. Proposal Preparation:

   a. Proposals shall be signed by an authorized representative of the Offeror. All information requested should be submitted. Failure to submit all information requested may result in Virginia Tech requiring prompt submission of missing information and/or giving a lowered evaluation of the proposal. Proposals which are substantially incomplete or lack key information may be rejected by Virginia Tech at its discretion. Mandatory requirements are those required by law or regulation or are such that they cannot be waived and are not subject to negotiation.

   b. Proposals should be prepared simply and economically providing a straightforward, concise description of capabilities to satisfy the requirements of the RFP. Emphasis should be on completeness and clarity of content.

   c. Proposals should be organized in the order in which the requirements are presented in the RFP. All pages of the proposal should be numbered. Each paragraph in the proposal should reference the paragraph number of the corresponding section of the RFP. It is also helpful to cite the paragraph number, subletter, and repeat the text of the requirement as it appears in the RFP. If a response covers more than one page, the paragraph number and subletter should be repeated at the top of the next page. The proposal should contain a table of contents which cross references the RFP requirements. Information which the offeror desires to present that does not fall within any of the requirements of the RFP should be inserted at an appropriate place or be attached at the end of the proposal and designated as additional material. Proposals that are not organized in this manner risk elimination from consideration if the evaluators are unable to find where the RFP requirements are specifically addressed.

   d. Ownership of all data, material and documentation originated and prepared for Virginia Tech pursuant to the RFP shall belong exclusively to Virginia Tech and be subject to public inspection in accordance with the Virginia Freedom of Information Act. Trade secrets or proprietary information submitted by an Offeror shall not be subject to public disclosure under the Virginia Freedom of Information Act. However, to prevent disclosure the Offeror must invoke the protections of Section 2.2-4342F of the Code of Virginia, in writing, either before or at the time the data or other materials is submitted. The written request must specifically identify the data or other materials to be protected and state the reasons why protection is necessary. –The proprietary or trade secret material submitted must be identified by some distinct method such as highlighting or underlining and must indicate only the specific words, figures, or paragraphs that constitute trade secret or proprietary information. The classification of an entire proposal document, line item prices and/or total proposal prices as proprietary or trade secrets is not acceptable and may result in rejection of the proposal.

3. Oral Presentation: Offerors who submit a proposal in response to this RFP may be required to give an oral presentation of their proposal to Virginia Tech.—This will provide an opportunity for the Offeror to clarify or elaborate on the proposal but will in no way change the original proposal. Virginia Tech will schedule the time and location of these presentations. Oral presentations are an option of Virginia Tech and may not be conducted. Therefore, proposals should be complete.

VIII. SELECTION CRITERIA AND AWARD:

A. Selection Criteria

Proposals will be evaluated by Virginia Tech using the following:

Criteria	Maximum Point Value
1. Quality of products/services offered and suitability for the intended purposes	20
2. Qualifications and experiences of Offeror in providing the goods/services	25
3. Specific plans or methodology to be used to provide the Services	25
4. Cost (or Price)	20
5. Participation of Small, Women-Owned and Minority (SWAM) Business	10
Total	100

B. Award

Selection shall be made of two or more offerors deemed to be fully qualified and best suited among those submitting proposals on the basis of the evaluation factors included in the Request for Proposal, including price, if so stated in the Request for Proposal. Negotiations shall then be conducted with the offerors so selected. Price shall be considered, but need not be the sole determining factor. After negotiations have been conducted with each offeror so selected, Virginia Tech shall select the offeror which, in its opinion, has made the best proposal, and shall award the contract to that offeror. Virginia Tech may cancel this Request for Proposal or reject proposals at any time prior to an award. Should Virginia Tech determine in writing and in its sole discretion that only one offeror has made the best proposal, a contract may be negotiated and awarded to that offeror. The award document will be a contract incorporating by reference all the requirements, terms and conditions of this solicitation and the Contractor's proposal as negotiated.

Virginia Tech reserves the right to award multiple contracts as a result of this solicitation.

IX. INVOICES:

Invoices for goods or services provided under any contract resulting from this solicitation shall be submitted by email to vtinvoices@vt.edu or by mail to:

Virginia Polytechnic Institute and State University (Virginia Tech)
Accounts Payable
North End Center, Suite 3300
300 Turner Street NW
Blacksburg, Virginia 24061

X. METHOD OF PAYMENT:

Virginia Tech will authorize payment to the contractor as negotiated in any resulting contract from the aforementioned Request for Proposal.

Payment can be expedited through the use of the Wells One AP Control Payment System. Virginia Tech strongly encourages participation in this program. For more information on this program please refer to Virginia Tech's Procurement website: http://www.procurement.vt.edu/vendor/wellsone.html or contact the procurement officer identified in the RFP.

XI. ADDENDUM:

Any **ADDENDUM** issued for this solicitation may be accessed at http://www.apps.vpfin.vt.edu/html.docs/bids.php. Since a paper copy of the addendum will not be mailed to you, we encourage you to check the web site regularly.

XII. COMMUNICATIONS:

Communications regarding this solicitation shall be formal from the date of issue, until either a Contractor has been selected or the Procurement Department rejects all proposals. Formal communications will be directed to the procurement officer listed on this solicitation. Informal communications, including but not limited to request for information, comments or speculations regarding this solicitation to any University employee other than a Procurement Department representative may result in the offending Offeror's proposal being rejected.

XIII. CONTROLLING VERSION OF SOLICITATION:

The posted version of the solicitation and any addenda issued by Virginia Tech Procurement Services is the mandatory controlling version of the document. Any modification of/or additions to the solicitation by the Offeror shall not modify the official version of the solicitation issued by Virginia Tech Procurement Services. Such modifications or additions to the solicitation by the Offeror may be cause for rejection of the proposal; however, Virginia Tech reserves the right to decide, on a case by case basis, in its sole discretion, whether to reject such a proposal.

XIV. TERMS AND CONDITIONS:

This solicitation and any resulting contract/purchase order shall be governed by the attached terms and conditions, see Attachment A.

XV. CONTRACT ADMINISTRATION:

A. Michael Mulhare, Assistant Vice President for Emergency Management at Virginia Tech or their designee, shall be identified as the Contract Administrator and shall use all powers under the contract to enforce its faithful performance.

B. The Contract Administrator, or their designee, shall determine the amount, quantity, acceptability, fitness of all aspects of the services and shall decide all other questions in connection with the services. The Contract Administrator, or their designee, shall not have authority to approve changes in the services which alter the concept or which call for an extension of time for this contract. Any modifications made must be authorized by the Virginia Tech Procurement Department through a written amendment to the contract.

XVI. ATTACHMENTS:

Attachment A - Terms and Conditions

ATTACHMENT A

TERMS AND CONDITIONS

RFP GENERAL TERMS AND CONDITIONS

See:
https://www.procurement.vt.edu/content/dam/procurement_vt_edu/docs/terms/GTC_RFP_02182022.pdf

ADDITIONAL TERMS AND CONDITIONS

1. **ADDITIONAL GOODS AND SERVICES**: The University may acquire other goods or services that the supplier provides other than those specifically solicited. The University reserves the right, subject to mutual agreement, for the Contractor to provide additional goods and/or services under the same pricing, terms and conditions and to make modifications or enhancements to the existing goods and services. Such additional goods and services may include other products, components, accessories, subsystems, or related services newly introduced during the term of the Agreement.

2. **AUDIT**: The Contractor hereby agrees to retain all books, records, and other documents relative to this contract for five (5) years after final payment, or until audited by the Commonwealth of Virginia, whichever is sooner. Virginia Tech, its authorized agents, and/or the State auditors shall have full access and the right to examine any of said materials during said period.

3. **AVAILABILITY OF FUNDS**: It is understood and agreed between the parties herein that Virginia Tech shall be bound hereunder only to the extent of the funds available or which may hereafter become available for the purpose of this agreement.

4. **CANCELLATION OF CONTRACT**: Virginia Tech reserves the right to cancel and terminate any resulting contract, in part or in whole, without penalty, upon 60 days written notice to the Contractor. In the event the initial contract period is for more than 12 months, the resulting contract may be terminated by either party, without penalty, after the initial 12 months of the contract period upon 60 days written notice to the other party. Any contract cancellation notice shall not relieve the Contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation.

5. **CONTRACT DOCUMENTS**: The contract entered into by the parties shall consist of the Request for Proposal including all modifications thereof, the proposal submitted by the Contractor, the written results of negotiations, the Commonwealth Standard Contract Form, all of which shall be referred to collectively as the Contract Documents.

6. **IDENTIFICATION OF PROPOSAL**: Virginia Tech will only be accepting electronic submission of proposals. All submissions must be submitted to the Virginia Tech online submission portal. Upon completion you will be directed to your Submission Receipt. Virginia Tech will not confirm receipt of proposals. It is the responsibility of the offeror to make sure their proposal is delivered on time. **Attachments must be smaller than 50MB in order to be received by the University.** Proposals may **NOT** be hand delivered to the Procurement Office.

7. **NOTICES**: Any notices to be given by either party to the other pursuant to any contract resulting from this solicitation shall be in writing via email.

8. **SEVERAL LIABILITY:** Virginia Tech will be severally liable to the extent of its purchases made against any contract resulting from this solicitation. Applicable entities described herein will be severally liable to the extent of their purchases made against any contract resulting from this solicitation.

9. **CLOUD OR WEB HOSTED SOFTWARE SOLUTIONS**: For agreements involving Cloud-based Web-hosted software/applications refer to link for additional terms and conditions: http://www.ita.vt.edu/purchasing/VT_Cloud_Data_Protection_Addendum_final03102017.pdf

10. **WORK SITE DAMAGES:** Any damage to existing utilities, equipment or finished surfaces resulting from the performance of this contract shall be repaired to the Owner's satisfaction at the contractor's expense.

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
PROCUREMENT DEPARTMENT

ADDENDUM NO. 1

DATE:	July 7th, 2023
TO:	All Offerors
FROM:	Bryan Holloway, Contracting Officer
TOTAL PAGE(S):	2 page(s) (not including attachments)
SOLICITATION TITLE:	Security Operations Consultant
SOLICITATION NUMBER:	218672311

I. CLARIFICATIONS AND ADDITIONAL INFORMATION

The due date and time for this solicitation remains Wednesday, July 19th, 2023 by 3:00 PM.

II. REQUESTS FOR INFORMATION

1.) **Vendor Question:** Regarding this solicitation and the CEIA OpenGate system, can you clarify something for me? In sections 4D and 4E of the SOW, are you needing someone who is cognizant in the application and use of this system, or someone who can install, repair, breakdown the system?

Virginia Tech Response: Support deployment, operation and supervision during events

2.) **Vendor Question:** Is travel to overseas locations or to other facilities across the State / US anticipated for this role?

Virginia Tech Response: No, just travel to our main campus in Blacksburg, VA.

3.) **Vendor Question:** If travel is anticipated, is there an estimated number of days per year?

Virginia Tech Response: Travel is not anticipated

4.) **Vendor Question:** For supplies and production of material will VT allow contractors to leverage their services, or is the expectation for contractors to use commercial facilities and to bill VT? This question is related to training materials to be provided as there no number of personnel to be trained and type of training materials required.

Virginia Tech Response: All training costs should be presented in either an hourly rate format, or a cost per person format.

5.) **Vendor Question:** Is there an anticipated number of hours per year the contractor will work? Or are the hours invoiced per event?

Virginia Tech Response: Per event

6.) **Vendor Question:** Who or which department report to?

Virginia Tech Response: Virginia Tech Police Department

7.) **Vendor Question:** Can you clarify what is defined as “security infrastructure” and should this be factored into my consulting pricing?

Virginia Tech Response: One of the services that may be requested by VT is assessing currents security practices related to event management and the addition and implementation of the CEIA Open Gate system.

8.) **Vendor Question:** Would this “security infrastructure” assessment include all facets of security technology such as: Magnetometers (metal detectors), CCTV, Access Control, Intrusion, visitor management, key management etc. and would this be for multiple facilities? Also, will there be a requirement for integrating the aforementioned security technologies to allow security operations to become more centralized, efficient and productive.

Virginia Tech Response: If VT determined that additional assessment of current systems is desirable then a specific scope of work would be developed. The bidder can include its capabilities and a cost structure for these services.

RFP #218672311

Security Operations Consultant for Virginia Tech

Virginia Polytechnic Institute and State University
300 Turner Street NW
Blacksburg, Virginia 24061

828 Brooke Road
Virginia Beach, VA 23454
Virginia DCJS#: [redacted]
Email: rjohnson@rileen1.com
Tel#: (757)630-9109

Proposal Submission Date: July 19, 2023

CERTIFIED SWaM Small, Women and Minority-Owned
Supplier Diversity Strengthens the Commonwealth
by the Virginia Department of Small Business & Supplier Diversity

July 19, 2023

Mr. Bryan Holloway
Purchasing Agent
Virginia Polytechnic Institute and State University
Purchasing Department
300 Turner Street NW
Blacksburg, Virginia 24061

Subj: RILEEN Innovative Technologies, Inc. Proposal Submission in Response to Solicitation Number RFP 218672311 Titled Security Operations Consultant for Virginia Tech

Dear Mr. Holloway:

RILEEN Innovative Technologies, Inc. is pleased to submit our response to the subject matter solicitation for your review and consideration. RILEEN Innovative Technologies, Inc. is a fully licensed security consulting firm with highly qualified and certified staff. RILEEN is fully qualified to perform, deliver, and comply with all the requirements of this solicitation.

RILEEN Innovative Technologies, Inc. is excited about earning your business and is ready to go to work immediately. Once you have had the opportunity to review our proposal submission, please feel free to contact me with any questions or issues that you may have.

Sincerely,

Richard A. Johnson Sr.
President/CEO

828 Brooke Road, Virginia Beach, VA 23454
Website: www.rileen1.com
Email: rjohnson@rileen1.com Tel#: (757)6309109

Table of Contents

RILEEN references each proposal Paragraph Number to the corresponding section of the RFP by identifying the specific RFP reference in our Paragraph Title.

Introduction [RFP § VII]

1.1 Prime Offeror - RILEEN Introduction [RFP § VII]

RILEEN Innovative Technologies, Inc., a Virginia based firm, has been in business since 2000 serving Federal, State, Local Government and private industry markets specializing in security and advisory support services. RILEEN is federally certified as a VOSB (**Veteran Owned Small Business**) and as a Commonwealth of **Virginia SWAM and Micro Business certified** business. Our Founder and President holds an active FBI issued Secret Security Clearance. Our President is an active member of the Board of Directors and is the current President of the FBI Sponsored National InfraGard Program with the Norfolk, Virginia Chapter. The following presents the advantages of selecting the Rileen/Linux Team:

The unique RILEEN/LINXX Team attributes are ideally suited to the Virginia Tech Security Consulting requirements.
• We have current and **ongoing experience using CEIA Open Gate** systems for government clients, national-level amusement parks, airports, cruise lines, ports and railroads. • We have proven past performance in the planning and operation of National Special Security Events (NSSE) and Special Event Assessment Rating (SEAR) events Levels 1 through 5, as defined by the U.S. Department of Homeland Security, wherein CEIA Open Gate systems were deployed as part of the layered approach to security. • Our corporate leadership team consists of an array of FBI and DEA Senior Executives, and Special Operations Subject Matter Experts, with dynamic experience at the Policy, Strategic, Operational, and Tactical levels across governmental departments as well as Energy and Critical Infrastructure sectors. • Major events include: Super Bowls, Republican and Democrat National Conventions (RNCs/DNCs), and Presidential inaugurations - supporting strategic planning, operational readiness, tactical crisis intervention, and continual quality control and review of tactics, techniques and procedures. • Our Team has extensive past performance and is currently delivering Security and associated Training and Advisory services to the U.S. Department of State's Global Anti-Terrorism Assistance program (with courses taught around the globe); the NASA Glenn Research Center; U.S. Coast Guard, Department of Justice (DOJ), and Department of Homeland Security (DHS). • Despite our extensive past performance, we maintain a flat organizational structure which promotes immediate response, rapid decision-making and maximum efficiency. • We provide reach-back to nationally recognized scientific and technical experts in the fields of Aviation, Communications, Biometrics, as well as Chemical Biological, Radiological, Nuclear, and Explosive (CBRNE) detection.

Figure VT-1. The RILEEN/LINXX Team Discriminators

1.2 Major Subcontractor - Linxx Introduction [RFP § VII]

For this security operations effort for Virginia Tech, RILEEN has teamed with ***Linxx Global Solutions (Linxx)***, www.linxxglobal.com, a Virginia based Veteran-Owned Business, and nationally recognized provider of Training, Physical and Cyber Security solutions, in addition to providing worldwide support of security development Training, Implementation, Staffing, and Analysis programs. Linxx's primary focus is on enhancing the safety, security, resiliency, and productivity of our clients. They accomplish this through insightful analysis, innovative problem-solving, and an unwavering commitment to excellence. With a proven track record of success and highly qualified Security personnel, they have earned the trust of clients and remain dedicated to upholding the highest standards of quality, safety and integrity. Linxx provides for the security, safety, and well-being of American citizens and our foreign allies worldwide. Over the last 17 years, they have evolved into a leading provider of training, security, and cyber security to federal, state, and local agencies and the private sector.

Linxx has assembled a highly qualified team with the experience, financial stability, management structure, and technical expertise to effectively manage Security Operations for multiple Federal clients, including: the National Aeronautics and Space Administration (**NASA**), the U.S. Drug Enforcement Administration (**DEA**), and the U.S. Coast Guard (**USCG**). Linxx is currently providing Security Services contracts at multiple locations for each of these agencies. Additionally, Linxx has excellent past performance and is currently providing security and tactical training to the U.S. Navy and U.S. Department of State.

In addition, we are honored to introduce the RILEEN Team's Technical Advisor, Mr. John Canonico. As a retired Supervisory Special Agent for the FBI, Mr. Canonico spent the majority of his distinguished career with the FBI Hostage Rescue Team. His roles in this capacity placed him at the forefront of security operations for numerous National Special Security Events (NSSE), ranging from Presidential inaugurations and international summits, to **major sporting events such as the Super Bowl and Olympics**.

John's unparalleled expertise lies in strategic planning, operational readiness, and tactical crisis intervention for these high-profile events. Moreover, his continual dedication to quality control ensures a comprehensive review and refinement of tactics, techniques, and procedures. His unique skills and experience bring an invaluable perspective to our team, reinforcing our commitment to providing world-class security consultation services.

1.3 Team RILEEN/Linxx Consulting Strategy [RFP § VI A. 4 a) to e) /VII A.1 / VIII A, #1, 2 & 3]

1.3.1 Our Team's Consulting Strategy [RFP § VI A. 4 a) to e) /VII A.1 / VIII A, #1, 2 & 3]

Our Team's security consulting strategy uses a systematic approach and processes to assess, analyze, and enhance the security posture of organizations. Our Team will identify potential risks, vulnerabilities, and threats, and recommend appropriate measures to mitigate those risks and protect Virginia Tech's assets. This collaborative consulting strategy enables Our Team to seamlessly integrate with the Virginia Tech Police Department and host security personnel to:

Our Team is composed of ASIS CPPs (Certified Protection Professionals) who use a layered security approach methodology to produce client-approved threat scenarios (in other words, The Team does not act unilaterally – we continuously engage with the client as a paramount factor to achieve successful outcomes). Our process considers asset criticality, vulnerability, probability of occurrence, existing countermeasures, and impact to Virginia Tech (economic, reputation, compliance, among others.). The Team has outstanding proven past performance using this risk management process to evaluate current security postures and procedures, identify any security gaps, and, make recommendations to enhance complimentary security countermeasures to reduce the risk of occurrence and impact of the client-approved scenarios.

The advantage of our Team's consulting strategy is that if offers Virginia Tech an unbiased, professional, and thorough understanding of its security posture, and furthermore, if security gaps are identified, we will provide recommendations to minimize risks so that Virginia Tech can be best positioned to protect its assets – namely the students, staff and the tens of thousands of fans who visit Lane Stadium on . Our Team's strategy and approach will also help to reduce risk to Virginia Tech on a continual and ongoing basis every day.

The following provides additional details of our consulting strategy in 4 phases, namely (1) Initial Assessment, (2) Game Day Oversight, (3) Ensuring Appropriate VT Resources, and (4) Compiling Security Operations Data.

1.3.1.1 Providing an Initial Assessment [RFP VI. A.4 a)]

As part of our initial assessment process, it is noteworthy to introduce our initial core team who will be dedicated to Security Operations Consulting to Virginia Tech. The team is composed of Principal Manager Mr. Richard Johnson, President of RILEEN, Project Manager Mr. Richard Dobrich, and Technical Advisor Mr. John Canonico – we are prepared to augment the team with our highly qualified staff as requirements dictate. We are prepared to conduct a full spectrum vulnerability assessment within any scope defined by Virginia Tech. This includes the Virginia Tech main campus, including all athletic venues, and any other areas of interest. Cost structures are cited in **2.0 Detailed Pricing Plan [RFP § VI. B / VII A.2 / VIII #4]** and will refined to a higher detail based on our evaluation of our initial assessment. The initial assessment is our critical phase of the security consulting methodoly and Our Team is highly qualified to deliver an industry-best product. Our initial assessment involves the gathering of Virginia Tech (and Virginia Tech Police Department and security personnel) data to include current intelligence threat estimates or actual threats, review of previous risk/vulnerability assessments, review of security standing orders and standard operating procedures, interview of Virginia Tech Police Department and security personnel, clearly understanding the security goals, penetration testing, and review of existing security controls. Our Team is fully cognizant, capable, and ready to oversee the utilization of the CEIA Open Gate system in order to enhance the security readiness and posture of Virginia Tech.

Our Team also recognizes the critical role that major sporting events play in the Virginia Tech community. Therefore, we approach the initial assessment of the university's existing security infrastructure, policies, and procedures with particular emphasis on optimizing security for these events. Here's how we would proceed:

A. **Stakeholder Engagement:** We would start by holding in-depth discussions with key stakeholders at Virginia Tech, including university leadership, athletics department personnel, campus security heads, and others who play a role in organizing and securing major sporting events. This dialogue would help us understand the specific challenges and requirements associated with these events, and provide us with valuable context for our assessment.
B. **Site Visits and Infrastructure Evaluation:** Next, we would conduct site visits at Virginia Tech's athletic venues, such as Lane Stadium and Cassell Coliseum. Our experts would closely examine the existing physical security measures, including entry and exit controls, barriers, surveillance systems, and lighting. We would assess these features in the context of large-scale sporting events, considering factors such as crowd flow, visitor safety, and emergency evacuation protocols.
C. **Policy and Procedure Review:** We would then thoroughly review Virginia Tech's existing security policies and procedures, particularly those relating to major sporting events. This includes examining protocols for ticketing and access control, crowd management, emergency response, incident reporting, and staff training. We aim to ensure these procedures align with best practices for securing large-scale events and can effectively handle the unique dynamics of major sporting events.
D. **Digital Systems and Data Security Evaluation:** Our evaluation would also extend to the digital systems in place, particularly those used during major sporting events. We would assess the security of ticketing

1.3.1.1 Providing an Initial Assessment [RFP VI. A.4 a)] [Continued]

systems, network security measures at venues, data protection protocols for personal information of attendees, and the effectiveness of cybersecurity measures in place.

E. **Compliance Audit:** We realize that compliance with regulatory standards and industry best practices is paramount, especially for high-profile events that attract large crowds. Our team would conduct a thorough audit of Virginia Tech's game day security operations, ensuring compliance with all relevant standards and identifying areas for improvement.
F. **Risk and Threat Assessment:** We would conduct a specific risk and threat assessment for major sporting events, analyzing past incident reports, local and national crime statistics, and potential threats unique to Virginia Tech's context and high-profile athletic events. This assessment would help us identify potential vulnerabilities and inform our recommendations.
G. **Reporting and Recommendations:** Upon completion of our evaluation, we would compile a comprehensive report outlining our findings. This report would highlight strengths, potential areas of risk, and recommendations for enhancing security infrastructure, policies, and procedures specifically for Virginia Tech's major sporting events.

Our Team's approach to assessing Virginia Tech's existing security operations is holistic, rigorous, and tailored to meet the specific needs and context of the university, with particular emphasis on the challenges and requirements of securing major sporting events. Our goal is to provide practical, effective recommendations that enhance security and ensure the safety and enjoyment of all attendees.

1.3.1.2 Providing Oversight during Game Day Operations [RFP VI. A.4 b)]

The RILEEN/LINXX Team is well-versed in operating the CEIA Open Gate system, as well as other products in that category, used in a high-volume environment. We have current and ongoing **experience using CEIA Open Gate systems for government clients, national-level amusement parks, airports, cruise lines, ports and railroads.** Additionally, The Team has past performance in the planning and operation of National Special Security Events (NSSE) and Special Event Assessment Rating (SEAR) events Levels 1 through 5, as defined by the U.S. Department of Homeland Security, wherein CEIA Open Gate systems were deployed as part of the layered approach to security. The Team has advanced training, an abundance of experience, and, a concierge approach to security delivery that emphasizes positive customer engagement with impeccable standards for respect and kindness while ensuring that security functions are expertly conducted according to the client's requirements.

1.3.1.2 Providing Oversight during Game Day Operations [RFP VI. A.4 b)] [Continued]

As security consultants to Virginia Tech, The Team applies a robust, multi-faceted approach to oversee game day operations, ensuring that security protocols are implemented effectively and efficiently. We do not inappropriately directly manage the operations but provide strategic guidance, technical advice, and analytical expertise. This methodology combines proactive planning, real-time advisory, post-event analysis, and ongoing refinement of strategies. The following provides the systematic steps involved in our process:

A. **Strategic Planning Guidance:** Leveraging our collective experience with high-stakes events, we provide comprehensive guidance during the planning phase for each game. This includes recommending best practices for anticipated threats, crowd management strategies, and overall security operations based on Virginia Tech's specific circumstances. We will use our expertise to advise Virginia Tech's security team on their roles and responsibilities, fostering clarity and confidence ahead of the game day.
B. **Real-time Advisory:** Utilizing Virginia Tech's surveillance tools and data feeds, including AI-assisted technology, facial recognition systems, and drone surveillance, we can provide real-time strategic advice during games. We assess and interpret the incoming data and, when needed, provide prompt advice on how to address emerging issues, ranging from unauthorized access attempts to crowd management challenges.
C. **Rapid Response Consulting:** In the event of a security incident, our team is well-positioned to provide immediate, effective guidance. Our background in large-scale, high-pressure events has honed our ability to make swift, informed recommendations. We will work in coordination with Virginia Tech's security personnel, local law enforcement, and emergency services, providing strategic advice to help manage the situation effectively.
D. **Ongoing Feedback:** During the game, we maintain open channels of communication with Virginia Tech's security personnel, offering regular check-ins and feedback. This approach facilitates real-time advisory, enabling us to suggest adjustments to the operational strategies as the dynamics of the event evolve.
E. **Post-event Analysis:** After each game, we conduct a detailed review of the event's operations, examining incident reports, surveillance data, crowd management records, and more. We use this data to identify operational strengths, potential vulnerabilities, and areas for improvement. Our findings will be the basis for our recommendations for refining security strategies for future games.
F. **Compliance Reviews:** Our team will ensure Virginia Tech's security operations remain compliant with all relevant regulations and adhere to industry best practices. We conduct regular audits of the game day operations and provide guidance on maintaining and enhancing compliance standards.
G. **Stakeholder Communication:** As consultants, we prioritize clear, concise communication with all key stakeholders at Virginia Tech. We will offer updates on security preparations, real-time advisory, post-event analysis, and any significant incidents. Our open dialogue ensures all parties are well-informed and confident in the overall security approach.

1.3.1.2 Providing Oversight during Game Day Operations [RFP VI. A.4 b)] [Continued]

While not directly managing the security operations, our Team will play an instrumental role in shaping, evaluating, and refining the security strategies for Virginia Tech's game day operations. Our objective is to ensure not only the security but also the overall success and enjoyment of every game day event at the institution.

1.3.1.3 Ensuring & Advising VT Purchased Equipment [RFP VI. A.4 c)]

The RILEEN/LINXX Team, comprised of nationally recognized experts and former senior executives experienced in managing National Special Security Events (NSSE) and Special Event Assessment Ratings (SEAR), adopts a multi-faceted approach to ensuring that Virginia Tech has all the necessary equipment and accessories for its security functions, with an emphasis on major sporting events. The following provides details of this operational and logistic analysis phase of our security consulting:

Implementing a Comprehensive Inventory Management System: The first step in our process is establishing a robust, comprehensive inventory management system. This system would catalog all existing security equipment, including detailed information about their functionalities, maintenance schedules, and expected lifespans. Regular audits would be conducted to ensure the inventory remains accurate and up-to-date, allowing us to monitor the condition of each piece of equipment. We will use a state-of-the-art software solution, chosen for its ability to automate many of these tasks and provide alerts when equipment is due for maintenance or nearing the end of its life. Our proactive approach prevents any lapses in security due to unanticipated equipment failures or shortages.

A. **Continual Professional Development and Industry Engagement:** The Team stays at the cutting edge of security technology and best practices by engaging in ongoing professional development and networking activities. These activities include participating in relevant workshops, webinars, and industry conferences, subscribing to key publications, and maintaining active memberships in top security organizations. The knowledge and insights gained from these activities allow us to stay informed about emerging technologies and trends, which we can then evaluate for potential implementation at Virginia Tech.
B. **Collaborative Relationships with Key Stakeholders:** We believe that maintaining close, collaborative relationships with key stakeholders on campus is essential to understanding and effectively addressing Virginia Tech's specific security needs. Regular meetings with the athletics department, emergency management team, and other relevant groups will be scheduled to discuss upcoming events, potential security challenges, and equipment needs. Furthermore, we will foster relationships with local law enforcement and emergency services to gain a broader perspective on security in the surrounding community. These relationships will inform our understanding of the unique challenges and security requirements of each venue and event.
C. **Recommendations Based on Expert Analysis:** Drawing from our wealth of experience in managing security for large-scale events, The Team will apply our experience and knowledge to provide insightful recommendations for additional or upgraded equipment that Virginia Tech may need. As an example, if our assessment identifies a need for an additional enhanced, proactive approach to threat detection and

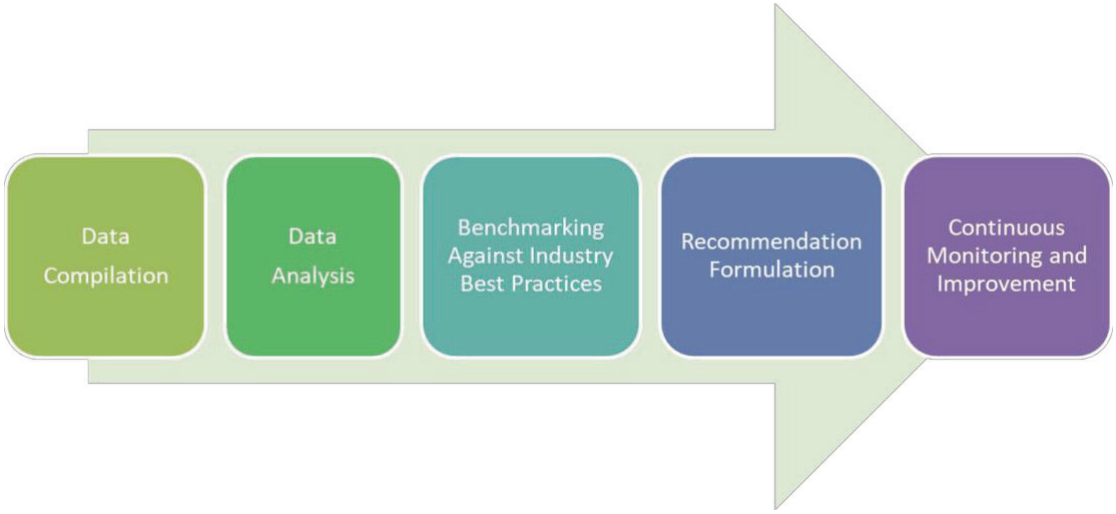
1.3.1.3 Ensuring & Advising VT Purchased Equipment [RFP VI. A.4 c)] [Continued]

management, we may recommend the integration of AI-assisted technology coupled with facial recognition systems. These advanced tools, besides identifying potential threats early by cross-referencing a database of known individuals of interest, also provide evidentiary quality data that can prove invaluable in post-event analyses and potential legal proceedings, thus enhancing the overall security apparatus. Furthermore, if we recognize that certain areas of a venue are challenging to monitor due to their size or layout, our team could recommend the implementation of drone technology. Drones, equipped with high-definition cameras and sensors, not only offer real-time aerial surveillance and expand coverage, but also capture high-quality visual evidence that could be vital in assessing incidents. This approach significantly improves situational awareness and contributes to the overall safety and security of attendees at large events.

D. **Ongoing Evaluation and Continuous Improvement:** Finally, our team believes in the power of ongoing evaluation and continuous improvement. After each event, we will conduct a thorough review of security operations, gathering feedback from all stakeholders and evaluating the performance of our equipment and strategies. Our reviews will help us identify any areas of improvement and adjust our approach as needed, ensuring that Virginia Tech's security operations continually evolve to meet changing needs and circumstances.

In summary, the RILEEN/LINXX Team's unique combination of deep industry expertise, collaborative approach, and commitment to continuous improvement puts us in a strong position to ensure Virginia Tech is fully equipped to meet its security needs, particularly during major sporting events. We are committed to providing the most effective and cost-efficient security solutions, guaranteeing the safety and enjoyment of all event attendees.

1.3.1.4 Compiling Security Operations Data [RFP VI. A.4 d)]



1.3.1.4 Compiling Security Operations Data [RFP VI. A.4 d)] [Continued]

The Team employs a methodical, data-driven approach to security operations, incorporating state-of-the-art technology, industry best practices, and our extensive expertise to compile, analyze, and provide actionable recommendations based on security operations data. The following describes our data collection and analysis process:

A. **Data Compilation**: The first phase in our process involves capitalizing on Virginia Tech's existing data acquisition tools to assemble a comprehensive collection of relevant security data. Virginia Tech's existing technology infrastructure, which might include AI-enabled surveillance systems, crowd monitoring tools, incident reporting software, and access control systems, can provide invaluable real-time and historical data. These tools are especially effective during high-profile events, such as football games, where the demand for security and crowd management is particularly high. By closely collaborating with Virginia Tech's IT department and other relevant staff, we will effectively extract and utilize this data to inform our security strategies.

B. **Data Analysis**: With the collected data, we will then conduct a rigorous analysis using advanced analytics software. This phase is aimed at revealing trends, patterns, and potential vulnerabilities that might not be immediately apparent. Focusing on key performance indicators, like incident rates, response times, crowd behavior patterns during football games, and equipment efficiency, we will derive meaningful insights. We will ensure our analyses align with Virginia Tech's specific goals, needs, and concerns, providing valuable context to our findings.

C. **Benchmarking Against Industry Best Practices**: With our team's considerable experience in managing National Special Security Events (NSSE) and other national-level events, we are intimately familiar with industry best practices and compliance standards. These standards will be used as benchmarks to evaluate Virginia Tech's current security operations, including specific aspects of football game day operations. The comparison between our data-driven insights and industry best practices will highlight areas where Virginia Tech is succeeding and areas where enhancements could be beneficial.

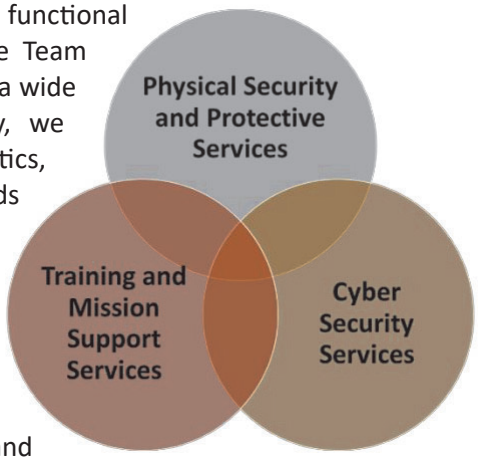
D. **Recommendation Formulation**: After our detailed analysis and benchmarking, we will then formulate detailed, data-informed recommendations. These recommendations could range from suggesting equipment upgrades to enhance stadium security, proposing procedural changes to streamline access control on game days, or initiating new training programs to better prepare security personnel for high-pressure situations. All our recommendations will be rooted in our data findings and aligned with industry best practices and compliance standards.

E. **Continuous Monitoring and Improvement**: Our commitment to Virginia Tech's security extends beyond simply making recommendations. We believe in the philosophy of continuous improvement. Once our recommended changes are implemented, we will maintain robust monitoring processes, persistently gathering and analyzing data to evaluate the impact of these changes, particularly during high-attendance football games. This ongoing process allows us to fine-tune our strategies, adapt to evolving security trends, and consistently optimize Virginia Tech's security operations.

By blending cutting-edge data analytics, deep industry knowledge, and a commitment to continuous improvement, the RILEEN/LINXX team is equipped to help Virginia Tech meet and exceed the highest standards of security practices and compliance. Our mission is not just to bolster Virginia Tech's security but to enhance the overall safety, efficiency, and success of every event hosted by the institution, with particular emphasis on its renowned football games.

1.4 Quality of Products/Services offered & Suitability for Intended Purpose [RFP § VIII #1]

The Team is a top-tier provider of Training, Physical and Cyber Security solutions. Our primary focus is on enhancing the safety, security, resiliency, and productivity of our clients. We accomplish this through understanding customer requirements, insightful analysis, innovative problem solving, and an unwavering commitment to excellence. With a proven track record of success, we have earned the trust of our clients and remain dedicated to upholding the highest standards of quality and integrity. Our services, which are relevant and applicable regarding the security, safety and operational mission of having a flawless and enjoyable Game Day, include:



- **Training and Mission Support Services**: By leveraging our deep functional experience gained from the Special Operations Community, The Team offers tailored strategic through tac2cal-level training programs to a wide range of government and non-governmental entities. Notably, we provide accredited training courses worldwide in counter-narcotics, anti-terrorism, small-unit tactics, and specialized skills to thousands of U.S. and allied students on an annual basis. Our proven track record serves as a testament to our unwavering dedication in delivering customized mission-support solutions that address the ever-changing needs of our clients.

- **Security Operations and Protective Services:** The Team has a well-established track record of delivering exemplary Security and Protective Services, both domestically and internationally. We offer a comprehensive range of security services; including: consulting, vulnerability assessments, training, and, direct support to both public sector and government entities. Our extensive past performance serves as a testament to our unwavering commitment to excellence, integrity, and the delivery of outstanding security solutions to our valued clients.

- **Cyber Security Services:** Internal and external cyber security threats to operational continuity, secure data management, and consistent functionality, are a real concern of businesses, organizations, and nations around the world. The Team has the experience, knowledge, and skill to address these specific challenges. We have provided cyber security solutions for the federal government and commercial businesses for over ten years.

1.5 Qualifications and Experiences [RFP § VI. A. 1, 2 & 3 / VIII #2 / VI A.4.e)]

As previously described, the RILEEN/LINXX has extensive past performance and is currently successfully delivering security and training services to include: the U.S. Department of State's Global Anti-Terrorism Assistance (GATA) program with course taught around the globe; the U.S. Navy's counter-piracy security training; the U.S. Army's International Traffic in Arms Regulations (ITAR)-sensitive inventory control;

1.5 Qualifications and Experiences [RFP § VI. A. 1, 2 & 3 / VIII #2 / VI A.4.e)] [Continued]

infrastructure security services for NASA Research Centers; U.S. Coast Guard land/maritime facilities, Department of Justice (DOJ) facilities, and Department of Homeland Security (DHS) facilities.

How we provide security operations consulting services, with an emphasis on major events and athletic venues

Our Team employs a comprehensive consultative approach that allows us to quickly target our client's specific needs, identify their challenges, implement security enhancements, monitor progress, and improve their security posture by reducing risks to assets. The following are the case descriptions associated with major events:

- **Security Consulting:** Our team firmly holds the belief that an effective security solution should be comprehensive, coordinated, and cost-effective. The journey towards achieving these objectives begins with evaluating the existing threats, challenges, client expectations, and the current physical and technical infrastructure. The task of managing security operations can be overwhelming without a solid understanding of the prevailing conditions. Such understanding comprises validated risks, budget constraints, and external pressure to conform to industry norms and national security mandates. Our team offers these insights as part of our professional security advice, delivered in the form of consulting products or as an ongoing consulting services support. A testament to our team's capability is Mr. Canonico's distinguished service history. He served as a lead planner and was part of the FBI Hostage Rescue Team (HRT) security contingency for the 2002 Olympics held in Salt Lake City, Utah. This hands-on experience in managing security for a high-profile international event underscores our team's expertise and readiness to handle security operations of any scale.

- **Security-Specific Training and Exercise Support:** Our team is known for delivering state-of-the-art nationwide and worldwide security training. While our initial focus was on maritime challenges, we have expanded our reach to include infrastructure security on both land and sea. Our services are also extensively availed by commercial enterprises and corporate facilities. We aid our clients in assessing their competency levels in the context of their unique environment and mission. A blend of training, education, and exercise support not only enhances performance but also optimizes the return on investment in security. An exemplification of our team's credentials is Mr. Canonico's extensive contribution to **numerous Republican National Committee (RNC) and Democratic National Committee** (DNC) Presidential Committees. In these roles, he served as a supervisory planner and was a critical part of the Government's crisis management response team. His experience further reinforces our team's capability to provide top-tier security consultation and training.

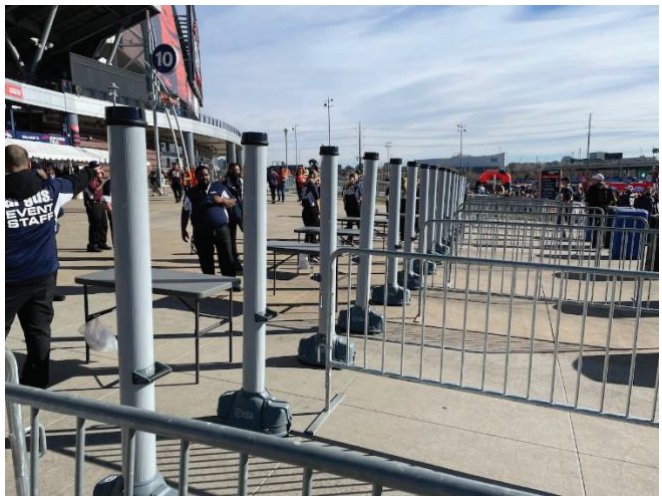
- **Security Resources Support:** The Team leverages our professional services division to gain access to top-tier security personnel. We recruit, vet, hire, and train security support personnel covering every facet of skill and knowledge. Our security management teams are handpicked leaders with exemplary track records of success. We are adept at analyzing gaps in security staffing resources, staff performance and capability, and staff leadership. We have a proven assessment process to repair and upgrade existing conditions, resulting in improved security plans and enhanced personnel capabilities. Mr. Canonico developed the

1.5 Qualifications and Experiences [RFP § VI. A. 1, 2 & 3 / VIII #2 / VI A.4.e)] [Continued]

FBI's Unconventional Law Enforcement Operations (ULEO) program which harnessed overt and discreet security protocols for all NSSE events to identify and assess threats well before established access points using a layered methodology which is still in effect today.

- **Security Focused General Contracting and Project Management:** Our clients are often best served by engaging our Team as a general contractor for security infrastructure installation and testing. We are adept at project management and believe a well-designed security risk mitigation plan deserves cost and time efficient installation and upgrade project execution. Our Team is capable of coordinating and communicating with all subcontractors and vendors in accordance with our client's detailed master security policies, practices, and procedures.

The RILEEN/LINXX team has extensive experience with security operations of major events and athletic venues including the **Super Bowl, Olympics, G20 Summits, Presidential Inaugurations, RNC/DNC Conventions**, and similar events with large crowds in attendance. The U.S. Department of Homeland Security (DHS) designates these as National Special Security Events (NSSE). DHS also oversees Special Event Assessment Ratings (SEARs) Level 1 through 5 which range for significant events with national and/or international importance that require extensive federal interagency support (**SEAR Level 1)** to events that may be nationally recognized but generally have local or state importance (**SEAR Level 5**). Technical Advisor John Canonico is a retired FBI Supervisory Special Agent who served the overwhelming majority of his career with the FBI Hostage Rescue Team. In that capacity, he was intricately involved in dozens of NSSE and SEAR events as a strategic planner, operational readiness coordinator, and tactical crisis intervention responder. Mr. Canonico led efforts for continual quality control and review of tactics, techniques, and procedures.



Demonstrated experience with the CEIA Open Gate Security Screening System

In accordance with RFP VI. A.4 e, our team brings a wealth of operational knowledge and extensive experience specific to the CEIA Open Gate system, which is an advanced, state-of-the-art metal detector system designed for high-traffic public spaces. We possess a deep understanding of its technological specifications, functionality, optimal deployment strategies, and successful utilization techniques. This understanding stems not only from rigorous training but also from proven past performance in real-world contexts.

1.5 Qualifications and Experiences [RFP § VI. A. 1, 2 & 3 / VIII #2 / VI A.4.e)] [Continued]

A prominent illustration of our expertise is the successful review, analysis, technical and operational recommendations, and budgetary provisions for the deployment of **the CEIA Open Gate system at the Virginia Department of Transportation** (VDOT) facilities (District Offices, Residencies, AHQ's, etc.) to include the aesthetics of each lobby where these units may be deployed such as VDOT's Central Office lobby and the space limitation in other lobbies. As part of this VDOT project, we coordinated with the Director of Security at Busch Gardens Williamsburg and conducted an in-depth review and assessment of the CEIA Open Gate system currently in use.

This initiative was not a stand-alone project, but rather an integral part of a **comprehensive threat reduction and visitor / employee control strategy** that we developed and implemented for VDOT after a meticulous risk assessment of the facility.

To align security measures with the specific threats and risks identified, we conducted an in-depth evaluation of the venue, focusing on visitor traffic patterns, potential security vulnerabilities, and logistical considerations. Based on this assessment, we recognized the CEIA Open Gate system as the optimal solution for enhancing the park's security apparatus without impeding visitor flow.

We then recommended the installation process, ensuring the system was optimally located and correctly integrated into the existing security infrastructure. In essence, our team's experience with the CEIA Open Gate system goes beyond mere familiarity. We possess in-depth, practical knowledge, drawn from hands-on experience in diverse contexts. We are fully prepared to bring this level of expertise to Virginia Tech, ensuring that the university's deployment and utilization of the CEIA Open Gate system is not only successful but also custom-tailored to its unique security needs and operational context.

Our team fully acknowledges and understands that we may be required to work cooperatively with Virginia Tech's existing security services provider. We recognize the significance of such partnerships in achieving shared security goals, and we are committed to fostering an environment of collaboration and respect.

In our experience, effective security consultancy requires not only expert knowledge but also strong collaboration and effective communication. We understand that Virginia Tech's existing security services provider possesses unique insights into the day-to-day security operations and challenges of the university. As such, we see this provider as a crucial partner in our work, and we look forward to a cooperative relationship where we can learn from one another, align our efforts, and collectively enhance the security posture of the university.

We are fully prepared to share our expertise, listen to their perspective, and work together to ensure that the appropriate services and procedures are in place. We firmly believe that by doing so, we can contribute to a more robust and effective security framework at Virginia Tech, ensuring the safety and well-being of all students, faculty, staff, and visitors.

1.6 Specific Plans & Methodology [RFP § VIII A. #3]

We address selected aspects of our strategy, plans and methodology in section 1.3 above. The following provides additional detail. Our team applies a systematic, evidence-based approach to provide top-tier

1.6 Specific Plans & Methodology [RFP § VIII A. #3] [Continued]

security consultancy services. This approach combines our deep industry knowledge with practical experience to create tailored solutions for each client. In the case of Virginia Tech, we would follow a multi-step methodology:

A. **Understanding the Context:** Before formulating specific plans, we immerse ourselves in understanding the unique context of Virginia Tech. This includes discussions with key stakeholders, review of existing security documents and data, and a detailed site visit. We pay particular attention to the specific challenges and requirements of the university, such as the major sporting events and high-traffic venues.

B. **Risk and Threat Assessment**: Drawing upon our understanding of Virginia Tech's unique context, we implement an all-encompassing risk and threat appraisal. Our approach includes reviewing recent incident reports, analyzing crime data at the local and national levels, and assessing potential vulnerabilities tied specifically to the university's environment. Furthermore, we evaluate any additional potential threats. This holistic assessment empowers us to pinpoint areas that demand attention and identify any shortcomings in the university's current security infrastructure and policies.

C. **Strategy Development**: Upon completion of the risk and threat assessment, we develop a customized security strategy for Virginia Tech. This strategy outlines the recommended changes or enhancements to existing security infrastructure, policies, and procedures. The strategy incorporates our expertise in cutting-edge security technologies like AI-assisted systems, facial recognition, and drone technology, and complies with industry best practices and regulatory standards.

D. **Implementation Support**: Once the strategy is approved, we provide full support in its implementation. This process includes offering advice on equipment procurement, developing training procedures for the new security measures, and working collaboratively with Virginia Tech’s existing security services provider.

E. **Continuous Evaluation and Improvemen**t: Post-implementation, we continue to monitor and evaluate the effectiveness of the new security measures. We use data-driven methods to measure performance, and we provide periodic reports to Virginia Tech’s leadership. If necessary, we refine and adjust the security strategy based on these evaluations.

Our methodology ensures that our services are not only based on best practices and expert knowledge, but also specifically tailored to the unique needs and context of Virginia Tech. We are committed to providing the university with the most effective, efficient, and suitable security solutions.

2.0 Detailed Pricing Plan [RFP § VI. B / VII A.2 / VIII #4]

In this section of our proposal, we present a comprehensive and detailed pricing plan for the consulting services, training materials, and other associated costs that will be involved in providing Virginia Tech with top-tier security consultancy. Our approach is to offer a variety of labor categories and associated skill sets, reflecting our diverse expertise and ability to provide specialized services tailored to Virginia Tech's unique needs. This strategy not only gives Virginia Tech the flexibility to scale our services up or down according to

2.0 Detailed Pricing Plan [RFP § VI. B / VII A.2 / VIII #4] [Continued]

changing requirements, but it also ensures that our pricing remains transparent, fair, and directly tied to the value we provide. All pricing related to consulting services will be submitted in a Labor/Hour format, offering

a clear and straightforward understanding of cost allocations. We are confident that this pricing model will facilitate optimal cost control, while ensuring that Virginia Tech gets the most value from our partnership.

The following tables contain our Consulting Services Labor Categories in an Hour Pricing Plan. For the purpose of this RFP, Tier 1 Labor Categories and pricings are contained in Table 1 as follows:

Table 1. Proposed Tier 1 Labor Categories and Hourly Rates

Consultant Title	Description of Services	Fully Burdened Rate
PROGRAM MANAGER	This person is responsible for overall performance of the contract. They assign project managers for specific work and performs quality control of the work and resulting documents	$150.00
PROJECT MANAGER	This person is responsible for the overall success of the project. They coordinate all the studies, analysis and staff required to fully define the security elements. This person meets with the Owner on a regular basis and monitors and maintains schedules and resources for a successful completion of the project.	$125.00
TECHNICAL ADVISOR 15 YEARS EXPERIENCE OR MORE	Extensive security leadership experience and technical expert in all aspects of risk assessments. This person should be capable or providing site assessments for all aspects of physical security. This person should be capable of developing master plans for physical security needs. This person will develop policies and provide training in the same.	$110.00
SECURITY CONSULTANT LESS THAN 15 YEARS EXPERIENCE	This person should have experience, no less than 5 years, in facility infrastructure assessments. The person should have experience is leading some physical site assessments and making recommendations. This person would conduct interviews and do most of the field work for the higher-level consultant.	$95.00
SECURITY ENGINEER/DESIGNER 15 YEARS OR MORE IN EXPERIENCE	This person shall be capable of producing the design documents and specifications required for any security system installation. This person shall be knowledgeable in local building codes. This	$110.00

Consultant Title	Description of Services	Fully Burdened Rate
	person has the ultimate responsibility for creating bidding documents for the Owner.	
SECURITY ENGINEER/DESIGNER LESS THAN 15 YEARS EXPERIENCE	This person shall provide support to the more senior level person, via CAD, field work, calculations, etc. in the production of the bidding documents. This person shall also be capable of producing smaller scale project bidding documents for the Owner.	$95.00
ADMINISTRATIVE SUPPORT	This person types specifications and reports as may be required for the project.	$50.00
CAD OPERATOR/DRAFTER	Person that puts together drawings	$60.00
ESTIMATOR	Person who put together the costs of the projects as may be applicable.	$85.00

For the purpose of sharing the breadth and scope of our team's experience and capabilities, we are including Tier 2 Labor Categories and pricings for future reference, if applicable.

Table 2. Proposed Tier 2 Labor Categories and Hourly Rates

Consultant Title	Description of Services	Hourly Rate
Structural Blast Engineer-Senior	Performs blast damage modeling, assessment, and analyses of at-grade critical infrastructure and below grade transportation tunnels. Performs blast glazing and damage analyses for building structures. Monitors the oversight of Junior-Transportation Security Structural Blast Engineer tasks.	189.06
Structural Blast Engineer-Junior	Assists with performing blast damage modeling, assessment, and analyses of at-grade critical infrastructure and below grade transportation tunnels; and assists with performing blast glazing and damage analyses for building structures.	99.45
Security Civil Engineer-Senior PE	Senior Security Civil Engineer develops, reviews, & stamps drawings, investigates utility service locations, and designs site civil plans.	173.36

Consultant Title	Description of Services	Hourly Rate
Civil Engineer-Junior PE	Under Security Civil Engineer - Senior PE guidance, a Security Civil Engineer - Junior PE reviews drawings, investigates utility service locations, and designs site civil plans.	96.04
Security Electrical Engineer-Senior	Analyzes, assesses, and designs electronic security systems, i.e., closed circuit television, access control, and intrusion detection systems and other security communication systems. Performs Quality Control and Assurance checks of security system designs, drawings, and plans.	196.03
Security Specialist	Performs risk assessments of critical infrastructure; analyzes findings, and identifies countermeasures that reduce risk. Monitors the oversight of Transportation Security Analyst tasks.	155.34
Security Analyst	Assists with critical infrastructure risk assessments; analyzes findings, and identifies countermeasures that reduce risk.	51.19
Administrative Support - Senior	Using current office technologies, prepares memoranda, reports, presentations, meeting minutes, etc. and other administrative tasks in support of project task orders and deliveries. Monitors the oversight and tasks performance of Junior-Administrative Support staff.	64.02
Security CADD Operator-Senior	Using software applications and technologies prepares technical drawings of critical infrastructure systems, sites, and elements.	108.88
Project Administrator-Senior	Responsible for capturing, analyzing, and reporting project financial data and information. Monitors the oversight of task performance of other Program Support Administrators.	113.17
Program Support Administrator	Provided program coordination as well as other security related duties including but not limited to security policy development, research, and outreach.	79.68
Program Supplies Coordinator	Assist with the high-level site-specific security access control system programming and configuration of new systems. Provide system operation training to personnel (issuance, reporting and procedural compliance).	51.56

Consultant Title	Description of Services	Hourly Rate
Project Manager - Senior	Responsible to the client for overall project, staff, and deliverable performance. Oversees project effort by direct management of scope, schedule, and budget through oversight and task performance of other Project Managers and Task Leads.	170.50
Network Technician	Experienced in security systems programming. Possess certifications in access control systems, etc.	62.40
Technical Writer-Senior	Reviews and edits technical documents and reports for compliance with acceptable client standards and requirements. Uses administrative technologies to research, investigate, and prepare technical reports and presentations for the client. Monitors the oversight and task performance of Junior-Technical Writers.	135.95
Technical Writer-Junior	Create narrative, edit narrative, organize, word process, and produce high-quality technical documentation such as security system plans, master planning documents, installation design plans, implementation plans, training plans, maintenance plans, and test plans.	54.37
Special Systems Trainer	Provide training for security solutions at specialized sites, and for specialized security access control systems.	79.70

2.0 Detailed Pricing Plan [RFP § VI. B / VII A.2 / VIII #4] [Continued]

Our team is well-equipped to provide all necessary training materials essential for operating the security equipment we recommend, such as and including the CEIA Open Gate system. Our approach to this service is strategic, ensuring that all training materials are practical, comprehensive, and tailored to the unique needs of Virginia Tech.

The cost of any training materials needed will be discussed and approved by Virginia Tech prior to the production of those materials. We believe in a transparent and collaborative approach to all aspects of our partnership, including the production and pricing of training materials.

In addition to these custom materials, our team will provide onsite training as necessary, upon request. These sessions will be led by our experts, ensuring that your staff gain in-depth operational knowledge and confidence in using the provided equipment.

2.0 Detailed Pricing Plan [RFP § VI. B / VII A.2 / VIII #4] [Continued]

Importantly, our team has an extensive network of senior subject matter experts across the technology and security industry. This reach-back capability enables us to access specialist knowledge and advice as needed, further enriching the training we provide. We also maintain a close working relationship with federal, state, and local law enforcement agencies. This relationship allows us to stay informed about the latest trends, threats, and best practices in security, which we can then incorporate into our training materials and sessions.

In summary, our team is committed to ensuring that Virginia Tech staff have the knowledge and skills necessary to operate provided equipment effectively and confidently. We will work closely with you to develop training materials and sessions that meet your specific needs, and we will provide clear, upfront pricing for these services.

3.0 Primary Contact for the University [RFP § VII A.3]

Mr. Richard Johnson, President of RILEEN, will act as the **primary contact** for Virginia Tech in relation to this proposal. With more than twenty-three years in the Security Consulting Industry, Mr. Johnson has a stellar record, having successfully completed all projects undertaken during his tenure at RILEEN. These projects have spanned a broad spectrum of specialized security skill sets, reflecting the unique needs of each client within the industry's shared foundational requirements. Understanding that every project carries its unique demands occasionally necessitates the engagement of specialized industry experts. Mr. Johnson, who holds an active FBI-issued Secret Security Clearance, is fully equipped to handle such scenarios. Furthermore, he is an active member and the current President of the Board of Directors for the FBI Sponsored National InfraGard Program with the Norfolk, Virginia Chapter.

4.0 Our Expertise, Qualifications and Experience [RFP § VII A.4]

The RILEEN/LINXX team offers a unique blend of expertise, qualifications, and experience that makes us an exceptional choice for providing security services to Virginia Tech. We are a diverse team of nationally recognized experts and former senior-level executives who have a deep understanding of the dynamics of security in high-stakes, high-traffic environments. Our team members have planned and participated in National Special Security Events (NSSE) and Special Event Assessment Ratings (SEAR), including national conventions, presidential inaugurations, G20 summits, the Olympics, the Super Bowl, the Indy 500, and more. Our Team's core competencies include:

RILEEN / Linxx Core Competencies
Design and specification development of Life Safety and Security Solutions
Design of Indoor/Outdoor Gunshot Detection & Ballistic Identification Systems

RILEEN / Linxx Core Competencies
Design & Assessment of Emergency/Crisis Mass Notification Systems
Develop Technology Refreshment Strategies & Recommendations
Develop Security and Life Safety Installation & Operational Budgets
Provide cyber and physical security organizational leadership strategic and tactical operational consultative services
Executive Protection Planning & Consulting Services
Conduct Security Vulnerability & Assessment Consulting Services
Conduct client site Threat and Hazard Identification and Risk Assessments
Conduct TSCM (Technical Surveillance Counter Measure) Surveys
Event Security Planning
Security/Emergency Response Exercise Planning & Coordination
Security or Emergency Response Plan Development
Perform Security & Safety assessments to help corporate security departments, corporate travel and safety departments, event planners, meeting organizers, and tour operators to conduct security, safety, and health survey assessments of hotels using the OSCA, HSWG, and AHLA sponsored guidelines.

4.0 Our Expertise, Qualifications and Experience [RFP § VII A.4] [Continued]

Our expertise encompasses the latest technologies in security, including AI-assisted systems, facial recognition, and drone technology, and we have extensive operational knowledge of advanced screening equipment like the CEIA Open Gate system. This experience enables us to provide informed guidance on equipment procurement, develop effective crowd flow plans, and construct rigorous security screening processes that balance safety with efficiency.

Moreover, we have proven experience in working collaboratively with existing security service providers, which we understand is an essential aspect of this role. We are committed to forming a productive partnership

4.0 Our Expertise, Qualifications and Experience [RFP § VII A.4] [Continued]

with Virginia Tech's security provider, ensuring that our services enhance and complement the existing security operations.

Lastly, our commitment to transparency and collaboration extends to all aspects of our services, including our pricing. We offer a flexible and clear pricing plan, with the aim of providing Virginia Tech with the ability to adjust our services to suit changing needs while maintaining optimal cost control.

In summary, our team combines rich industry experience with a keen understanding of the unique security challenges posed by major sporting events and large-scale venues. We are fully prepared to leverage this knowledge to enhance the safety and security of Virginia Tech.

4.1 Resume Submission [RFP § VII A.4]

RILEEN is providing abbreviated resumes for our lead project team members and Security/Safety Subject Matter Experts (SME) for Virginia Tech's considerations.

Mr. Richard A. Johnson – [redacted]

Mr. Richard Dobrich – [redacted]

4.1 Resume Submission [RFP § VII A.4] [Continued]

[redacted]

Mr. John Canonico – [redacted]

Frank Cucci – [redacted]

4.2 References [RFP § VII A.4]

Our Team is providing the following project references for further considerations:

Project 1. Virginia Department of Transportation (VDOT)
Our team has a proven track record of delivering comprehensive security solutions, notably for large organizations such as the Virginia Department of Transportation (VDOT). In that project, we conducted a broad industry review, a thorough analysis, and offered tailored security operational recommendations for a range of Weapons Detection solutions across VDOT's statewide facilities.

The scope of work took into account the unique needs of each facility, including District Offices, Residencies, AHQ's, and more. It required careful consideration of a multitude of factors including unit mobility, the non-intrusive aspect of the systems, operational use, and the aesthetic compatibility with each potential deployment site.

4.2 References [RFP § VII A.4] [Continued]

With a deep understanding of the **CEIA Open Gate system**, we provided VDOT's Agency Security Manager with a solution that not only enhanced security but also improved operational efficiency. This recommendation was derived after a meticulous risk assessment of the VDOT facilities, affirming that the system would bolster VDOT's security without negatively affecting the visitor experience.

The deliverables for this project, which included a comprehensive Report of Findings, Recommendations, Solution Specifications, and Implementation Budgetary Estimates, are applicable to the requirements set forth by Virginia Tech. Furthermore, the operational consultation offered and the training provided to personnel for the effective and sustainable use of the CEIA Open Gate system showcase our ability to ensure ongoing success post-implementation. As part of this VDOT project, we coordinating with the Director of Security at Busch Gardens Williamsburg and conducted an in-depth review and assessment of the CEIA Open Gate system currently in use.

This example vividly illustrates our team's ability to formulate a balanced security solution that aligns threat mitigation with crowd control considerations. It underscores our expertise in the successful deployment and utilization of advanced security systems like the CEIA Open Gate system, making us uniquely suited to support Virginia Tech's security needs.

Project 2. NSSE and SEAR Venues

Our team has supervised the operational planning and security coordination of numerous National Special Security Events (NSSE) and Special Event Assessment Rating (SEAR) venues including: the 2002 Olympics (NSSE), Democratic & Republican National Committee (DNC/RNC) Presidential Nomination Conventions (NSSE), Presidential Inaugurations (NSSE), and Super Bowls (SEAR Level 1). Specific to the National Football

League (NFL), our team developed and implemented the FBI's discreet security operations program to address emerging high consequence terrorist threats and worked in coordination with the NFL, and other Federal agencies, to ensure the safety, security, and resiliency of Super Bowl events. Our team specializes in a layered security approach that fuses seamless cooperation with local, state, and federal agencies to capture all available intelligence regarding credible threats and actively implement security protocols upstream of access points to target, identify, assess, and interdict potential security treats before they reach the CEIA Open Gate systems. We are experts in assisting clients in developing and refine their emergency preparedness and crisis intervention plans using their organic assets and in conjunction with first responders and supporting tactical police units.

Project 3. Commonwealth Of Virginia Norfolk State University (NSU) Security Assessment

Our team has also proven its capabilities in the field of university security consultation, exemplified by our extensive work with Norfolk State University (NSU) within the Commonwealth of Virginia. This project involved performing a comprehensive security assessment of designated university facilities, including an in-depth examination of Mass Notification Systems and the provision of strategic operational consultation.

4.2 References [RFP § VII A.4] [Continued]

Throughout the project, we meticulously evaluated the university's existing security infrastructure and identified potential areas for improvement. Our approach was comprehensive, examining all aspects of security, ranging from physical barriers to advanced technology systems like Mass Notification Systems.

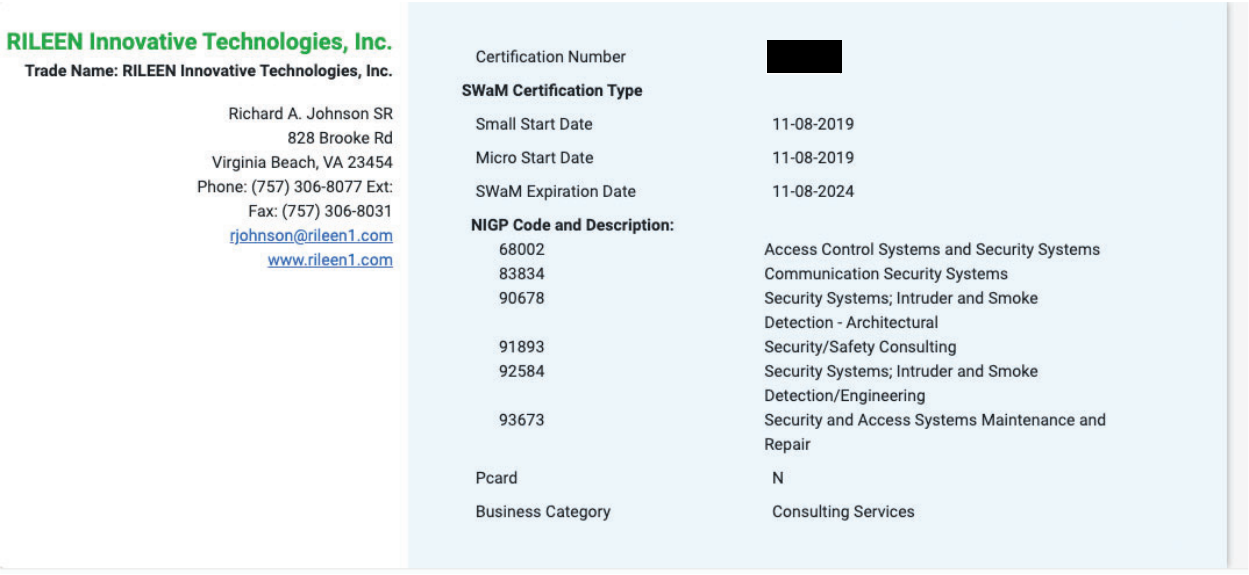
As part of our deliverables, we developed a detailed Report of Findings, provided recommendations, designed a future-oriented Technology Roadmap, outlined Solution Specifications, and devised a Phased Implementation Budgetary Estimates. Each of these components was aimed at enhancing NSU's overall security posture while ensuring the solutions proposed were aligned with the university's resources and long-term objectives.

Notably, the deliverables from our project with NSU mirror the requirements outlined in Virginia Tech's RFP. Our work with NSU, therefore, serves as a direct testament to our ability to fulfill and exceed the expectations set forth by Virginia Tech. The experience gained from working with NSU, coupled with our deep understanding of the unique security considerations associated with an educational institution, positions us well to support the multifaceted security needs of Virginia Tech.

5.0 Our SWAM Certification [RFP § VII A.5 / VIII #5]

RILEEN is a Commonwealth of Virginia Certified SWAM and Micro Business Enterprise by Virginia's DSBSD. Our certification number is: [redacted]

The following is a screen capture from the Virginia Department of Small Business & Supplier Diversity (SBSD) web site. This is provided as evidence of RILEEN's SWAM Certification.



RILEEN Innovative Technologies, Inc.
Trade Name: RILEEN Innovative Technologies, Inc.

Richard A. Johnson SR
828 Brooke Rd
Virginia Beach, VA 23454
Phone: (757) 306-8077 Ext:
Fax: (757) 306-8031
rjohnson@rileen1.com
www.rileen1.com

Certification Number	[redacted]
SWaM Certification Type	
Small Start Date	11-08-2019
Micro Start Date	11-08-2019
SWaM Expiration Date	11-08-2024
NIGP Code and Description:	
68002	Access Control Systems and Security Systems
83834	Communication Security Systems
90678	Security Systems; Intruder and Smoke Detection - Architectural
91893	Security/Safety Consulting
92584	Security Systems; Intruder and Smoke Detection/Engineering
93673	Security and Access Systems Maintenance and Repair
Pcard	N
Business Category	Consulting Services

6.0 Submission Instruction & Addenda Submission [RFP § VII A.6]

The following RFP documents that are required to be submitted with our RFP response (proposal) are contain herein as follows:

6.1 Proposal Submission Signature Page [RFP § VII A.6]

RFP # 218672311, Security Operations Consultant

INCLUDE THIS PAGE WITH YOUR PROPOSAL, SIGNATURE AT SUBMISSION IS REQUIRED

DUE DATE: Proposals will be received until Wednesday July 19th, 2023 at 3:00 PM. Failure to submit proposals to the correct location by the designated date and hour will result in disqualification.

INQUIRIES: All inquiries for information regarding this solicitation should be directed to Bryan Holloway, Phone: (540) 231- 8545 e-mail: bryanh91@vt.edu. All inquiries will be answered in the form of an addendum. Inquiries must be submitted by 12:00PM on Friday July 7th, 2023. Inquiries must be submitted to the procurement officer identified in this solicitation.

PROPOSAL SUBMISSION:

Please note, proposal submission procedures have changed effective March 2023.

Proposals may NOT be hand delivered to the Procurement Office.

Proposals should be submitted electronically through Virginia Tech's procurement portal. This portal allows you access to view business opportunities and submit bids and proposals to Virginia Tech digitally and securely.

Proposals must be submitted electronically at:
https://bids.sciquest.com/apps/Router/PublicEvent?CustomerOrg=VATech

Vendors will need to register through this procurement portal, hosted by Jaggaer. **It is encouraged for all vendors to register prior to the proposal submission deadline to avoid late submissions.** Registration is easy and free. If you have any challenges with the registration process, please contact Jaggaer Support at 1-800-233-1121 or procurement@vt.edu.

Click on the opportunity and log in to your vendor account to begin preparing your submission. Upon completion, you will receive a submission receipt email confirmation. Virginia Tech will not confirm receipt of proposals. It is the responsibility of the offeror to make sure their proposal is delivered on time.

Hard copy or email proposals will not be accepted. Late proposals will not be accepted, nor will additional time be granted to any individual Vendor.

Attachments must be smaller than 50MB in order to be received by the University.

In compliance with this Request For Proposal and to all the conditions imposed therein and hereby incorporated by reference, the undersigned offers and agrees to furnish the goods or services in accordance with the attached signed proposal and as mutually agreed upon by subsequent negotiation.

AUTHORIZED SIGNATURE: _____ Date: **July 19, 2023**

[INCLUDE THIS PAGE]

2

6.2 Addendum 1 [RFP § VII A.6]

VIRGINIA TECH

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
PROCUREMENT DEPARTMENT

ADDENDUM NO. 1

DATE:	July 7th, 2023
TO:	All Offerors
FROM:	Bryan Holloway, Contracting Officer
TOTAL PAGE(S):	2 page(s) (not including attachments)
SOLICITATION TITLE:	Security Operations Consultant
SOLICITATION NUMBER:	218672311

I. CLARIFICATIONS AND ADDITIONAL INFORMATION

The due date and time for this solicitation remains Wednesday, July 19th, 2023 by 3:00 PM.

II. REQUESTS FOR INFORMATION

1.) **Vendor Question:** Regarding this solicitation and the CEIA OpenGate system, can you clarify something for me? In sections 4D and 4E of the SOW, are you needing someone who is cognizant in the application and use of this system, or someone who can install, repair, breakdown the system?

Virginia Tech Response: Support deployment, operation and supervision during events

2.) **Vendor Question:** Is travel to overseas locations or to other facilities across the State / US anticipated for this role?

Virginia Tech Response: No, just travel to our main campus in Blacksburg, VA.

3.) **Vendor Question:** If travel is anticipated, is there an estimated number of days per year?

Virginia Tech Response: Travel is not anticipated

4.) **Vendor Question:** For supplies and production of material will VT allow contractors to leverage their services, or is the expectation for contractors to use commercial facilities and to bill VT? This question is related to training materials to be provided as there no number of personnel to be trained and type of training materials required.

Virginia Tech Response: All training costs should be presented in either an hourly rate format, or a cost per person format.

5.) **Vendor Question:** Is there an anticipated number of hours per year the contractor will work? Or are the hours invoiced per event?

6.2 Addendum 1 [RFP § VII A.6] [Continued]

Virginia Tech Response: Per event

6.) **Vendor Question:** Who or which department report to?

Virginia Tech Response: Virginia Tech Police Department

7.) **Vendor Question:** Can you clarify what is defined as "security infrastructure" and should this be factored into my consulting pricing?

Virginia Tech Response: One of the services that may be requested by VT is assessing currents security practices related to event management and the addition and implementation of the CEIA Open Gate system.

8.) **Vendor Question:** Would this "security infrastructure" assessment include all facets of security technology such as: Magnetometers (metal detectors), CCTV, Access Control, Intrusion, visitor management, key management etc. and would this be for multiple facilities? Also, will there be a requirement for integrating the aforementioned security technologies to allow security operations to become more centralized, efficient and productive.

Virginia Tech Response: If VT determined that additional assessment of current systems is desirable then a specific scope of work would be developed. The bidder can include its capabilities and a cost structure for these services.

RFP 218672311 Summary of Negotiations

1. **Virginia Tech Question:** As part of Virginia Tech standard procedures, all awarded contracts will be publicly posted on an online contracts portal. Is there any information included that would be used to identify or harm a person's identity, finances or personal information? If so, please provide a redacted copy of your proposal.

   Vendor Response: There is not any information included that would be used to identify or harm a person's identity, finances, or personal information.

2. **Virginia Tech Question:** Are there any additional financial or value-added incentives you would like to offer at this time?

   Vendor Response: RILEEN offers a 5% (five percent) prompt payment discount if invoices are paid within 30 (thirty) days of submission.

3. **Virginia Tech Question:** Are there any additional forms or documents that you will require to be incorporated into the contract documents? If so, please submit.

   Vendor Response: There are not any additional forms or documents that RILEEN will require to be incorporated into the contract documents.

4. **Virginia Tech Question:** Does Rileen Innovative Technologies, Inc. agree to provide monthly invoices with payment due thirty (30) days after receipt of invoice or goods/services, whichever is later?

   Vendor Response: RILEEN Innovative Technologies, Inc. agrees to provide monthly invoices with payment due thirty (30) days after receipt of invoice or goods/services, whichever is later.

5. **Virginia Tech Question:** Do you agree that you will be performing services as an Independent Contractor, Company, Corporation or other business entity and are not an employee of Virginia Tech or any other Commonwealth Entity?

   Vendor Response: RILEEN agrees that RILEEN (and our subcontractors that may be used) will be performing services as an Independent Contractor, Company, Corporation, or other business entity and are not an employee of Virginia Tech or any other Commonwealth Entity.

6. **Virginia Tech Question:** Do you further agree that Virginia Tech will not withhold any income taxes from its payments to contractors nor will it provide any employment benefits to the contractor or contractor's employees?

   Vendor Response: RILEEN further agrees that Virginia Tech will not withhold any income taxes from its payments to contractors nor will it provide any employment benefits to the contractor or contractor's employees.

7. **Virginia Tech Question:** End of Contract Service Transition Expectations**:** If or when a transition of service to another provider is required (end of contract life or otherwise), the university would require the incumbent firm to cooperative fully in a

successful transition of services. Explain any requirements your firm might have in preparing for such a transition of services. Additionally, please indicate your willingness to establish a transition plan alongside the new provider of service which may include but not be limited to sharing important data and/or existing service information via a cooperative knowledge transfer process.

Vendor Response: RILEEN does not have requirements your firm might have in preparing for such a transition of services. Additionally, RILEEN is willing to establish a transition plan alongside the new provider of service which may include but not be limited to sharing important data and/or existing service information via a cooperative knowledge transfer process.

8. **Virginia Tech Question:** How did Rileen Innovative Technologies, Inc. arrive at the figure for price adjustments? Is this a similar adjustment made to all your clients, or an industry standard?

   Vendor Response: The labor categories and related labor rates offered are aligned to a VPPA (Virginia Public Procure Act) prime contract that was issued to RILEEN by the Virginia Department of General Services for security consulting work efforts. This was an open competitive procurement.

9. **Virginia Tech Question:** Do you agree that the initial contract period shall be one year?

   Vendor Response: RILEEN agrees that the initial contract period shall be one year.

10. **Virginia Tech Question:** Upon completion of the initial contract period, does Rileen Innovative Technologies, Inc. agree that the contract may be renewed by Virginia Tech upon written agreement of both parties for four (4) one year periods, under the terms of the current contact?

    Vendor Response: RILEEN Innovative Technologies, Inc. agrees that the contract may be renewed by Virginia Tech upon written agreement of both parties for four (4) one year periods, under the terms of the current contact.

11. **Virginia Tech Question:** If awarded a contract, do you agree to limit price increases to no more than the increase in the Consumer Price Index, CPI-W, All Items category for the latest twelve (12) months for which statistics are available at the time of renewal or 3 percent, whichever is less?

    Vendor Response: RILEEN agrees to limit price increases to no more than the increase in the Consumer Price Index, CPI-W, All Items category for the latest twelve (12) months for which statistics are available at the time of renewal or 3 percent, whichever is less.

12. **Virginia Tech Question:** If awarded a contract, are you willing to hold prices firm for the initial contract period and the first renewal year?

    Vendor Response: RILEEN is willing to hold prices firm for the initial contract period and the first renewal year.

13. **Virginia Tech Question:** Will Rileen Innovative Technologies, Inc. agree to participate in the Wells One AP Control Payment System?

    Vendor Response: RILEEN Innovative Technologies, Inc. agree to participate in the Wells One AP Control Payment System.

14. **Virginia Tech Question:** Please identify the highest-level executive in your organization that is aware of this solicitation. Describe that person's commitment to assuring the highest quality service to Virginia Tech if your organization is awarded a contract.

    Vendor Response: Mr. Richard Johnson is the highest-level executive in our organization that is aware of this solicitation. As the Founder, President and CEO of RILEEN, Mr. Johnson is and always has been fully committed to assuring the highest quality service to all of our customers. RILEEN is proud of our client relations over the past 20 (Twenty) years. RILEEN has been VDOT's trusted security consultant for over 15 (Fifteen) years with total success in all projects. RILEEN offers the same commitment and dedication to Virginia Tech.

15. **Virginia Tech Question:** Please describe your quickest turn-around time if emergency services are needed.

    Vendor Response: RILEEN offers a minimum of a six-hour response to a emergency services call. If on-site emergency services are required, we can arrive within 12 (twelve) hours, weather permitting. If requested, RILEEN would provide a full-time on-site security specialist that lives local to Virginia Tech.

16. **Virginia Tech Question:** Are you willing to contact departments on a monthly basis to address service issues?

    Vendor Response: RILEEN is willing to contact departments on a monthly basis to address service issues.

17. **Virginia Tech Question:** Will you be able to handle increased volumes of business and/or provide service to additional departments during the course of the contract?

    Vendor Response: RILEEN will be able to handle increased volumes of business and/or provide service to additional departments during the course of the contract.

18. **Virginia Tech Question:** Please provide your best schedule of prices for all services offered.

    Vendor Response: RILEEN offers a comprehensive and detailed pricing plan for the consulting services, training materials, and other associated costs that will be involved in providing Virginia Tech with top-tier security consultancy. Our approach is to offer a variety of labor categories and associated skill sets, reflecting our diverse expertise and ability to provide specialized

services tailored to Virginia Tech's unique needs. This strategy not only gives Virginia Tech the flexibility to scale our services up or down according to changing requirements, but it also ensures that our pricing remains transparent, fair, and directly tied to the value we provide. All pricing related to consulting services will be submitted in a Labor/Hour format, offering a clear and straightforward understanding of cost allocations. We are confident that this pricing model will facilitate optimal cost control, while ensuring that Virginia Tech gets the most value from our partnership.
The following tables contain our Consulting Services Labor Categories in an Hour Pricing Plan. Our offered Tier 1 Labor Categories and pricings are contained in Table 1 as follows:

Consultant Title	Description of Services	Fully Burdened Rate
PROGRAM MANAGER	This person is responsible for overall performance of the contract. They assign project managers for specific work and performs quality control of the work and resulting documents	$150.00
PROJECT MANAGER	This person is responsible for the overall success of the project. They coordinate all the studies, analysis and staff required to fully define the security elements. This person meets with the Owner on a regular basis and monitors and maintains schedules and resources for a successful completion of the project.	$125.00
TECHNICAL ADVISOR 15 YEARS EXPERIENCE OR MORE	Extensive security leadership experience and technical expert in all aspects of risk assessments. This person should be capable or providing site assessments for all aspects of physical security. This person should be capable of developing master plans for physical security needs. This person will develop policies and provide training in the same.	$110.00
SECURITY CONSULTANT LESS THAN 15 YEARS EXPERIENCE	This person should have experience, no less than 5 years, in facility infrastructure assessments. The person should have experience is leading some physical site assessments and making recommendations. This person would conduct interviews and do most of the field work for the higher-level consultant.	$95.00
SECURITY ENGINEER/DESIGNER 15 YEARS OR MORE IN EXPERIENCE	This person shall be capable of producing the design documents and specifications required for any security system installation. This person shall be knowledgeable in local building codes. This person has the ultimate responsibility for creating bidding documents for the Owner.	$110.00
SECURITY ENGINEER/DESIGNER LESS THAN 15 YEARS EXPERIENCE	This person shall provide support to the more senior level person, via CAD, field work, calculations, etc. in the production of the bidding documents. This person shall also be capable of producing smaller scale project bidding documents for the Owner.	$95.00
ADMINISTRATIVE SUPPORT	This person types specifications and reports as may be required for the project.	$50.00
CAD OPERATOR/DRAFTER	Person that puts together drawings	$60.00
ESTIMATOR	Person who put together the costs of the projects as may be applicable.	$85.00

For the purpose of sharing the breadth and scope of our team's experience and capabilities, we are including Tier 2 Labor Categories and pricings for future reference, if applicable.

Consultant Title	Description of Services	Hourly Rate
Structural Blast Engineer-Senior	Performs blast damage modeling, assessment, and analyses of at-grade critical infrastructure and below grade transportation tunnels. Performs blast glazing and damage analyses for building structures. Monitors the oversight of Junior-Transportation Security Structural Blast Engineer tasks.	189.06
Structural Blast Engineer-Junior	Assists with performing blast damage modeling, assessment, and analyses of at-grade critical infrastructure and below grade transportation tunnels; and assists with performing blast glazing and damage analyses for building structures.	99.45
Security Civil Engineer-Senior PE	Senior Security Civil Engineer develops, reviews, & stamps drawings, investigates utility service locations, and designs site civil plans.	173.36
Civil Engineer-Junior PE	Under Security Civil Engineer - Senior PE guidance, a Security Civil Engineer - Junior PE reviews drawings, investigates utility service locations, and designs site civil plans.	96.04
Security Electrical Engineer-Senior	Analyzes, assesses, and designs electronic security systems, i.e., closed circuit television, access control, and intrusion detection systems and other security communication systems. Performs Quality Control and Assurance checks of security system designs, drawings, and plans.	196.03
Security Specialist	Performs risk assessments of critical infrastructure; analyzes findings, and identifies countermeasures that reduce risk. Monitors the oversight of Transportation Security Analyst tasks.	155.34
Security Analyst	Assists with critical infrastructure risk assessments; analyzes findings, and identifies countermeasures that reduce risk.	51.19
Administrative Support - Senior	Using current office technologies, prepares memoranda, reports, presentations, meeting minutes, etc. and other administrative tasks in support of project task orders and deliveries. Monitors the oversight and tasks performance of Junior-Administrative Support staff.	64.02

Consultant Title	Description of Services	Hourly Rate
Security CADD Operator-Senior	Using software applications and technologies prepares technical drawings of critical infrastructure systems, sites, and elements.	108.88
Project Administrator-Senior	Responsible for capturing, analyzing, and reporting project financial data and information. Monitors the oversight of task performance of other Program Support Administrators.	113.17
Program Support Administrator	Provided program coordination as well as other security related duties including but not limited to security policy development, research, and outreach.	79.68
Program Supplies Coordinator	Assist with the high-level site-specific security access control system programming and configuration of new systems. Provide system operation training to personnel (issuance, reporting and procedural compliance).	51.56
Project Manager - Senior	Responsible to the client for overall project, staff, and deliverable performance. Oversees project effort by direct management of scope, schedule, and budget through oversight and task performance of other Project Managers and Task Leads.	170.50
Network Technician	Experienced in security systems programming. Possess certifications in access control systems, etc.	62.40
Technical Writer-Senior	Reviews and edits technical documents and reports for compliance with acceptable client standards and requirements. Uses administrative technologies to research, investigate, and prepare technical reports and presentations for the client. Monitors the oversight and task performance of Junior-Technical Writers.	135.95
Technical Writer-Junior	Create narrative, edit narrative, organize, word process, and produce high-quality technical documentation such as security system plans, master planning documents, installation design plans, implementation plans, training plans, maintenance plans, and test plans.	54.37
Special Systems Trainer	Provide training for security solutions at specialized sites, and for specialized security access control systems.	79.70

19. **Virginia Tech Question:** If awarded a contract, will you agree to work with each user department before you begin to provide service so that issues such as pick-up/delivery times and days and service requirements may be addressed?

    Vendor Response: RILEEN agrees to work with each user department before you begin to provide service so that issues such as pick-up/delivery times and days and service requirements may be addressed.

20. **Virginia Tech Question:** How soon after contract award can you begin providing services?

    Vendor Response: RILEEN can begin providing our services 7 (seven) days after contract award.

21. **Virginia Tech Question:** Are you registered with and willing to participate in the eVA internet procurement solution described in the terms and conditions of the RFP?

    Vendor Response: RILEEN is registered with and willing to participate in the eVA internet procurement solution described in the terms and conditions of the RFP.

22. **Virginia Tech Question:** Do you acknowledge, agree and understand that Virginia Tech cannot guarantee a minimum amount of business if a contract is awarded to your company?

    Vendor Response: RILEEN acknowledges, agrees and understands that Virginia Tech cannot guarantee a minimum amount of business if a contract is awarded to your company.

23. **Virginia Tech Question:** Are the prices for all goods/services listed in your proposal inclusive of all applicable eVA system transaction fees?

    Vendor Response: The prices for all goods/services listed in our proposal is inclusive of all applicable eVA system transaction fees.

24. **Virginia Tech Question:** Are you willing to rescind your Standard Terms and Conditions of Sale?

    Vendor Response: Yes

25. **Virginia Tech Question:** Does the vendor acknowledge, agree, and understand that the terms and conditions of the RFP # 218672311 shall govern the contract if a contract is awarded to your company?

    Vendor Response: RILEEN acknowledges, agrees, and understands that the terms and conditions of the RFP # 218672311 shall govern the contract if a contract is awarded to RILEEN.

26. **Virginia Tech Question:** Please submit a revised quotation to incorporate any changes resulting from these negotiations.

Vendor Response: Please see our response to question number 18 (eighteen) of this document for our quotation. No other revisions are needed by RILEEN.

27. **Virginia Tech Question:** Do you agree to become a certified SWaM vendor with the Virginia Department of Small Business and Supplier Diversity and maintain that certification throughout the term of this contract?

    Vendor Response: RILEEN is currently and has been a Commonwealth of Virginia Certified SWAM and Micro Business Enterprise by Virginia's DSBSD (Department of Small Business & Supplier Diversity). Our certification number is: [redacted]. RILEEN will maintain that certification throughout the term of this contract.

28. **Virginia Tech Question:** Virginia Tech's Communication Network Services Department (CNS) network utilizes the entire frequency range allocated to the Industrial, Scientific, and Medical (ISM) band, 2.4 to 2.4835 GHz. Does vendor agree that there will be no conflicts with the existing CNS wireless 802.11g network at (dept)? (Always consult CNS to approve wording).

    Vendor Response: RILEEN agrees that there will be no conflicts with the existing CNS wireless 802.11g network related to our services offered.

29. **Virginia Tech Question:** For purposes of interacting with HokieMart, please identify the person (name, phone number, email address, etc.) in your company that will serve as liaison for a) e-commerce, b) accounts receivable, c) emergency orders.

    Vendor Response: The person, for purposes of interacting with HokieMart, is Mr. Richard Johnson, 757-630-9109, rjohnson@rileen1.com. Mr. Johnson will serve as liaison for a) e-commerce, b) accounts receivable, c) emergency orders.

30. **Virginia Tech Question:** Cost to the University is a significant component of this solicitation and one of the 5 factors considered during the award process. With this in mind, please submit a detailed cost proposal for the pricing scenario listed below:

    Virginia Tech is hosting Clemson University for a football game in Lane Stadium on a Saturday in September with kickoff at 3:31PM. VT is expecting 66,312 people to enter the stadium including fans, staff, players/teams, officials, media, etc. VT will use Gates 1, 1S, and 2-7 for the game while, Gate 8 will remain closed (only available for evacuation). Assume a greater distribution of fans at Gates 3, 6, and 7 with an appropriate ratio of magnetometers deployed at each. VT will deploy magnetometers at each of the gates being used for the game at least 8 hours prior to kickoff. Gates will open at 1:30PM, two-hours prior to kickoff. The majority of fans will attempt to enter the stadium between 2:30PM and 3:15PM. VT will leverage an existing contract for staffing security, ticket scanning, and guest services at each gate. Assume the game lasts until 7:30PM with the last people clearing the stadium at 8:30PM. Please describe the approach, cost, and any other relevant details to supporting the management of magnetometers prior to, during, and after the event.

Vendor Response:

RILEEN is submitting our response to this question with best efforts considering some unknowns such as:

- **Stadium perimeter configurations, use of the OpenGate solution versus conventional metal detectors**
- **Past acts of violence**
- **Past criminal activity that may have occurred in the past**
- **Is there threat intel or historical data that should be factored into our approach (what are we trying to stop)?**
- **What are the current emergency protocols and evac plan?**
- **Will there be any other state or federal LEO's on-site? and**
- **Communications Plan (internal and external). What's the current event comm plan? Can we use VaTech radios, or do we need to provide our own?**

For purposes of responding to this question, we are making the following general assumptions:

- **The existing VaTech security staff are operationally proficient in the use of existing metal detectors to include hand wands when conducting bag searching techniques when needed**
- **VaTech metal detectors will be used as a backup to the use of weapons detection systems**
- **The VaTech security staff have been adequately trained on the operational use of the OpenGate weapons detection system prior to game day**
- **VaTech will have additional weapons detection OpenGate batteries available for use on game day, and**
- **If this game will be the first time that the weapons detection OpenGate system(s) will be used, VaTech will make arrangements for a manufacturer representative to be on-site to deal with any equipment issues that may arise.**

Any of these unknowns or assumptions could modify our submitted support strategy to this scenario.

General Note:

RILEEN feels that is worth noting that the RFP focused on the use of the OpenGate weapons detection solution. Our assumption in submitting our response is that use of the term, magnetometer, refers to the additional use of the OpenGate solution. The operational strategy for the OpenGate solution is significantly different than that of a magnetometer (metal detector).

For clarity, we offer the following operational / technology differences between weapon detection systems and those of metal detectors (magnetometers).

In summary, while metal detectors primarily focus on identifying metallic objects, weapon detectors go beyond metal detection by incorporating advanced technologies (such as milliwave) to detect both metallic and non-metallic threats. Weapon detectors offer enhanced precision, accuracy, and adaptability, making them ideal for environments that require comprehensive security measures. It's crucial to assess the specific needs and risks of the environment when selecting the appropriate security solution. Whether it's airports, educational institutions, or government facilities, understanding the distinctions between metal detectors and weapon detectors helps in making informed decisions to ensure the safety and well-being of individuals in various settings.

Our Proposed Strategy:

Given the above-mentioned unknowns and assumptions (as of this response), we offer the following strategy followed by our pricing.

- **RILEEN proposes that we will arrive on-site at VaTech two (2) days prior to game day. Pre-game activities by our on-site team will include gaining familiarity of stadium layout and configuration, discussing, and reviewing existing security protocols with VaTech Police Department and security, ticket scanning, and guest services staff.**
- **We will provide an on-site lead Security Manager / Advisor as our primary point of contact (with comms to the Command Center), accompanied by two (2) Security Advisors to support gates 1, 1S, and 2-7 (for use by fans, staff, players/teams, officials, media, etc) and two (2) Security Advisors to support gates 3, 6, and 7.**
- **Our Security Advisors will offer security consulting support to VaTech Police Department and VaTech supplied staffing such as security, ticket scanning, and guest services at each gate.**
- **Our on-site team will arrive on-site on game day at the time required to support game day gate security activities and remain on-site through the end of the game day.**
- **We propose to remain at VaTech the following post-game day to conduct a hot-wash debrief to the VaTech Police Department. Upon completion of post-game day hot-wash debrief, our team will depart VaTech.**

Our Proposed Pricing:

The following table offers our detailed breakdown of our cost to support our proposed question response. Our following pricing includes our proposed labor categories, hourly rate, number of hours, and related incidentals.

Labor Category	Hourly Rate	Number Hours	Cost
Security Manager / Advisor	$150.00	56	$8,400.00
Security Advisor	$110.00	60	$6,600.00
Security Advisor	$110.00	60	$6,600.00
Security Advisor	$110.00	60	$6,600.00
Security Advisor	$110.00	60	$6,600.00
		Total	$34,800.00

RILEEN believes that our proposed staff's level of effort to support this type of event (given the potential high target security event) is necessary to assist VaTech in providing a secure, safe and enjoyable experience to all.

31. **Virginia Tech Question:** If awarded a term contract, do you agree to participate in a post-event briefing upon the completion of each sanctioned event and provide a written after-action report at no additional cost?

Vendor Response: **If awarded a term contract, RILEEN agrees to participate in a post-event briefing upon the completion of each sanctioned event and provide a written after-action report at no additional cost.**

32. **Virginia Tech Question:** If awarded a term contract, do you agree to have all marketing materials and signage, as it pertains to security screening operations for a specific event, reviewed and approved by Virginia Tech prior to soliciting?

Vendor Response: If awarded a term contract, RILEEN agrees to have all marketing materials and signage, as it pertains to security screening operations for a specific event, reviewed and approved by Virginia Tech prior to soliciting.

33. **Virginia Tech Question:** Do you agree to these additional terms and conditions listed below?

Vendor Response: RILEEN agrees to these additional terms and conditions listed below.

11. INSURANCE:

By signing and submitting a Proposal/Bid under this solicitation, the offeror/bidder certifies that if awarded the contract, it will have the following insurance coverages at the time the work commences. Additionally, it will maintain these during the entire term of the contract and that all insurance coverages will be provided by insurance companies authorized to sell insurance in Virginia by the Virginia State Corporation Commission.

During the period of the contract, Virginia Tech reserves the right to require the contractor to furnish certificates of insurance for the coverage required.

INSURANCE COVERAGES AND LIMITS REQUIRED:

A. Worker's Compensation - Statutory requirements and benefits.
B. Employers Liability - $100,000.00
C. General Liability - $2,000,000.00 combined single limit. Virginia Tech and the Commonwealth of Virginia shall be named as an additional insured with respect to goods/services being procured. This coverage is to include Premises/Operations Liability, Products and Completed Operations Coverage, Independent Contractor's Liability, Owner's and Contractor's Protective Liability and Personal Injury Liability.
D. Automobile Liability - $500,000.00

E. The contractor agrees to be responsible for, indemnify, defend and hold harmless Virginia Tech, its officers, agents and employees from the payment of all sums of money by reason of any claim against them arising out of any and all occurrences resulting in bodily or mental injury or property damage that may happen to occur in connection with and during the performance of the contract, including but not limited to claims under the Worker's Compensation Act. The contractor agrees that it will, at all times, after the completion of the work, be responsible for, indemnify, defend and hold harmless Virginia Tech, its officers, agents and employees from all liabilities resulting from bodily or mental injury or property damage directly or indirectly arising out of the performance or nonperformance of the contract.

12. CRIMINAL CONVICTION CHECKS: All criminal conviction checks must be concluded before the Contractor's employees gaining access to the Virginia Tech Campus. Employees who have separated employment from Contractor shall undergo another background check before re-gaining access to the Virginia Tech campus. Contractor shall ensure subcontractors conduct similar background checks. All criminal conviction checks will normally include a review of the individual's records to include Social Security Number Search, Credit Report (if related to potential job duties), Criminal Records Search (any misdemeanor convictions and/or felony convictions are reported) in all states in which the employee has lived or worked over the past seven years, and the National Sex Offender Registry. In addition, the Global Watch list (maintained by the Office of Foreign Assets Control of The US Department of Treasury) should be reviewed. Virginia Tech reserves the right to audit a contractor's background check process at any time. All employees must self-disclose any criminal conviction(s) occurring while assigned to the Virginia Tech campus. Such disclosure shall be made to Contractor, which in turn shall notify the designated Virginia Tech contract administrator within 5 days. If, any time during the term of the contract, Virginia Tech discovers an employee has a conviction which raises concerns about university buildings, property, systems, or security, the contractor shall remove that employee's access to the Virginia Tech campus, unless Virginia Tech consents to such access in writing. Failure to comply with the terms of this provision may result in the termination of the contract.

a. The University has an awarded contract with a service provider for criminal conviction screening and background checks. The University prefers this vendor

be utilized by the Contractor to comply with the contractual obligations and University Policy 4060.

b. If Contractor chooses to utilize a different firm than the university's preferred provider, the Contractor's selected service provider shall be pre-approved by the Virginia Tech Police department as an acceptable service provider for criminal conviction and background checks to ensure that firm's service levels meet the requirements of University Policy 4060.

c. If a Contractor chooses to utilize a different firm than the university's preferred provider, a five-day hold will be required before placement of employees deemed by the Contractor to meet all of the requirements of the University including a clean background check. Contractor shall provide the University with the name, date of birth and the last four digits of the social security number of all individual(s) to be placed in a temporary position under this contract. The University reserves the right to conduct its own background check process during this hold period.

13. PRIME CONTRACTOR RESPONSIBILITIES: The contractor shall be responsible for completely supervising and directing the work under this contract and all subcontractors that he may utilize, using his best skill and attention. Subcontractors who perform work under this contract shall be responsible to the prime Contractor. The contractor agrees that he is as fully responsible for the acts and omissions of his subcontractors and of persons employed by them as he is for the acts and omissions of his own employees.

14. WORK SITE DAMAGES: Any damage to existing utilities, equipment or finished surfaces resulting from the performance of this contract shall be repaired to the Owner's satisfaction at the contractor's expense.

Vendor Response: RILEEN agrees.