26	**AGENDA ITEM** **ST. JOHNS COUNTY BOARD OF COUNTY COMMISSIONERS**
	Deadline for Submission - Wednesday 9 a.m. – Thirteen Days Prior to BCC Meeting

12/21/2021

BCC MEETING DATE

TO: **Hunter S. Conrad, County Administrator** **DATE:** **November 24, 2021**

FROM: **Jaime Locklear, Asst. Director Purchasing** **PHONE:** **904 209-0158**

SUBJECT OR TITLE: **RFP No. 22-06 Cyber Security Assessment**

AGENDA TYPE: **Consent Agenda, Contract, Resolution**

BACKGROUND INFORMATION:

This project includes a comprehensive cyber security assessment that provides for testing for vulnerabilities of our networks, servers, interfaces with partner entities, and other network components to determine the level of security in place and where changes must be made to ensure protection and mitigation for corruption. SJC Purchasing issued the Request for Proposals (RFP) in accordance with the SJC Purchasing Procedure Manual. Thirteen (13) proposals were responsive and forwarded to the Evaluation Committee for review.The Evaluation Committee found Illumant LLC to be the top ranked firm based upon the criteria provided in the RFP. The pricing proposal from Illumant is a not-to-exceed amount of $91,968.75 for the BOCC portion and a not to exceed amount of $30,656.25 for the Clerk of Court portion. Staff recommends Board authorization to enter negotiations with Illumant LLC, and upon successful negotiations, awarding and entering into an Agreement for performance of the services, in accordance with RFP 22-06.

1. IS FUNDING REQUIRED? Yes **2. IF YES, INDICATE IF BUDGETED.** Yes

IF FUNDING IS REQUIRED, MANDATORY OMB REVIEW IS REQUIRED:

INDICATE FUNDING SOURCE: 0012-53120 $100,000

SUGGESTED MOTION/RECOMMENDATION/ACTION:

Motion to adopt Resolution 2021-_____, authorizing the County Administrator, or his designee, to enter into negotiations with Illumant LLC under RFP No. 22-06 Cyber Security Assessment, and upon successful negotiations, award and execute a contract for the completion of the work.

For Administration Use Only:
Legal: Jalisa Ferguson 12/3/2021 **OMB: Sarah Newell 12/7/2021** **Admin: Brad Bradley 12/8/2021**

RESOLUTION NO. 2021 -_____

A RESOLUTION BY THE BOARD OF COUNTY COMMISSIONERS OF ST. JOHNS COUNTY, FLORIDA, AUTHORIZING THE COUNTY ADMINISTRATOR, OR DESIGNEE, TO ENTER INTO NEGOTIATIONS WITH ILLUMANT LLC AS THE TOP RANKED FIRM UNDER RFP NO: 22-06 CYBER SECURITY ASSESSMENT, AND UPON SUCCESSFUL NEGOTIATIONS, AWARD AND EXECUTE A CONTRACT FOR COMPLETION OF THE WORK.

RECITALS

WHEREAS, the County requires a comprehensive cyber security assessment for the St. Johns County Board of County Commissioners' local and wide area network which serves the Board of County Commissioners (BCC), St. Johns County Clerk of Courts, and the St. Johns County Sheriff's Office, as specified, in accordance with RFP No. 22-06; and

WHEREAS, through the County's formal RFP process, Illumant LLC was selected as the highest ranked firm, and it is recommended to enter into negotiations, and upon successful negotiations, enter into contract with Illumant LLC to complete the project; and

WHEREAS, the County has reviewed the terms, provisions, conditions and requirements of the proposed contract (attached hereto, an incorporated herein) and finds that entering into contract to complete the work services serves a public purpose.

WHEREAS, the contracts will be finalized after negotiations but will be in substantial conformance with the attached draft contract.

NOW, THEREFORE BE IT RESOLVED BY THE BOARD OF COUNTY COMMISSIONERS OF ST. JOHNS COUNTY, FLORIDA, as follows:

Section 1. The above Recitals are incorporated by reference into the body of this Resolution and such Recitals are adopted as finds of fact.

Section 2. The County Administrator, or designee, is hereby authorized to enter into negotiations with Illumant LLC to come to agreement over terms and conditions. In the event an agreement cannot be reached, the County Administrator, or designee, is authorized to cease negotiations and negotiate with the next successively ranked firm until an agreement can be reached, or it no longer serves the County's best interest to proceed.

Section 3. Upon successful negotiations, the County Administrator, or designee, is further authorized to execute agreements in substantially the same form and format as the attached draft on behalf of the County to provide the scope of services as specifically provided in RFP 22-06.

Section 4. To the extent that there are typographical and/or administrative errors that do not change the tone, tenor, or concept of this Resolution, then this Resolution may be revised without subsequent approval by the Board of County Commissioners.

PASSED AND ADOPTED by the Board of County Commissioners of St. Johns County, Florida, on this ____ day of _____, 2021.

BOARD OF COUNTY COMMISSIONERS OF ST. JOHNS COUNTY, FLORIDA

By: _____
Henry Dean, Chair

ATTEST: Brandon J. Patty,
Clerk of the Circuit Court & Comptroller

By: _____
Deputy Clerk

CONTRACT AGREEMENT
RFP NO: 22-06 Cyber Security Assessment
Master Contract #: _____

This Contract Agreement, ("Agreement") is made as of this _____ day of _____, 2021, ("Effective Date"), by and between **St. Johns County, FL** ("County"), a political subdivision of the State of Florida, with principal offices located at 500 San Sebastian View, St. Augustine, FL 32084, and **Illumant LLC** ("Contractor"), authorized to do business in the State of Florida, with offices located at 431 Florence Street, Suite 210, Palo Alto, CA 94301; Phone: (650) 961-5911 Email: siljak@illumant.com.

In consideration of the mutual promises contained herein, the County and the Contractor agree as follows:

ARTICLE 1 – DURATION and EXTENSION

This Agreement shall become effective upon signature by both parties, as of the Effective Date shown above, and shall remain in effect for a period of **one (1) calendar year**. This Agreement may be extended as necessary to complete the required services, upon satisfactory performance by the Contractor, mutual agreement by both parties, and the availability of funds. While this Agreement may be extended as stated in this Article, it is expressly noted that the County is under no obligation to extend this Agreement**.** It is further expressly understood that the option of extension is exercisable only by the County**,** and only upon the County's determination that the Contractor satisfactorily performed the Services noted in the Contract Documents**.**

ARTICLE 2 - ENUMERATION OF CONTRACT DOCUMENTS

The term "Contract Documents" shall include this Agreement, all Specifications and any addenda/exhibits thereto; all Specifications; this Agreement, any duly executed amendments, addenda, and/or exhibits hereto; and any and all Change Orders.

ARTICLE 3 - SERVICES

The Contractor's responsibility under this Agreement is to provide a comprehensive cyber security assessment for the St. Johns County Board of County Commissioners' local and wide area network which serves the Board of County Commissioners (BCC), St. Johns County Clerk of Courts, and the St. Johns County Sheriff's Office.

Services provided by the Contractor shall be under the general direction of St. Johns County Management Information Systems or other authorized County designee, who shall act as the County's representative throughout the duration of this Agreement.

ARTICLE 4 – SCHEDULE

The Contractor shall perform the required Services according to the schedule submitted and approved by the County. No changes to said schedule shall be made without prior written authorization from the County's representative.

ARTICLE 5 – COMPENSATION/BILLING/INVOICES

A. The County shall compensate the Contractor an amount of total amount not-to-exceed **ninety-one thousand nine hundred sixty-eight dollars and seventy-five cents ($91,968.75)**, which shall include any and all direct and indirect costs, and reimbursable expenses. The maximum amount available as compensation to Contractor under this Agreement shall not exceed the amount stated above without the County's express written approval, and amendment to this Agreement.

B. It is strictly understood that Contractor is not entitled to the above-referenced amount of compensation. Rather, Contractor's compensation is based upon Contractor's adhering to the Scope of Work, detailed in this Agreement. As such, the Contractor's compensation is dependent upon satisfactory completion and delivery of

all work product and deliverables noted in the Scope of Work, and detailed in this Agreement.

C. The Contractor shall bill the County for services satisfactorily performed, and materials satisfactorily delivered at the end of each week. The signature of the Contractor's authorized representative on the submitted invoice shall constitute the Contractor's certification to the County that:

   1. The Contractor has billed the County for all services rendered by it and any of its Contractors or sub-contractors through the date of the invoice;

   2. As of the date of the invoice, no other outstanding amounts are due from the County to the Contractor for services rendered;

   3. The reimbursable expenses, if any, have been reasonably incurred; and

   4. The amount requested is currently due and owing.

D. Though there is no billing form or format pre-approved by either the County**,** or the Contractor, bills/invoices submitted by the Contractor shall include a detailed written report of the Work accomplished in connection with the Scope of Work, and must be submitted with a Request for Payment Form 1550, as provided by the County. The County may return a bill/invoice from the Contractor, and request additional documentation/information. Under such circumstances, the timeframe for payment will be extended by the time necessary to receive a verified bill/invoice.

E. The Contractor's acceptance of the County's payment of an invoiced amount shall release the County from any claim by the Contractor, or by the Contractor's sub-contractors, for work performed but not invoiced during the time period indicated on the invoice for which payment was issued.

F. Unless otherwise notified, bills/invoices should be delivered to:

   St. Johns County Management Information Systems
   Attn: Katrina Carroll
   4455 Avenue A, Suite 103
   St. Augustine, FL 32095

G. FINAL INVOICE: In order for the County and the Contractor to reconcile/close their books and records, the Contractor shall clearly indicate "Final Invoice" on the Contractor's final bill/invoice to the County. Such indication establishes that all services have been satisfactorily performed and that all charges and costs have been invoiced to the County and that there is no further Work to be performed under this Agreement.

ARTICLE 6 – TRUTH-IN-NEGOTIATION CERTIFICATE

The signing of this Agreement by the Contractor shall act as the execution of a truth-in-negotiation certificate certifying that wage rates and other factual unit costs supporting the compensation are accurate, complete, and current as of the date of this Agreement.

The original contract price and any additions thereto shall be adjusted to exclude any significant sums by which the County determines the contract price was increased due to inaccurate, incomplete, or noncurrent wage rates and other factual unit costs. All such contract adjustments shall be made within one (1) year following the end of the Agreement.

ARTICLE 7 – ARREARS

The Contractor shall not pledge the County's credit or make it a guarantor of payment or surety for any contract, debt, obligation, judgement, lien, or any form of indebtedness. The Contractor further warrants and represents that it has no obligation or indebtedness that would impair its ability to fulfill the terms of this Agreement.

ARTICLE 8 – TERMINATION

A. This Agreement may be terminated by the County without cause upon at least thirty (30) calendar days advance written notice to the Contractor of such termination without cause.

B. This Agreement may be terminated by the County with cause upon at least seven (7) calendar days advance written notice of such termination with cause. Such written notice shall indicate the exact cause for termination.

ARTICLE 9 – NOTICE OF DEFAULT/RIGHT TO CURE

A. Should the County fail to perform (default) under the terms of this Agreement, then the Contractor shall provide written notice to the County, which such notice shall include a timeframe of no fewer than fifteen (15) business days in which to cure the default. Failure to cure the default within the timeframe provided in the notice of default (or any such amount of time as mutually agreed to by the parties in writing), shall constitute cause for termination of this Agreement.

B. Should the Contractor fail to perform (default) under the terms of this Agreement, then the County shall provide written notice to the Contractor, which such notice shall include a timeframe of no fewer than five (5) calendar days in which to cure the default. Failure to cure the default within the timeframe provided in the notice of default (or any such amount of time as mutually agreed to by the parties in writing), shall constitute cause for termination of this Agreement.

C. Consistent with other provisions in this Agreement, Contractor shall be paid for services authorized and satisfactorily performed under this Contract up to the effective date of termination.

D. Upon receipt of a notice of termination, except as otherwise directed by the County in writing, the Contractor shall:

1. Stop work on the date to the extent specified.
2. Terminate and settle all orders and subcontracts relating to the performance of the terminated work.
3. Transfer all work in process, completed work, and other material related to the terminated work to the County.
4. Continue and complete all parts of the work that have not been terminated.

ARTICLE 10 – PERSONNEL

The Contractor represents that it has, or shall secure at its own expense, all necessary personnel required to perform the Work as provided in the Contract Documents. It is expressly understood that such personnel shall not be employees of, or have any contractual relationship with the County.

All Work required hereunder shall be performed by the Contractor, or under its supervision. All personnel engaged in performing the Work shall be fully qualified and, if required, authorized or permitted under federal, state and local law to perform such Work.

Any changes or substitutions in the Contractor's key personnel must be made known to the County's representative and written approval granted by the County before said change or substitution can become effective.

The Contractor warrants that all Work shall be performed by skilled and competent personnel to the highest professional standards in the field. The Contractor is responsible for the professional quality, technical accuracy, and timely completion of all work performed hereunder, and shall correct or revise any errors or deficiencies in the Work, without additional compensation.

ARTICLE 11 – SUBCONTRACTING

The County reserves the right to approve the use of any subcontractor, or to reject the selection of a particular subcontractor, and to inspect all facilities of any subcontractors in order to determine the capability of the subcontractor to perform the Work described in the Contract Documents. The Contractor is encouraged to seek minority and women business enterprises for participation in subcontracting opportunities.

If a subcontractor fails to satisfactorily perform in accordance with the Contract Documents, and it is necessary to replace the subcontractor to complete the Work in a timely fashion, the Contractor shall promptly do so, subject to approval by the County.

The County reserves the right to disqualify any subcontractor, vendor, or material supplier based upon prior unsatisfactory performance.

ARTICLE 12 – FEDERAL AND STATE TAX

In accordance with Local, State, and Federal law, the County is exempt from the payment of Sales and Use Taxes. The County shall provide a tax exemption certificate to the Contractor upon request. The Contractor shall not be exempt from the payment of all applicable taxes in its performance under this Agreement. It is expressly understood by the County and by the Contractor that the Contractor shall not be authorized to use the County's Tax Exemption status in any manner.

The Contractor shall be solely responsible for the payment and accounting of any and all applicable taxes and/or withholdings including but not limited to Social Security payroll taxes (FICA), associated with or stemming from Contractor's performance under this Agreement.

ARTICLE 13 – AVAILABILITY OF FUNDS

The County's obligations under this Agreement are contingent upon the lawful appropriation of sufficient funds, for that purpose, by the St. Johns County Board of County Commissioners. Pursuant to the requirements of Section 129.07, Florida Statutes, payment made under this Agreement shall not exceed the amount appropriate in the County's budget for such purpose in that fiscal year. Nothing in this Agreement shall create any obligation on the part of the Board of County Commissioners to appropriate such funds for the payment of services provided under this Agreement during any given County fiscal year. Moreover, it is expressly noted that the Contractor cannot demand that the County provide any such funds in any given County Fiscal Year.

ARTICLE 14 - INSURANCE

The Contractor shall not commence work under this Agreement until he/she has obtained all insurance required under this section and such insurance has been approved by the County. All insurance policies shall be issued by companies authorized to do business under the laws of the State of Florida. The Contractor shall furnish proof of Insurance to the County prior to the commencement of operations. The Certificate(s) shall clearly indicate the Contractor has obtained insurance of the type, amount, and classification as required by contract and that no material change or cancellation of the insurance shall be effective without thirty (30) days prior written notice to the County. Certificates shall specifically include the County as Additional Insured for all lines of coverage except Workers' Compensation and Professional Liability. A copy of the endorsement must accompany the certificate. Compliance with the foregoing requirements shall not relieve the Contractor of its liability and obligations under this Agreement.

Certificate Holder Address: St. Johns County, a political subdivision of the State of Florida
500 San Sebastian View
St. Augustine, FL 32084

The Contractor shall maintain during the life of this Agreement, Comprehensive General Liability Insurance with minimum limits of $1,000,000 per occurrence, $2,000,000 aggregate to protect the Contractor from claims for damages for bodily injury, including wrongful death, as well as from claims of property damages which may arise from any operations under this Agreement, whether such operations be by the Contractor or by anyone directly employed by or contracting with the Contractor.

The Contractor shall maintain during the life of this Agreement, Comprehensive Automobile Liability Insurance with minimum limits of $300,000 combined single limit for bodily injury and property damage liability to protect the Contractor from claims for damages for bodily injury, including the ownership, use, or maintenance of owned and non-owned automobiles, including rented/hired automobiles whether such operations be by the Contractor or by anyone directly or indirectly employed by a Contractor.

The Contractor shall maintain during the life of this Agreement, adequate Workers' Compensation Insurance in at least such amounts as are required by the law for all of its employees (if three or more) per Florida Statute 440.02.

In the event of unusual circumstances, the County Administrator, or his designee, may adjust these insurance requirements.

ARTICLE 15 – EMPLOYMENT ELIGIBILITY AND MANDATORY USE OF E-VERIFY

As a condition precedent to entering into this Agreement, and in accordance with section 448.095, F.S., Contractor and its subcontractors shall register with and use the E-Verify system to verify the work authorization status of all employees hired on or after January 1, 2021.

a. Contractor shall require each of its subcontractors to provide Contractor with an affidavit stating that the subcontractor does not employ, contract with, or subcontract with an unauthorized alien. Contractor shall maintain a copy of such affidavit for the duration of this Agreement.

b. The County, Contractor, or any subcontractor who has a good faith belief that a person or entity with which it is contracting has knowingly violated section 448.09(1), F.S. or these provisions regarding employment eligibility shall terminate the contract with the person or entity.

c. The County, upon good faith belief that a subcontractor knowingly violated these provisions regarding employment eligibility, but Contractor otherwise complied, shall promptly notify Contractor and Contractor shall immediately terminate the contract with the subcontractor.

d. The County and Contractor hereby acknowledge and mutually agree that, a contract terminated pursuant to these provisions regarding employment eligibility is not a breach of contract and may not be considered as such. Any contract terminated pursuant to these provisions regarding employment eligibility may be challenged in accordance with section 448.095(2)(d), F.S.

e. Contractor acknowledges that, in the event that the County terminates this Contract for Contractor's breach of these provisions regarding employment eligibility, then Contractor may not be awarded a public contract for at least one (1) year after such termination. Contractor further acknowledges that Contractor is liable for any additional costs incurred by the County as a result of the County's termination of this Agreement for breach of these provisions regarding employment eligibility.

Contractor shall incorporate in all subcontracts made pursuant to this Agreement the provisions contained herein regarding employment eligibility.

ARTICLE 16 – INDEMNIFICATION

The Contractor shall indemnify and hold harmless the County, and its officers, and employees, from liabilities, damages, losses, and costs, including, but not limited to, reasonable attorneys' fees, to the extent caused by the negligence, recklessness, intentional/unintentional conduct or omission of the Contractor and other persons employed or utilized by the Contractor.

ARTICLE 17 – SUCCESSORS AND ASSIGNS

The County and the Contractor each binds itself and its partners, successors, executors, administrators and assigns to the other party of this Agreement and to the partners, successors, executors, administrators and assigns of such other party, in respect to all covenants of this Agreement. Except as above, neither the County nor the Contractor shall assign, sublet, convey or transfer its interest in this Agreement without the written consent of the other. Nothing herein shall be construed as creating any personal liability on the part of any officer or agent of the County, which may be a party hereto, nor shall it be construed as giving any rights or benefits hereunder to anyone other than the County and the Contractor.

ARTICLE 18 – NO THIRD PARTY BENEFICIARIES

It is expressly understood by the County, and the Contractor, and this Agreement explicitly states that no third party beneficiary status or interest is conferred to, or inferred to, any other person or entity.

ARTICLE 19 – REMEDIES

No remedy herein conferred upon any party is intended to be exclusive, or any other remedy, and each and every such remedy shall be cumulative and shall be in addition to every other remedy given hereunder or nor or hereafter existing at law or in equity or by statute or otherwise. No single or partial exercise by any party or any right, power, or remedy hereunder shall preclude any other or further exercise thereof.

In any action brought by either party for the enforcement of the obligations of the other party, the prevailing party shall be entitled to recover reasonable attorney's fees.

ARTICLE 20 – CONFLICT OF INTEREST

The Contractor represents that it presently has no interest and shall acquire no interest, either directly or indirectly, which would conflict in any manner with the performance of services required hereunder. The Contractor further represents that no person having any interest shall be employed for said performance.

The Contractor shall promptly notify the County, in writing, by certified mail, of all potential conflicts of interest for any prospective business association, interest or other circumstance, which may influence or appear to influence the Contractor’s judgment or quality of services being provided hereunder. Such written notification shall identify the prospective business association, interest or circumstance, the nature of work that the Contractor may undertake and request an opinion of the County, whether such association, interest, or circumstance constitutes a conflict of interest if entered into by the Contractor.

The County agrees to notify the Contractor of its opinion by certified mail within thirty (30) days of receipt of notification by the Contractor. If, in the opinion of the County, the prospective business association, interest or circumstance would not constitute a conflict of interest by the Contractor, the County shall so state in the notification and the Contractor shall, at his/her option enter into said association, interest or circumstance and it shall be deemed not in conflict of interest with respect to services provided to the County by the Contractor under the terms of this Agreement.

ARTICLE 21 – EXCUSABLE DELAYS

The Contractor shall not be considered in default by reason of any delay in performance if such delay arises out of causes reasonably beyond the Contractor’s control and without its fault or negligence. Such cases may include, but are not limited to: acts of God; the County's ommissive and commissive failures; natural or public health emergencies; freight embargoes; and severe weather conditions.

If delay is caused by the failure of the Contractor's subcontractor(s) to perform or make progress, and if such delay arises out of causes reasonably beyond the control of the Contractor and its subcontractor(s) and is without the fault or negligence of either of them, the Contractor shall not be deemed to be in default.

Upon the Contractor's request, the County shall consider the facts and extent of any delay in performing the work and, if the Contractor's failure to perform was without its fault or negligence, the Contract Schedule and/or any other affected provision of this Agreement shall be revised accordingly; subject to the County's right to change, terminate, or stop any or all of the Work at any time.

ARTICLE 22 – DISCLOSURE AND OWNERSHIP OF DOCUMENTS

The Contractor shall deliver to the County for approval and acceptance, and before being eligible for final payment of any amounts due, all documents and materials prepared by and for the County under this Agreement.

All written and oral information not in the public domain, or not previously known, and all information and data obtained, developed, or supplied by the County, or at its expense, shall be kept confidential by the Contractor and shall not be disclosed to any other party, directly or indirectly, without the County's prior written consent, unless required by a lawful order. All drawings, maps, sketches, and other data developed, or purchased under this Agreement, or at the County's expense, shall be and remains the County's property and may be reproduced and reused at the discretion of the County.

The County and the Contractor shall comply with the provisions of Chapter 119, Florida Statutes (Public Records Law).

All covenants, agreements, representations and warranties made herein, or otherwise made in writing by any party pursuant hereto, including but not limited to, any representations made herein relating to disclosure or ownership of documents, shall survive the execution and delivery of this Agreement and the consummation of the transactions contemplated hereby.

ARTICLE 23 – INDEPENDENT CONTRACTOR RELATIONSHIP

The Contractor is, and shall be, in the performance of all work services and activities under this Agreement, an independent Contractor, and not an employee, agent, or servant of the County. All persons engaged in any of the work or services performed pursuant to this Agreement shall at all times and in all places be subject to the Contractor's sole direction, supervision, and control.

The Contractor shall exercise control over the means and manner in which it and its employees perform the work, and in all respects the Contractor's relationship and the relationship of its employees to the County shall be that of an independent Contractor and not as employees or agents of the County. The Contractor does not have the power or authority to bind the County in any promise, agreement or representation other than specifically provided for in this Agreement.

ARTICLE 24 – CONTINGENT FEES

Pursuant to Section 287.055(6), Florida Statutes, the Contractor warrants that it has not employed or retained any company or person, other than a bona fide employee working solely for the Contractor to solicit or secure this Agreement and that it has not paid or agreed to pay any person, company, corporation, individual, or firm, other than a bona fide employee working solely for the Contractor, any fee, commission, percentage, gift, or any other consideration contingent upon or resulting from the award or making of this Agreement.

Violation of this section shall be grounds for termination of this Agreement. If this Agreement is terminated for violation of this section, the County may deduct from the contract price, or otherwise recover, the full amount of such fee, commission, percentage, gift, or other consideration.

ARTICLE 25 – ACCESS AND AUDITS

The Contractor shall maintain adequate records to justify all charges, expenses, and costs incurred in performing the work for at least three (3) years after completion of this Agreement. The County shall have access to such books, records, and documents as required in this section for the purpose of inspection or audit during normal business hours, at the County's cost, upon five (5) days written notice.

ARTICLE 26 – NONDISCRIMINATION

The Contractor warrants and represents that all of its employees are treated equally during employment without regard to race, color, religion, physical handicap, sex, age or national origin.

ARTICLE 27 – ENTIRETY OF CONTRACTUAL AGREEMENT

The County and the Contractor agree that this Agreement, signed by both parties sets forth the entire agreement between the parties, and that there are no promises or understandings other than those stated herein, or are incorporated by reference into this Agreement. None of the provisions, terms, conditions, requirements, or responsibilities noted in this Agreement may be amended, revised, deleted, altered, or otherwise changed, modified, or superseded, except by written instrument, duly executed by authorized representatives of both the County, and the Contractor.

ARTICLE 28 – ENFORCEMENT COSTS

If any legal action or other proceeding is brought for the enforcement of this Agreement, or because of an alleged dispute, breach, default or misrepresentation in connection with any provisions of this Agreement, the successful or prevailing party or parties shall be entitled to recover reasonable attorney's fees, court costs and all reasonable expenses even if not taxable as court costs (including, without limitation, all such reasonable fees, costs and expenses incident to appeals), incurred in that action or proceedings, in addition to any other relief to which such party or parties may be entitled.

ARTICLE 29 – COMPLIANCE WITH APPLICABLE LAWS

Both the County and the Contractor shall comply with any and all applicable laws, rules, regulations, orders, and policies of the County, State, and Federal Governments.

ARTICLE 30 – AUTHORITY TO PRACTICE

The Contractor hereby represents and warrants that it has and shall continue to maintain all licenses and approvals required to conduct its business, and that it shall at all times, conduct its business activities in a reputable manner.

ARTICLE 31 – SEVERABILITY

If any term or provision of this Agreement, or the application thereof to any person or circumstances shall, to any extent, be held invalid or unenforceable, the remainder of this Agreement, or the application of such items or provision, to persons or circumstances other than those as to which it is held invalid or unenforceable, shall not be affected and every other term and provision of this Agreement shall be deemed valid and enforceable to the extent permitted by law.

ARTICLE 32 – AMENDMENTS AND MODIFICATIONS

No amendments or modifications of this Agreement shall be valid unless in writing and signed by each of the parties.

The County reserves the right to make changes in the work, including alterations, reductions therein or additions thereto. Upon receipt by the Contractor of the County’s notification of a contemplated change, the Contractor shall: (1) if requested by the County, provide an estimate for the increase or decrease in cost due to the contemplated change; (2) notify the County of any estimated change in the completion date; and (3) advise the County in writing if the contemplated change shall effect the Contractor's ability to meet the completion dates or schedules of this Agreement. If the County instructs in writing, the Contractor shall suspend work on that portion of the project, pending the County's decision to proceed with the change. If the County elects to make the change, the County shall issue a Change Order for changes, or a contract change order, if the original contract is be changed or amended the Contractor shall not commence work on any such change until such written change order has been issued and signed by each of the parties.

ARTICLE 33 – FLORIDA LAW & VENUE

This Agreement shall be governed by the laws of the State of Florida. Any and all legal action necessary to enforce this Agreement shall be held in St. Johns County, Florida.

ARTICLE 34 – ARBITRATION

The County shall not be obligated to arbitrate or permit any arbitration binding on the County under any of the Contract Documents or in connection with the project in any manner whatsoever.

ARTICLE 35 – NOTICES

All notices required in this Agreement shall be sent by certified mail, return receipt requested, and if sent to the County shall be mailed to:

St. Johns County Purchasing Division
Attn: Purchasing Manager
500 San Sebastian View
St. Augustine, FL 32084

and if sent to the Contractor shall be mailed to:

Illumant LLC
Attn: Matija Siljak
431 Florence Street, Suite 210
Palo Alto, CA 94301

ARTICLE 36 – HEADINGS

The heading preceding the articles and sections herein are solely for convenience of reference and shall not constitute a part of this Agreement, or affect its meaning, construction or effect.

ARTICLE 37 – PUBLIC RECORDS

A. The cost of reproduction, access to, disclosure, non-disclosure, or exemption of records, data, documents, and/or materials, associated with this Agreement shall be subject to the applicable provisions of the Florida Public Records Law (Chapter 119, Florida Statutes), and other applicable State and Federal provisions. Access to such public records, may not be blocked, thwarted, and/or hindered by placing the public records in the possession of a third party, or an unaffiliated party.

B. In accordance with Florida law, to the extent that Contractor's performance under this Contract constitutes an act on behalf of the County, Contractor shall comply with all requirements of Florida's public records law. Specifically, if Contractor is expressly authorized, and acts on behalf of the County under this Agreement, Contractor shall:

(1) Keep and maintain public records that ordinarily and necessarily would be required by the County in order to perform the Services;

(2) Upon request from the County's custodian of public records, provide the County with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost as provided in Chapter 119, Florida Statutes, or as otherwise provided by law;

(3) Ensure that public records related to this Agreement that are exempt or confidential and exempt from public

records disclosure requirements are not disclosed except as authorized by applicable law for the duration of this Agreement and following completion of this Agreement if the Contractor does not transfer the records to the County; and

(4) Upon completion of this Agreement, transfer, at no cost, to the County all public records in possession of the Contractor or keep and maintain public records required by the County to perform the Services.

If the Contractor transfers all public records to the County upon completion of this Agreement, the Contractor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Contractor keeps and maintains public records upon completion of this Agreement, the Contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the County, upon request from the County's custodian of public records, in a format that is compatible with the County's information technology systems.

Failure by the Contractor to comply with the requirements of this section shall be grounds for immediate, unilateral termination of this Agreement by the County.

IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO ITS DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT: 500 San Sebastian View, St. Augustine, FL 32084, (904) 209-0805, publicrecords@sjcfl.us

ARTICLE 38 – USE OF COUNTY LOGO

Pursuant to, and consistent with, County Ordinance 92-2 and County Administrative Policy 101.3, the Contractor may not manufacture, use, display, or otherwise use any facsimile or reproduction of the County Seal/Logo without express written approval St. Johns County, Florida.

ARTICLE 39 – SURVIVAL

It is explicitly noted that the following provisions of this Agreement, to the extent necessary, shall survive any suspension, termination, cancellation, revocation, and/or non-renewal of this Agreement, and therefore shall be both applicable and enforceable beyond any suspension, termination, cancellation, revocation, and/or non-renewal: (1) Truth-in-Negotiation; (2) Federal and State Taxes; (3) Insurance; (4) Indemnification; (5) Access and Audits; (6) Enforcement Costs; and (7) Access to Records.

ARTICLE 40 – AUTHORITY TO EXECUTE

Each party represents that it has the lawful authority to enter into this Agreement and has authorized the execution of this Agreement by the party's authorized representative shown below.

IN WITNESS WHEREOF, authorized representatives of the County and Contractor have executed this Contract Agreement on the day and year below noted.

RFP NO: 22-06 Cyber Security Assessment
Master Contract #: _____

Owner:

St. Johns County, FL
(Typed Name)

By: _____
Authorized Representative Signature

Leigh A. Daniels, CPPB
Printed Name – County Representative

Purchasing Manager
Printed Title – County Representative

_____
Date of Execution

Contractor:

Illumant LLC
(Typed Name)

By: _____
Authorized Representative Signature

_____
Printed Name & Title

_____
Date of Execution

ATTEST:
St. Johns County, FL Clerk of Courts & Comptroller:

By: _____ (Seal)
Deputy Clerk

_____

Date of Execution

Legally Sufficient:

By: _____
Office of County Attorney

_____
Date of Execution

St. Johns County Board of County Commissioners

Purchasing Division

NOTICE OF INTENT TO AWARD

November 24, 2021

RE: RFP No. 22-06; Cyber Security Assessment

Please be advised that the Purchasing Department of St. Johns County is issuing this notice of its Intent to Award a contract to **Illumant, LLC** as the highest ranked firm(s) under **RFP No. 22-06; Cyber Security Assessment.** This notice will remain posted to the **St. Johns County Purchasing Department bulletin board** until 5:00 PM, Wednesday, December 1, 2021.

Any person (including any bidder or proposer) who is, or claims to be, adversely affected by the County's decision or proposed decision shall file a written Notice of Protest with the Purchasing Department of St. Johns County within 72 hours after the posting of the notice of decision or proposed decision. Failure to file a Notice of Protest within the time prescribed in Section 304.10 of the St. Johns County Purchasing Manual (the Bid Protest Procedure), or failure to post the bond or other security required by the County within the time allowed for filing a bond, shall constitute a waiver of proceedings and a waiver of the right to protest. The protest procedures may be obtained from the Purchasing Department and are included in the County's Purchasing Manual. All of the terms and conditions of the County Purchasing Manual are incorporated herein by reference and are fully binding.

Should the Purchasing Department receive no protests in response to this notice, an agenda item will be submitted to the St. Johns County Board of County Commissioners for their consideration and subsequent approval to negotiation, and upon successful negotiations, execute a contract.

Please forward all correspondence, requests or inquiries directly to my attention at the information provided below.

Sincerely,
St. Johns County
Board of County Commissioners

County Representative Signature

Date: 11/24/21

Leigh A. Daniels, CPPB
Purchasing Manager
(904) 209-0154 – Direct
(904) 209-0155 – Fax
(904) 209-0150 – Main
ldaniels@sjcfl.us

ST. JOHNS COUNTY
PURCHASING DEPARTMENT
500 San Sebastian View
St. Augustine, Florida 32084

INTEROFFICE MEMORANDUM

TO: Wylie Thibault, Director of Information Systems

FROM: April Bacon, Purchasing Buyer

SUBJECT: RFP No. 22-06; Cyber Security Assessment

DATE: November 18, 2021

Attached please find a copy of the RFQ Evaluation Summary Sheet for your file as recorded and verified at the Evaluation Committee Meeting.

Please review, evaluate and make a written recommendation for this project. Also, indicate the budgeted amount for this item along with the appropriate charge code and return to my attention as soon as possible.

Please let me know if I can assist your department in any other way.

Dept. Approval Wyl Thibault

Date 11-19-21

Budget Amount $100,000

Account Funding Title Contractual Services

Funding Charge Code 0012-53120

Award to Pillsmant

Award Amount _____

ST JOHNS COUNTY

NOV 19 '21

PURCHASING

EVALUATION SUMMARY SHEET

ST. JOHNS COUNTY, FLORIDA

Date: November 18, 2021
RFQ No: RFP No. 22-06; Cyber Security Assessment

FIRM	RATER PAUL NORRIS	RATER CHAD ILISIE	RATER JOHN RUNDGREN	RATER JAKE PARHAM	RATER DEREK CRIBBS	RATER CHRISTOPHER SHILIDAY	TOTAL	Rank	COMMENTS
ILLUMANT LLC	67.6	88.6	87.6	89.6	89.6	79.6	502.6	1	
SECURANCE CONSULTING	99.0	89.0	66.0	87.0	90.0	57.0	488.0	2	
TRUE NORTH CONSULTING GROUP, LLC	74.0	81.0	79.0	85.0	79.0	90.0	488.0	2	
STEALTH ISS GROUP INC.	72.0	89.0	74.0	90.0	80.0	78.0	483.0	4	
TETRA TECH, INC.	94.1	81.1	55.6	87.1	75.1	84.1	477.1	5	
SECURE IDEAS, LLC	88.0	79.0	84.0	89.0	77.0	57.5	474.5	6	
COMPUTER AID, INC.	68.7	79.7	68.7	78.7	84.7	90.7	471.2	7	
MGT OF AMERICA CONSULTING, LLC	78.9	82.9	57.9	93.9	84.9	69.9	468.4	8	
MOTOROLA SOLUTIONS	65.7	80.7	76.7	82.7	72.7	88.7	467.2	9	
EMTEC INC.	92.0	82.0	57.0	87.0	74.0	59.0	451.0	10	
INTERNATIONAL CONSULTING ACQUISITON CORP ICAC DBA ISG PUBLIC SECTOR	69.1	84.1	57.1	91.1	78.1	68.1	447.6	11	
THE SILICON BLACKGROUP	51.5	82.5	50.5	78.5	76.5	67.5	407.0	12	
ZILLION TECHNOLOGIES INC.	55.0	73.0	43.0	77.0	68.0	45.0	361.0	13	

APPROVED: By signing below, both parties have reviewed and approve this evaluation summary of the responses submitted for this RFQ.

Purchasing Manager: Date:
Director of Management Information Systems 11-19-21 Date: 11/20/21

NOTE:
THE RANKING SHOWN ABOVE SHALL BE FOLLOWED UNLESS SPECIAL CONDITIONS MERIT A CHANGE IN THE NEGOTIATING ORDER, IN THIS CASE, THE SPECIAL CONDITIONS MUST BE EXPLAINED IN DETAIL IN THE COMMENTS SECTION OR ATTACHED TO THIS EVALUATION SUMMARY SHEET.

POSTING TIME/DATE FROM 4:00 p.m. November 22, 2021 UNTIL 4:00 p.m. November 29, 2021.

ANY RESPONDENT ADVERSELY AFFECTED BY AN INTENDED DECISION WITH RESPECT TO THE AWARD OF ANY SOLICITATION, SHALL FILE WITH THE ST. JOHNS COUNTY PURCHASING DEPARTMENT A WRITTEN NOTICE OF INTENT TO FILE A PROTEST NOT LATER THAN SEVENTY-TWO (72) HOURS (EXCLUDING SATURDAY, SUNDAY AND LEGAL HOLIDAYS) AFTER THE POSTING OF THE NOTICE OF INTENT TO AWARD, PROTEST PROCEDURES PROCEDURES MAY BE OBTAINED FROM THE PURCHASING DEPARTMENT.

illumant

Proposal

RFP No. 22-06: Cyber Security Assessment

October 27, 2021 (v1.0)

Prepared for:

St. Johns County

Illumant
431 Florence Street, Suite 210
Palo Alto, CA 94301
www.illumant.com
650-961-5911

Section 1: RFP Cover Page (Complete and Submit) and Cover Letter

COVER PAGE

SUBMIT ONE (1) ORIGINAL HARD-COPY AND ONE (1) EXACT ELECTRONIC PDF COPY ON A USB DRIVE IN A SEALED ENVELOPE OR CONTAINER TO:

PURCHASING DIVISION
ST. JOHNS COUNTY
500 SAN SEBASTIAN VIEW
ST. AUGUSTINE FLORIDA 32084

COMPANY NAME: Illumant LLC

CONTACT NAME & TITLE: Matija Siljak, CEO

CONTACT PHONE NUMBER: 650-961-5911

CONTACT EMAIL ADDRESS: siljak@illumant.com

DATE: 10/26/2021

April Bacon
Purchasing Buyer
St. Johns County Purchasing Division
500 San Sebastian View
St. Augustine, FL 32084

Dear April:

Illumant, LLC ("Illumant") appreciates the opportunity for our consulting group to assist the St. Johns County ("The County") with its requirement to have a Cyber Security Assessment

The County would like an outside party to conduct comprehensive internal and external assessments to assess the security of its web sites, web applications, networks, physical locations, staff, and systems. The assessments required include internal and external vulnerability analysis and penetration testing of sites, applications, servers, routers, desktops and firewalls, as well as social engineering, security technology/strategy analysis, deep analysis of regulatory environment/governance, and assessments of physical security.

Given our security expertise, extensive experience, and proven assessment methodologies we are prepared to assist the County with these requirements.

As part of every engagement, Illumant furnishes reports for each security assessment component providing a comprehensive analysis of security from both executive and technical perspectives. The reports include analyses of vulnerabilities and weaknesses, along with summary tables and graphical data, as well as prioritized action items and remediation recommendations for cost-effective improvement of security. Sample assessment reports accompany this proposal to provide examples of the form and quality of our work.

In the remaining sections of this proposal we describe the details of the services proposed and their associated deliverables along with the fees, terms and conditions for Illumant to perform the work. Also included are references, bios and a partial list of clients.

With respect to the specifics of the RFP, Illumant is ideally suited to assist the County with its requirements. This work is directly in line with our core competency and the work that Illumant provides on a regular basis. The included references and bios should provide additional confidence in Illumant's experience and expertise.

Matija Siljak, 650-248-4060, siljak@illumant.com

We look forward to assisting the St. Johns County with its security assessment requirements. For more information about our organization, please review the Company Overview in the following section.

Sincerely,

Matija Siljak
CEO / Founder
Illumant, LLC

RFP Direct Requests

- Illumant, LLC, 650-961-5911, info@illumant.com
- 431 Florence Street, Suite 210, Palo Alto, California 94301
- Matija Siljak CEO, Mark Snodgrass COO
- Established 15 July, 2006, 15+ years in business, a team of 20.
- Mission: Empowering organizations to defend themselves against security breaches through assessment, penetration testing, and compliance.
- Interest: This works is in line with Illumant's core competency. We have delivered these exact services to other agencies in Florida for years.

Table of Contents

Section 2: Qualifications

Company Overview

Illumant is a trusted strategic and tactical information security and risk management advisor to Fortune 500 companies, higher education institutions, government organizations, public and pre-public enterprises. Illumant leverages deep knowledge of security, governance, risk management, compliance, and information technology to partner with our clients to assess and solve their critical security and compliance issues. Whether the focus is on initiatives driven by regulatory compliance or best practices, Illumant provides the expertise and bandwidth necessary to help clients consistently meet their security objectives.

Since 2006, Illumant has provided its clients with over a thousand security assessments. The original organization was formed in 1999 under the name OLOSEC Network Security Solutions and provided the same core services, but was later merged with a larger IT consulting firm and then subsequently was spun back out as Illumant. The original founders are still with Illumant today.

Our wide range of experience over the years across all verticals gives us a uniquely broad perspective on information security, and allows us to bring the best ideas and techniques from disparate environments to each project, while our in-vertical experience allows us to frame our findings and recommendations appropriately for each client's specific needs.

Illumant has conducted security and risk assessment/management projects for organizations ranging from universities (including Stanford, Duke, UCLA) to disaster response companies like the Marine Spill Response Corporation, to government organizations and affiliated utilities like the Travis County, City of Burbank, Alameda Municipal Power, the City of Avondale, and more.

Our security experts are first and foremost intimate with best-practice information security policies, procedures, practices and technologies, as well as, compliance requirements such as NIST 800-53 (and SPs), CIS, GLB, HIPAA/HITECH, NERC, ISO27001/2, COBIT, PCI-DSS, DHS, FTC, FERPA, SOX, CJIS, SAS70 and others. Furthermore, our experts hold various security certifications such as CISA and CISSP.

With respect to the specifics of the RFP, Illumant is ideally suited to assist the County with its requirements. This work is directly in line with our core competency and the work that Illumant provides on a regular basis. The included references and bios should provide additional confidence in Illumant's experience and expertise.

Office Location
This project will be performed by Illumant's team located at 431 Florence St. Suite 210, Palo Alto, CA 94301. The project team is described in detail in the "Project Team Bios" section.

The following are a few things that set us apart from our competitors:

Why Illumant?

We're one of the best – We are not just making this up. Our clients often tell us that we're the best pen-testing firm they've worked with. And we have some great clients.

Hall of fame bug hunters – Became 1st ranked on Alibaba's Bug Bounty Hall of Fame for 2018 after only a month: Alibaba Bug Bounty Hall of Fame 2018 (or go to www.illumant.com/blog/ and find Alibaba entry).

Awesome deliverables – We take a lot of pride in our reporting. Our reports are super informative and look great – and following our recommendations improves your security.

Zero-days – We don't just find the vulnerabilities that everyone already knows about, we find new and undiscovered vulnerabilities as well – meaning with us you are ahead of the hackers. Check out our latest, here: www.owndigo.com.

Friendly, expert hackers – We have some of the top hacking talent around, with the best skills and certifications, as well (OSCE, OSCP, GPEN, etc.) But we're not just great at hacking, our people our great at presenting and discussing, too.

Great clients – here are a few:

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "H"

KEY PERSONNEL LIST

In the space below, list all qualified personnel who are permanent employees of the company that may be utilized to perform any aspect of the required services. Attach brief but comprehensive resumes for each staff member listed below.

Employee Name	Employee Title	# Years Employed	Total # Yrs. Experience
Goran Tuzovic	Sr. Security Analyst	8	10+
Matija Siljak	CEO	15	20
Mark Snodgrass	COO	15	20
Ben Kaufman	Sr. Security Analyst	4	7
Luis Rios	Lead Security Analyst	5	10
Claus Shafhalter	VP Compliance	11	21
Billens Crow	Sr. Solutions Advisor	9	9

Senior Advisors (Not Project Affiliated)

Ced Bennett, Emeritus Director, Information Security Services for Stanford University

As a Senior Lead Consultant at Illumant, Ced Bennett offers a dynamic combination of strategic leadership, large-scale management skills, and depth of technical expertise. In his role as Director, Information Security Services for Stanford University, Ced led a department tasked with building awareness and driving change in individual and organizational behavior with regard to increasing institutional information security. He led the team that was responsible for information security policy development and implementation and for moving the institution toward more effectively securing its information resources. As a well-respected source of technical leadership, Ced is considered an evolutionist in the field of information security. He maintains this edge by continuing to seamlessly integrate emerging technologies with future client needs.

Ced has been a part of information technology senior management for more than 30 years. During that time, he has been responsible for the leadership of a variety of information technology organizations including the development and support of administrative systems, the initial deployment and support of desktop and distributed computing, the development and support of library computing, and many others. Prior to joining Stanford, he held information technology leadership positions in the private sector for the electronics, wholesale/retail, health care, and IT services industries.

Ced is currently a member of the EDUCAUSE/Internet2 Computer and Network Security Task Force. A frequent speaker at professional conferences and seminars, Ced served as a founding faculty member from 1998 to 2001 in the CAUDIT-EDUCAUSE Institute held in Australia each year. He was instrumental in the creation of the CAUSE Management Institute (now the Leadership and Management Programs of the EDUCAUSE Institute) in 1990, in its direction through 1995 and as a faculty member through 1997. Ced was a member of the CAUSE Board of Directors from 1985 through 1989 serving as Chairman of the Board in 1987.

Ced holds a BA in philosophy from San Francisco State University and has completed graduate work in philosophy, cybernetic systems and business.

Roger Smith, CISA, CISSP, PCI Qualified Security Auditor (QSA)

Roger Smith is a Senior Consultant in Illumant's IT Risk Services practice, where he develops Illumant's consulting methodologies and project manages Illumant's security, SOX IT, SAS70, and other IT risk and compliance projects. Prior to joining Illumant, Roger was the principal at Argos I/T Security Services, where he led security, SOX general controls and application audit teams at Siebel, Verity, MIPS, E-Loan, and Essex Property Trust. Prior to founding Argos, Roger had senior roles in three high growth startups, including Napster, the original online music company, where Roger was Executive Director of Operations. In that role Roger took that company from 10 people to 250 in six months and built out a world class data center from a single T1 line to one that pushed a sustained 1Gigabit 24x7. Roger also worked at NASA's Ames Research center for 15 years, making significant contributions to projects such as the first successful Martian Lander and the Lunar Prospector Satellite.

Roger holds a BS in Computer Science from Trinity University. He holds CISSP, CISA and PCI DSS Qualified Security Auditor (QSA) certifications.

Project Staff (Project Affiliated)

Matija Siljak, CISA

Mat Siljak is Director, Advisory Services, at Illumant, where he drives compliance and enterprise security services at Illumant. Leveraging deep technology, regulatory, and risk management expertise, he has managed over 100 consulting engagements for firms ranging from Fortune 500 to pre-public companies. Mat has participated in many high profile conferences, including "Sarbanes-Oxley: Lessons from the Trenches" and "Sarbanes-Oxley and the CIO." He is CISA certified and is a member of ISACA, and the San Francisco Bay Area Chapter of InfraGard which provides channels for the exchange of information about infrastructure threats and vulnerabilities

Prior to joining Illumant, Mat co-founded OLOSEC Network Security Solutions, an information security consulting firm based in Menlo Park, California. He previously held the position of Chief Technology Officer for Bullhound, Ltd., a global technology hedge fund based in London.

Mat holds a B.S. and an M.S. in Electrical Engineering, both from Stanford University. Mat has a CISA certification.

Mark Snodgrass, CISSP, CISA

Apart from active roles in consulting engagements, Mark also drives the development of Illumant's consulting tools and systems, which enable and facilitate internal processes and drive consulting quality and efficiency. Mark is responsible for the development of a proprietary suite of tools and the integration of open-source products. He has focused on developing superior statistical analysis tools for vulnerability detection, IDS, denial of service prevention, and log review. Mark joined Illumant as a Senior Security Engineer in 2003. Prior to that, he co-founded OLOSEC Network Security Solutions. Over the past years, he has worked on hundreds of network security assessments and dozens of compliance audits.

During his tenure as a Ph.D. candidate at Stanford University, Mark researched large-scale stochastic systems, developing specialized statistical analysis tools and novel data-mining techniques.

Mark holds a B.S. and M.S. in Civil Engineering and a Ph.D. in Civil and Environmental Engineering, all from Stanford University. He is CISSP certified by the International Information Systems Security Certification Consortium and CISA certified by the Information Systems Audit and Control Association

Claus Schafhalter

Claus is a team leader and a member on a number of Illumant compliance and enterprise risk management projects. He has spent the last 15 years as a senior IT executive consultant to Fortune 500 and medium sized companies in numerous industries, including financial services, high tech, energy, and manufacturing. Claus is especially effective in providing executive oversight and strategic perspective while maintaining strong focus on essential details. Claus has consistently demonstrated the ability to commit to objectives while maintaining the flexibility to adjust to changing environments.

In recent years, Claus has focused on high-visibility SOX compliance projects, assisting clients with preparation of IT risk assessments, risk control matrices, and IT policies and procedures; designing and documenting control activities; performing testing; and remediating controls. Prior to his involvement in SOX, Claus engaged in over 100 consulting projects, specializing in IT planning and implementation, business process engineering, and development of methodologies for process documentation and improvement and change management. Claus previously provided program management services for a $100 million project portfolio, simultaneously overseeing the activities of 10 project teams. Claus has also engaged in several “project rescue” interventions, whose requirements have included project risk analysis, new project setup, initiatives prioritization, and interim project management.

Claus' expertise includes ERP, CRM, plant control, and logistic applications, and he has extensively applied the gamut of best practice frameworks including COBIT, ITIL, EIA649 (Configuration Management), and ISO 9000ff (Quality Management) to design and implement IT policies and procedures.

Claus obtained a BS and MS from the Technical University in Graz, Austria, European Union, with a major in Industrial Engineering.

Chris Anastasio, OSCP, CCNA, Linux+

Chris has been involved in the IT industry since 2006, performing networking and security work for datacenters, universities, and MSSPs. He is heavily involved in the technical portion of Illumant penetration testing engagements and has an endless appetite for hunting down and exploiting security vulnerabilities.

Using his strong foundation in networking and programming, combined with exposure to many of the latest offensive security techniques, Chris quickly identifies vulnerabilities on the network. A combination of manual and tool based exploitation methodologies allows him to clearly demonstrate the impact of these weaknesses. He has even discovered and exploited previously unknown vulnerabilities in commercial software and worked with the respective vendors to patch these bugs.

Besides writing exploits, Chris also works on tools to assist with recon, out of band data exfiltration, and automation. In his quest to become "1337" he has obtained the Linux +, Cisco Certified Network Associate, and Offensive Security Certified Professional certifications and is working relentlessly to become better and know more.

Goran Tuzovic GPEN

Goran began his career in IT in the late 90s. He has 10+ years of experience providing penetration testing services to Illumant's clients focusing on vulnerability analysis and penetration testing of Internet-facing and internal networks, wireless networks, and cloud, network-device, and virtualization security configuration reviews focused on specific platforms such as: AWS, O365, Azure, GCP, AD, etc., He has performed hundreds of security assessments engagements including successful black box penetration testing engagements demonstrating privilege escalation (e.g. escalating to domain admin), and wireless security assessments and penetration (e.g. successful over-the-air man-in-the-middle attacks and evil twin attacks to capture passwords and crack hashes to gain remote access). Goran has specialized experience around testing especially sensitive pieces of scope (VOIP, SCADA, High Frequency Trading Infrastructure, etc.).

Goran currently holds the GPEN certification.

Ben's Kaufman CCNA Cyber Ops, GCIA GIAC, GIAC, Advisory Board, OSCP

Ben kicked off his security career as a network security analyst in a security operations center for a cloud managed security provider in Houston Texas. His proclivity towards incident analysis led to a quick promotion to the Incident Response Escalation Team where he worked on only the most severe and vexing security incidents. Ben's skill for development was recognized quickly as well with another promotion after he pioneered tools to better track SOC performance and efficiency. This promotion had Ben working with the Structured Analysis team where he focused on proactive manual analysis to identify threats for enterprise customers. He uses this knowledge to help Illumant's clients get more out of their assessments and strategic technology purchases through purple team exercises. Ben is also a skilled hacker and loves rooting boxes. This led him to switch to the offensive side of security at Illumant. He is an Offensive Security Certified Professional.

Luis Rios OSCP

Luis's professional security career began in defense working as a Network Security Engineer for a major, cloud based, security monitoring provider before switching to offense as a full time penetration tester at Illumant. Luis's security experience took shape well before his career. When he was obtaining a B.S. in Computer Science from Sam Houston University, he founded HASH (Hacking at Sam Houston). Through HASH Luis provided hands on hacking training and taught other students how to develop security experience on their own as well. Many of these students are also as security professionals today. On a day-to-day basis he leverages advanced vulnerability identification and exploitation techniques to help demonstrate risk to clients. As well, he is constantly working to improve processes and efficiencies through software development and automation. His main interest in security is hacking web based products.

Even in his free time he is constantly sharpening his skills and staying engaged with the latest happenings in information security. He has placed in the top 10 at hacking challenges such as Collegiate Cyber Defense Club (CCDC), online Capture the Flag (CTF) competitions, as well as CTFs from well-known security conferences such as DerbyCon. He is also dedicated to helping other people, and is an organizer of multiple IT security meetings, The Dark Corner, being the latest one which has a few hundred members.

Luis currently holds the Offensive Security Certified Professional (OSCP) certification.

Why This Team?

This team represents a strong mix of technical security experts as well as organizational security experts with tremendous compliance expertise. Each of these people has led similar engagements with mixed technical and organizational components from start to finish and have successfully worked on similar projects together in the past. All technical analysts have certifications like OSCP which focus on exploitation rather than memorization (hacking to achieve vs. multiple choice tests). In addition to these certifications, Illumant requires technical analysts to pass extensive expertise testing and lab activities in order to be considered for employment.

Section 3: Project Approach

The County has established a need to evaluate the security controls currently in place, identifying gaps where no or insufficient controls exist that may be contributing to heightened risk or vulnerability. This work should be conducted thoughtfully and systematically to include all relevant aspects of information security – policies, procedures, people, physical access, technology, regulatory landscape, configuration, etc. This work is to be comprehensive, requiring Illumant to adopt multiple testing roles and perspectives, including several from the perspective of privileged insiders.

Illumant's assessment approach is best characterized as "refined". We have extensive experience performing security assessments just like those requested in the RFP document, having performed over a thousand assessments over the last 15 years. Our assessment methodologies have been evolved to maximize efficiency, thoroughness, and utility, and we continue to evolve them. This includes mechanisms to find and incorporate the latest security vulnerability information and exploit techniques in our assessments.

With all of our assessments, we leverage available "best-of-breed" tools to create a baseline, manual techniques to eliminate false positives, manual exploitation to confirm severity (e.g. ability to propagate attacks, escalate privileges or access sensitive information), and manual analysis to identity vulnerabilities not detected by tools.

Our project management approach has also been honed through experience to be efficient in gathering the information necessary to complete an assessment while minimizing disruption to the client where possible. Our approach provides transparency by setting expectations up front, forecasting hurdles, communicating progress, identifying obstacles as they arise, and ensuring expectations are met.

If we were to further characterize our approach it would be "thoughtful" and "flexible". Illumant works with its clients to ensure needs are met, and we are always willing to tweak our approach to meet special requests, constraints and requirements, maximizing the value of all Illumant contracts. As an example of how this works in practice:

We offer multiple angles from which to identify similar issues – take patch management for example:

- Review of policies and procedures in this area
- Interviews with IT staff to understand internal conception of practice
- Credentialed vulnerability scanning to identify volume of superseded patches, and actual state of patch management.

Similar projects only offer some insight into our experience, so we are also offering common hurdles these types of projects encounter and how Illumant's process is primed to avoid them:

<u>Interview Availability:</u>
Stakeholders in larger organizations are very busy. Illumant has streamlined our compliance assessment process to utilize questionnaires derived from checklists to minimize interview time and resource burden. Illumant also plugs into your schedule, and can perform last minute, on the fly interviews in cases where it's easiest for stakeholders to call us without notice. Or knock them all out in a short time period.

<u>Draft and Board Ready Reporting:</u>
Reporting and results material to those administrating security programs may be alarming to less technical boards. For instance, applying all patches as they are ready is a major undertaking. Reporting on superseded patches is necessary to better understand a patch management program's effectiveness, but these results may be alarming to boards less familiar

with common IT challenges. During the draft phases of reporting, Illumant works with client IT/Security/Compliance and other stakeholders to ensure results are presented in a way that drives remediation efforts and is politically effective.

Scope Gathering:
Like interview availability challenges, IT operations may make providing scope difficult to accommodate. To solve this, Illumant will not schedule an assessment component until scope is provided. During the brief weekly project meetings, it will become apparent if there are issues in providing scope. If this is the case, Illumant works to reorder timing of components to frontload non-scope reliant components and identifies alternative ways in which Illumant might be able to present a potential test scope for client approval.

Project Management Approach and Hours
At the project's outset, Illumant will work with the County's project liaison(s) to develop a plan (based on Illumant's refined project planning templates) to enumerate scope, schedule, testing windows, points of contact, and project objectives and milestones. For each project Illumant assigns three POCs: Project Coordinator, Project Lead, and Technical Lead. The Project Coordinator ensures smooth communication of testing-related information between The County and Illumant. They also work internally within Illumant to ensure that assessment objectives and timelines laid out during project planning are being met. The Technical Lead is also responsible for organizing the assessment team and ensuring the quality of our analysts' work. Weekly status meetings are brief, but effective ways of ensuring that project adheres to deadlines and anything that might delay them is forecasted well in advance. These meetings can be formal or informal.

Additionally, Illumant's project management team reviews org charts and works to understand who the relevant stakeholders are, and makes early introductions to ensure each understands their impact/role in the assessment to gain buy in.

Client Team Support
Illumant anticipates only requiring minimal support from the County's staff. The majority of this effort centers around scope gathering (for non-black-box activities), kick-off and findings calls (~1h), and brief weekly meetings which can be either formal or informal. Testing conducted remotely may require staff to plug in and turn on an appliance and testing on-site requires staff assistance with guest badges and workspace.

Internal Special Resources
Illumant maintains an internal library of complex payloads aimed at testing and bypassing antivirus and other common protections. We also maintain a vast library of internally developed scripts/tools that assist the efficiency of our testing. For instance, our phishing platform allows us to launch service based and customized phishing attacks at scale.

Specific Outline of Work
Once expectations have been aligned and scope gathered through project planning/management. Our staff will begin review and analyze documentation immediately, and deliver targeted questionnaires to relevant stakeholders, aimed at minimizing interview volume and therefore cost. This process ensures interviews are used for meaningful interactions that don't overlap information gathered between interview targets. Our Risk Assessment and Policies, Procedures, and Practices Assessment are performed in parallel via interview that can be scheduled in a series of days if there are aggressive deadlines. From a top down perspective, these efforts will identify information relevant to the RFP's primary assessment targets like internal network, external network, mobile device security, Partner Connectivity, Interface to Partner Entities, Client Remote Access to External Services, etc.

Follow up interviews will be conducted remotely as appropriate (based on RA/PPPA results) to analyze security and technology strategy further through our Security Technology Architecture and Roadmap Review.

We will have a technical team working concurrently with the team conducting top down work related to risk and governance. They'll begin with a Blind Exposure and Vulnerability Analysis to characterize The County's digital footprint, enumerate externally addressable systems, map potential trust relationships, etc. These results will be compared with the scope The County provides for the next phase – Perimeter Security Assessment for external vulnerability assessment and penetration testing of externally facing systems and unauthenticated applications. With approval we can utilize password spraying to access and further test these apps.

Illumant will move towards internally focused assessments from the perspective of a successful external hacker or malicious internal user. We will conduct internal vulnerability assessment and penetration testing through the LAN Security Assessment, Critical Asset Security Assessment, and Wireless Security Assessment. We can utilize credentials found in other components to escalate privileges if desired, or start the process over internally by using fake APs in the Wireless Security Assessment to gather credentials, or using LLMNR to get user hashes to crack offline. We'll work to identify the maximum volume of vulnerabilities in our time period, as well as attempting to Domain Takeover. These attempts will uncover valuable technical and practical information related to:

Additional analysis will be conducted for free to offer a report specific to the County's susceptibility to Ransomware.

Social Engineering will be broken into multiple vectors (planted media, attachments, social media, phishing, etc.) and launched partially through Illumant's phishing program, with some of the efforts like planted media or pretext calling requiring manual effort. Certain attacks will require additional target research like identifying critical access staff from school with large alumni network or professional development associations where one might review documents for another like a resume as a favor. This may be conducted at the project's outset to use stolen credentials in other components. Early social engineering is preferred to allow busier staff time to work through email backlogs. Physical Security may be evaluated as a social engineering vector or performed from a checklist and tour perspective without social engineering at any point in the assessment. Regardless of approach, we will need some access to validate that MAC filtering is implemented effectively and an attacker cannot hid and hack from a conference room or public use area.

Illumant will be delivering draft reports per component as they are available to allow the County to have a constant information flow and make comments on the fly that may impact the structure of future reporting. The final deliverable will contain a vulnerability assessment plan including a roadmap to reaching the next levels of security program maturity through remediation. The draft reports and plans will be discussed before finalization in specific findings calls to ensure impact of reporting is heavily considered, and County staff understand the remediation recommendations. Final deliverables will be approved by the County and then Illumant will make presentations formally to all relevant stakeholders.

Remediation is a long, arduous process and Illumant always remains available to support reports, usually at no additional charge. Our clients frequently call us for advice when implementing remediation recommendations, or shoot us an email if there are especially tricky vulnerabilities they cannot replicate. We'll happily offer guidance, and even send video of step by step vulnerability reproduction to make life easier on County staff.

Requested Services & Services Pairing

Guide to Pairing
RA – Risk Assessment – top down strategic security risk analysis
STARR - Security Technology Architecture and Roadmap Review – analysis of technology
PPPA – Policies, Procedures and Practices Assessment – documentation reviews, compliance
BVEA – Blind Visibility and Exposure Analysis – enumerating cyber-attack surface
PSA – Perimeter Security Assessment & Pen Testing – external vulnerability and penetration testing
CASA – Critical Asset Security Assessment – internal vulnerability and penetration testing

LANSA – LAN Security Assessment - internal vulnerability and penetration testing
WSA – Wireless Security Assessment – security analysis of wireless infrastructure
WASA – Web Application Security Assessment – credentialed/uncredentialed app testing
PhySA – Physical Security Assessment
Soc Eng – Social Engineering – testing employee awareness to phishing, USB drops, etc.
ADSA – Active Directory Security Assessment
WISP – Written Information Security Program Development

Services Pairing		
RFP Service	**Illumant's Matching Services**	**Additional Detail**
Benchmark existing IT Security Policies/Practices and Procedures	**PPPA, RA**	**Illumant's PPPA analyzes policies, procedures, and practices against predetermined security frameworks. RA also examines documentation and practices from a risk perspective.**
Vulnerability Assessment	**PSA, CASA, LANSA, WASA, WSA, Soc Eng, PhySA**	**The initial phases of these services are focused on the enumeration of vulnerabilities through vulnerability assessment. Once vuln assessment is complete penetration testing begins.**
Internal Network	**CASA, LANSA, WSA, ADSA, RA**	**Internal network is evaluated from both top down (organizational assessment) and bottom up (technical testing) perspectives.**
External Network	**RA, PSA, WASA, WSA**	**External network is evaluated from both top down (organizational assessment) and bottom up (technical testing) perspectives.**
Partner Connectivity **Interface to Partner Entities** **Evaluate Client Remote Access to External Services** **Evaluate Internal MIS Tools for Data Leakage**	**RA, PPPA, PSA, CASA, LANSA, BVEA**	**Evaluated on basis of technology used and vendor management perspectives during RA . From a policy/procedure perspective in PPPA. Tested technically for vulnerabilities and data leakage.**
Wireless Network	**WSA, RA**	**WSA is a penetration test focused on wireless. RA evaluates Wireless from a top down perspective.**
Physical Access Controls Evaluation	**PPPA, RA, PhySA**	**Testable top down thru RA, PPPA targets specific documentation around these controls. PhySA targets these controls in practice.**
Internet Usage	**PPPA, RA, PSA**	**Testable top down thru RA, PPPA targets Acceptable Use policy, but can also be evaluated technically, including reviews of PCAP files to understand traffic.**

Social Engineering Component	**PhySA, Soc Eng**	**Multiple vectors for phishing and social engineering staff, as well as in person testing to identify insecure practices in working environments.**
Mobile Device Security	**RA, PPPA**	**This can be evaluated top down through risk assessment, and specific policies and procedures can be evaluated through the PPPA**
Host Based Security	**PPPA, RA, STARR, CASA, LANSA,**	**Top down we can examine risk perspectives around hosts, analyze documentation around these hosts, and review the appropriateness of the technologies utilized. From a technical perspective, we can identify meaningful vulnerability information from hosts.** **If we are allowed to conduct credentialed scanning, we can also identify meaningful configuration information on hosts.** **Illumant can also evaluate the effectiveness of password policies through bottom up testing by cracking user password hashes identified during pen tests. This is done in Illumant's offline password cracker – prevents account lockouts during pen tests.**
Additional Services	**RansomSA**	**Illumant combines insights from all the testing performed through other components to offer free report on the impact of Ransomware to an organization.**
Additional Services	**WISP**	**The interviews in the RA, PPPA, and STARR afford us enough insight to quickly tailor policies and procedures for clients post assessment. The County indicated in Q/A that this could be a part of this exercise, so Illumant is offering it as an optional service.**

Core Services

Risk Assessment/ Strategic Planning (RA)	The risk assessment is a top down analysis of an organization's security posture. Leveraging vulnerability data and security information gathered through other assessment components, along with data collected through targeted questionnaires and interviews, Illumant performs a quantitative and qualitative risk analysis to determine the top threats to information security, the biggest vulnerabilities, and the largest opportunities for risk reduction through cost-benefit analysis. Illumant uses a proprietary risk evaluation model that provides the basis for a report which describes key assets, threats and vulnerabilities, and recommendations for risk mitigation. The model can be used for scenario planning and to revalidate the organization's security posture after risk mitigation activities. The risk assessment adds an important strategic level of analysis to security planning, helps to align security goals with overall organizational objectives. This global context is something lacking in most of our competitor's offerings.
	Scope: Illumant will conduct up to 8 interviews for this analysis. These interviews will overlap the interviews for the Security Technology Roadmap below.
Security Technology Architecture and Roadmap Review (STARR)	In conjunction with the Risk Assessment process, Illumant will review the technology currently used to secure critical data and operate a client's business. This process will identify the systems and services presenting the greatest risk to the organization, as well prioritize the transitioning from the riskiest systems to technologies that meet best practices or regulatory and contractual obligations. This assessment is helpful to organizations needing to make thoughtful investments in security technology that maximize impact to posture, while keeping a budget in mind.
	Scope: Illumant will conduct up to 8 interviews for this analysis. These interviews will overlap the interview for the risk assessment above.
Policies, Procedures and Practices Assessment (PPPA)	Illumant will assess the IT organization in terms of policies, procedures, documentation, and practices as they pertain to access control, breach response and incident handling, change management, operational controls, organization controls, assessment, and various technical security measures. We will also assess conformance with best practices and any relevant regulatory requirements (e.g. HIPAA/HITECH, PCI, FISMA CIPv5, SOC 2/SAS 70/SSAE 16 etc.)
	Scope: To conduct this assessment, Illumant will interview up to 8 designated members of IT staff and review any provided documentation.
Blind Visibility and Exposure Analysis (BVEA)	Without any assistance from the customer, our experts will attempt to identify all Internet-accessible networks systems, sites, applications and services; and any information about the company gleaned from public databases, forums and chat rooms that might be sensitive in nature, or useful in crafting a cyber-attack.

	The purpose of this exercise is to describe the client's cyber-attack surface, to make the customer aware of all assets and information which are currently visible from the Internet (the organization's "Internet footprint") and therefore exposed to possible Internet-based threats. Illumant also searches organizational and non-organization sites and sources to identify sensitive information that may have been exposed, or any chatter about the organization relating to security or planned attacks from chat rooms and forums. Furthermore bot lists, black lists, and web reputation sites, are inspected to serve as a leading indicator of malware infections with the client's systems. Notes: This assessment is typically performed prior to the Perimeter Security Assessment & Penetration Testing and serves to confirm assessment targets and scope for the subsequent testing.
	Scope: This is a blind test and requires no input from the client. Once the test has been completed the results will be reviewed with the client to confirm that all in-scope networks and systems have been properly identified.
Perimeter Security Assessment (PSA)	This assessment involves the enumeration of vulnerabilities and risks that are accessible from the Internet – the "hacker's perspective" – and includes expert manual validation and penetration testing. Illumant starts by using a cross section of best-of-breed scanning tools to harvest vulnerability data. Our experts then validate all results to eliminate false positives and uncover any other vulnerabilities that may have initially escaped detection. To the extent possible (without damaging systems or data) identified vulnerabilities are exploited to assess their real severity, the level of exposure they may allow, and the potential impact of a breach. Targets of this assessment include servers, applications (without credentials – see note), firewalls, routers, load balancers, VPNs, and any other perimeter or Internet-facing information assets. Protection measures are evaluated in terms of their ability to maintain the confidentiality, integrity and availability of networks, systems, applications, and data. As part of the PSA, penetration testing (without credentials) is performed on critical applications. The types of security issues identified during the PSA include SQL injection, URL injection, CSRF injection, directory traversal, auth vulnerabilities, AJAX vulnerabilities, insecure direct object references, security misconfigurations, sensitive data exposure, missing function level access controls, buffer overflows, missing patches, vulnerable versions, insecure credentials, and many others. Goals for the exercise include unauthorized access and privilege escalation as well as an analysis of availability (DOS) risks. Note: For in-depth, credentialed and non-credentialed testing of applications see our Web Application Security Assessment – WASA.
	Scope: The PSA will target The County's up to 80 externally addressable systems.
Critical Asset Security Assessment (CASA)	This internal assessment involves the enumeration of vulnerabilities and risks that are accessible from within the network perimeter, behind border firewalls. Similar to external assessments, like the PSA, Illumant starts by using scanning tools to harvest vulnerability data. Our experts then validate all results to eliminate false positives and uncover any other

	vulnerabilities that may have initially escaped detection. To the extent possible (without damaging systems or data) identified vulnerabilities are exploited to assess their real severity, the level of exposure they offer, and the potential impact of a breach. Targets of this assessment include servers, applications, portals, routers, switches, and any other critical internal systems. Testing may include Internet-facing systems, but viewed internally without filtering by firewalls. Protection measures are evaluated in terms of their ability to maintain the confidentiality, integrity and availability of networks, systems, applications, and data and to repel internal threats and attack propagation. *Note: Depending on the specifics of the in-scope environment, the CASA and LANSA (if selected) deliverables may be combined into a single report. This allows the client to view all affected systems for a given finding in one report rather than searching through multiple reports.*
	Scope: The CASA will target internal servers and infrastructure devices.
LAN Security Assessment (LANSA)	This internal assessment involves the enumeration of vulnerabilities and risks that are accessible from within the network perimeter, behind border firewalls, on end-user LANs. Similar to external assessments, like the PSA, Illumant starts by using scanning tools to harvest vulnerability data. Our experts then validate all results to eliminate false positives and uncover any other vulnerabilities that may have initially escaped detection. To the extent possible (without damaging systems or data) identified vulnerabilities are exploited to assess their real severity, the level of exposure they offer, and the potential impact of a breach. Targets of this assessment include desktops, laptops, workstations, LAN servers, LAN switches, and LAN-based systems. Protection measures are evaluated in terms of their ability to maintain the confidentiality, integrity and availability of networks, systems, applications, and data and to repel internal threats and attack propagation. Notes: Testing of end-user systems is performed with credentials to evaluate the security within the end-user's context including patch-levels, vulnerable applications and out-of-date Oss. *Note: Depending on the specifics of the in-scope environment, the CASA (if selected) and LANSA deliverables may be combined into a single report. This allows the client to view all affected systems for a given finding in one report rather than searching through multiple reports.*
	Scope: The LANSA will target the workstations. Illumant will report on a representative sample of laptops and desktops, and report specifically on any vulnerable outliers.
Wireless Security Assessment (WSA)	Ensures protection against unauthorized access to wireless networks and wireless data, as well as segregation of guest access from private networks and systems. The WSA identifies potential back-doors through rogue access points; assesses corporate, guest, and point-to-point wireless LAN deployments to identify weaknesses in architecture, configuration, authentication, and encryption including identification of rogue access points; and, verifies that authentication and encryption prevent unauthorized access or traffic snooping.

	Notes: The WSA may be performed on-site or off-site via remote access to testing laptop. The latter saves on the cost of service.
	Scope: The WSA will target a relative sample of in-scope locations (1 with 2 SSIDs)
Social Engineering (Soc Eng)	Just about every major security breach that has been featured in the news of the past decade has involved a social engineering component – Target, Sony, JP Morgan, etc. Coupled with technical penetration techniques, the two attack vectors provide a lethal recipe for successfully breaching an organization and gaining unauthorized access to sensitive information. Social engineering is typically the piece that give the attacker a foothold within the organization from where they can propagate their attacks to gain real access to sensitive information. Beyond just phishing, the Social Engineering exercise targets the human element using multiple attack vectors to test awareness of users to potential security threats. Illumant conducts simulated phishing, planted media, pretext calling, and social networking attack against a sample of the organizations users. Some companies prefer that the entire workforce be tested, others prefer that a representative sample be used. Illumant consults with the client during the proposal process to select the most appropriate sample size is chosen.
	Scope: Illumant together with The County will select a representative sample of individuals for social engineering testing across the organization.
Physical Security Assessment (PhySA)	Assessment of facilities and properties to analyze the key security measures that govern physical security that are required to control access to buildings and to protect the people and data within them. Includes a review of access controls at all egress and ingress points, including badging/pass protocols, guest access procedures, and reception/guard control, alarm systems, camera placement, lighting and patrol routes.
	Scope: The PhySA will include reviews of up to 2 locations on the same campus.
Ransomware and Endpoint Security Assessment (RansomSA)	Assessment of an organization's ability to defend itself against ransomware including analysis of the potential impact of a successful ransomware attack, the ability to respond and recover, and the potential for data loss. The assessment also covers other malware, analysis of endpoint protection measures, and recommendations. During the execution of the other components above, we will gather information about endpoint protection, backup procedures, disaster recovery, testing of backups and disaster recovery processes, incident response, etc. Based on the information collected, Illumant performs analysis and prepares a dedicated report on susceptibility to ransomware attacks, potential impact, and recommendation for improvement, along with the same for other malware threats.
	Scope: The RansomSA uses information gathered through the above components

After completion of the assessment and analysis, a report will be prepared that contains summary information, graphical data, and detailed technical analysis along with action items to facilitate remediation. Before any final deliverables are

submitted Illumant will engage key The County team members to review draft reports and to discuss results and incorporate relevant feedback and context into the report. This hands-on process will allow the organization to derive the maximum value from the assessment and associated report and ensures that all concerns are addressed appropriately.

Methodology

This section presents in more detail the methodology we employ for each of our services. Additionally, it lists the information and access we will need to be able to effectively perform the work.

Risk Assessment/Strategic Planning (RA)

Description

Combination of qualitative and quantitative analysis to determine the top threats to information security, biggest vulnerabilities, and largest opportunities for risk reduction through cost-benefit analysis.

Highlights

- **Top down risk assessment**
- Inventory of **critical assets**
- **Review and development of staffing model**
- Identification and severity of **vulnerabilities**
- Enumeration of **threats**
- **Calculation** of **risk**
- Risk factors
  - **Confidentiality**
  - **Integrity**
  - **Availability**
- **Cost-benefit** analysis of risk **remediation** efforts

Targets

- Sensitive data
  - Customer data
  - ePHI
  - Financial info
  - SSNs
  - CCNs
- Critical systems
  - Servers
  - Applications
  - Databases
  - Laptops
  - Desktops
  - USBs, DVDs, etc.

Methodology

Data gathering:

- Client provides relevant compliance requirements along with time slots for interviews and all relevant documentation
- Illumant interview IT personnel and risk assessment stakeholders about:
  - Assets: Illumant identifies the sensitive data at the organization including ePHI, CCNs, SSNs, customer data, financial information, IP to learn where it resides, how it is received and transmitted, how it is processed, and which systems are involved
  - Controls/vulnerabilities: Controls are discussed in terms of which are in place, how mature they are, and which control gaps exist (vulnerabilities)

Analysis:

- Identify and Document Potential Threats and Vulnerabilities

  As part of the risk assessment process, organizations must identify and document reasonably anticipated threats to sensitive data. Illumant risk assessment methodology includes a threat model that includes the following:
  - Natural threats such as floods, earthquakes, tornadoes, and landslides.
  - Human threats are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to sensitive data) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
  - Environmental threats such as power failures, pollution, chemicals, and liquid leakage.

  Illumant will review these threats with the organization in the context of their assets and infrastructure to determine the extent to which the organization could be subject to impact by these threats.

  As part of Illumant's model, we have identified vulnerabilities that could be triggered or exploited by the threats above to create a risk of inappropriate access to or disclosure of sensitive data. Illumant will explore the presence of these vulnerabilities with

the organization to determine how threats to sensitive data are augmented by any vulnerabilities that have been identified at the organization.

- Assess Current Security Measures
  Illumant will perform an evaluation of the security measures addressed/implemented at the organization that may help to reduce risk to inappropriate disclosure of sensitive data.
- Determine the Likelihood of Threat Occurrence
  Based on the evaluation of threats coupled with vulnerability information and security measures, Illumant's security model provides data for analysis of the likelihood of threat occurrence for each threat identified. Quantitative risk assessment techniques are used in the model, and every threat/vulnerability pair is considered and ranked from most to least likely.
- Determine the Potential Impact of Threat Occurrence
  Using the likelihood information generated above, and the inventory of sensitive data assets gathered in the first phase, Illumant will generate an analysis of the potential impact on the organization of each possibly threat/vulnerability/asset triplet from a criticality standpoint.
  For instance, a high-likelihood threat triggering or exploiting an existing vulnerability, that is unmitigated by existing security measures, and targeting a system with a high concentration of sensitive data would be considered extremely critical. Whereas, if the threat or risk were mitigated by the presence of security measures, this would lower the criticality rating of the impact of the threat.
- Determine the Level of Risk
  By comparing and aggregating the impacts of threat occurrence above, our model provides an overall risk analysis for the entity in terms of criticality.
- Most importantly, however, this analysis provides a list of corrective, or risk mitigating actions that can be taken to reduce risk. These corrective actions are prioritized by cost-benefit to describe which actions provide the maximum risk mitigation relative to the effort or cost.

Reporting:

- The findings of the risk assessment, including the details of the inputs, outputs and analysis of each step above will be documented in a final report.
- A summary section at the beginning of the report provides a management-consumable analysis of our findings and highlights any issues identified during the process of risk analysis.
- The report includes specific remediation recommendations prioritized by cost-benefit.

Tools
Proprietary analytical risk assessment model and questionnaires

Notes
While the Risk Assessment can be performed entirely independently, it also complements technical and other organizational assessments, by refining the analysis with findings from other reports.

Security Technology Architecture & Roadmap Review (STARR)

Description

Illumant will review current IT/security technologies, including capabilities and load to develop a security technology roadmap to meet strategic planning initiatives and security goals.

Highlights

- Review **current technologies**
  - Assess **security capabilities**
  - Compare against goals
- Develop **Security Technology Roadmap**
  - incorporate **strategic plan**
  - Incorporate **RA/Gap analysis**

Targets

- Current technologies
- Capabilities
- Capacity/utilization
- Future technology requirements for
  - Security goals
  - Strategic plan

Methodology

Illumant will perform the following to create the Security Technology Roadmap:

- Review security goals and strategic plan from the Risk Assessment to identify the areas that are expected to grow in the future. Consider any planned expansion.
- Identify technologies within the organization that are out of date, or otherwise not meeting security goals, strategic planning initiatives, or best practices.
- Identify the critical technologies needed to operate the business and meet security goals and strategic planning initiatives.
- Identify the appropriate vendor pools needed to achieve security goals within growth estimates.
- Prioritize the transitioning from out of date or insufficient technologies to the technologies identified in earlier steps based on risk and cost/benefit analysis.

Tools
Risk Assessment and gap analysis

Notes
The Security Technology Roadmap will leverage the interview and analysis performed during the risk assessment and gap analysis

Policies Procedures and Practices Assessment (PPPA)

Description

Ensures that documented IT policies and procedures, and associated practices, are aligned with best-practices and applicable regulatory requirements. Includes interviews with IT personnel and documentation review.

Highlights

- **Policies** and **procedures** review
- **Practices** review
- **Gap analysis** vs **best-practices/regulatory** requirements
- IT **interviews**
- **Documentation** reviews

Targets

- IT and security policies and procedures documentation
- De facto practices
- Access controls
- Breach response
- Change management
- Operational controls
- Technical controls
- Compliance

Methodology

Data gathering:

- Client informs Illumant of any relevant compliance requirements
- Client identifies stakeholders along with time slots for interviews
- Client provides all relevant documentation pertaining to IT and security policies and procedures, or any other documentation that governs information handling at the organization

Analysis:

- Illumant reviews the provided documentation and compares them with best-practices and regulatory requirements
- Illumant interviews IT personnel and risk assessment stakeholders about de facto IT and security practices at the organization to see how they compare to the documentation (if any)
- Illumant analyzes interview and documentation review results in terms and how they address the following security domains:
  - Access control – passwords, rotation, complexity, 2-factor, etc.
  - Change management – patch management, change control, segregation of duties, sand-boxes, etc.
  - Operations – log monitoring, incident response, incident handling, back-ups, etc.
  - Technical controls – Data loss prevention, intrusion detection/prevention systems, proxies, anti-virus, etc.

- Assessments – risk assessment, penetration testing, vulnerability assessment
- Organizational – security awareness training, acceptable use, background checks, etc.

- Illumant maps gaps and recommendations to relevant regulatory requirements such as HIPAA/HITECH, PCI, GLBA, FISMA, NIST 800-53, ISO27001, CIPv5, SOC 2/SAS 70/SSAE 16 etc.

Reporting:

- The PPPA report provides an overall maturity rating for the organization with respect to documentation and practices.
- Maturity rating are provide for the documentation and practices for each domain, as well.
- Illumant identifies all gaps between best-practices and regulatory requirements and provides recommendation for remediation
- Separate gap analysis appendices are provided for 1-to-1 mapping of gaps to regulatory requirements.

Tools
Regulatory guidance, checklists, questionnaires

Notes
Stakeholders include IT department leadership, but may also involve cross-departmental participation, as well

Blind Visibility & Exposure Analysis (BVEA)

Description

Blind Internet footprint analysis to ensure that only the information and systems needed for business purposes are exposed to the Internet. Recommendations are provided to minimize cyber-attack surface.

Highlights

- **Blind reconnaissance**
- Internet **footprint** analysis to describe/help minimize **cyber-attack surface**
- **Reputation** analysis
- **Black lists** and **bot lists** review
- **Chat**, **forum** and **deep web** searches
- Network **redundancy** analysis
- **Domain** ownership review
- **Exposure rating**
- Remediation **recommendations**

Targets

- Footprint/Internet-facing systems:
  - Networks
  - Web sites and applications
  - Servers, router, firewalls, etc.
- Chatter and sensitive info
  - Forums (tech support, etc.)
  - Chat rooms/IRC, dark web
- Public Internet information databases
  - Name servers, information aggregators
- Reputation databases
  Black lists, bot lists, web reputation sites

Methodology

Network and systems enumeration:

- Blind analysis - Illumant uses only the name of the company as a starting point
- Web searches and recursive spidering of web sites to identify related sub-organizations, domains and sub-domains
- Search of Internet-information and domain registration databases to identify netblocks and domain ownership – review for proper configuration, redundancy, ownership records
- Inventory of exposed sites and services

Sensitive information searches:

- Review of organizational sites, servers, tech support forums and other chat rooms to identify sensitive technical and organizational data that is sensitive, or could be useful in crafting a cyber-attack
- Dark web, IRC and hacker chatroom and forum searches to identify evidence of planned or successful attacks or intrusions against the organization

Reputation analysis or bot list/black list review

- Review of black lists and web reputation sites as an indicator of infection by malware
- Review of bot net lists as indicator of potential infection by bots or trojans

Reporting:

- Findings are described in the report including full technical details of each exposure or sub-optimal configuration.
- Recommendations are provided to reduce exposures and minimize the cyber-attack surface without compromising organizational effectiveness
- Findings are summarized to provide a high-level overview of the organization's footprint and exposures. Ratings are benchmarked against thousands of previous assessments.

Internet Information Databases
ARIN, InterNIC, APNIC, RIPE NCC, LACNIC, AfriNIC, IANA, Robtex, Who.is

Tools
Web crawlers/spiders, whois, NMAP, IRC search engines, forum search engines, blacklists, reputation lists, botnet lists

Notes
The BVEA is performed blind with only the company name as a starting point, to mimic what a hacker would see during a malicious reconnaissance exercise.

Perimeter Security Assessment & Penetration Testing (PSA)

Description

External vulnerability assessment, manual validation and penetration testing of Internet facing networks, systems, sites and applications (aka the hacker's perspective). Includes identification, manual validation and benign exploitation of vulnerabilities, along with actionable remediation recommendations for improved security.

Highlights

- **Scanning** to create a **baseline** of **vulnerabilities** and security risks
- Testing can be performed **overtly** or **covertly** (w or w/o informing IT and security personnel)
- **Best-of-breed** open source and commercial **vulnerability harvesting tools**
    - A cross section is used to limit exposure to the limitations of any single tool, and reap the benefits the strengths each tool provides
- **Manual validation** to eliminate **false positives**, confirm findings
- **Manual testing** to find additional vulnerabilities not found by scanning tools
- **Penetration testing** through custom-designed and pre-existing **exploits** to test real severity
    - Illumant's pen testing and manual testing techniques are continually updated through research and participation in hacker forums and conferences (e.g. BlackHat, DEFCON, SANS)
- Classification of **severity** of findings
- **Remediation** recommendations
- **Benchmark** analysis of results vs industry
- **Retesting** (within 6 months of initial test)

Targets

- Internet-facing networks, systems, applications, services, ports, protocols:
- Web sites
- Web applications (non-credentialed testing)
    - For credentialed testing see Web Application Security Assessment (WASA)
- Servers
- VPNs
- Firewalls
- Border routers
- Internet-facing services (FTP, Telnet, SSH, and many more)
- 100,000+ known vulnerabilities, client-specific vulnerabilities in custom applications, configurations and software

Methodology

Scoping:
- Illumant provides scoping worksheets
- Client provides in-scope target networks, system IPs, URLs
- Testing can be information with or without informing other IT or security personnel (overtly or covertly) to test response protocols and readiness.

Enumeration/Recon:
- Port mapping (ping sweeps, connection sweeps and malformed packet sweeps) to identify target services and applications, systems, versions, and OS guesses
- Manual review of IPs, ports, URLs, to refine information about in scope target systems including function, manufacturer, OS, applications, services, and their respective versions

Vulnerability Analysis/Harvesting:
- Automated scanning of in scope target networks, systems and applications using best-of-breed commercial and open-source tools and scripts
- Multiple tools are used to provide the widest possible initial baseline for additional analysis and limit exposure to the limitations of any single tool
- 100,000+ vulnerabilities are analyzed, including all known vulnerabilities across open source vulnerability databases and commercially maintained vulnerability databases

Manual validation and manual testing:
- Expert manual review of vulnerabilities identified to confirm validity of identified vulnerabilities and discard false positives
- Additional expert manual testing to identify vulnerabilities not detected by automated scanners, often due to custom configuration, custom designs, custom applications, and use of purpose-built scripts

Penetration testing and exploitation:
- Illumant identifies and attempts all known exploits against confirmed vulnerabilities. These are limited to exploits that are non-destructive (will not corrupt data or configurations, will not cause availability issues).
- Illumant attempts to craft custom exploits targeting custom designs, custom configurations, as well as custom on off-the shelf applications

Findings:
- PSA findings include: CGI abuses, buffer overflows, default credentials, malware sweeps, SQL injection, URL injection, CSRF injection, directory traversal, auth vulnerabilities, AJAX vulnerabilities, backdoors, trojans, viruses, insecure direct object references, security misconfiguration, sensitive data exposure, missing function level access control, buffer overflows, missing patches, vulnerable versions and many more

Reporting:
- Findings are described in the report including full technical details of each vulnerability and exploit.
- Findings are summarized to provide a high-level overview of the security posture and security rating of the target systems.
- Ratings are benchmarked against thousands of previous assessments.

Vulnerability Databases
Mitre.org CVE, CERT, OSVDB, Security Focus Bugtraq, NVD, Rapid7, OWASP

Tools
Qualys, Nessus, NeXpose, Saint, Metasploit, ZAP, NTO Spider, Burp Suite, Nikto

Notes
Internet-facing web applications are tested as part of this test without credentials. For full credentialed application testing (gray box testing), see the Web Application Security Assessment (WASA).

Critical Asset Security Assessment (CASA)

Description

Internal, unfiltered vulnerability analysis and penetration testing of mission-critical applications, systems and networks for validation of layered-security and defense in depth.

Highlights

- **Scanning** to create a **baseline** of **vulnerabilities** and security risks
- **Best-of-breed** open source and commercial **vulnerability harvesting tools**
  - A cross section is used to limit exposure to the limitations of any single tool, and reap the benefits the strengths each tool provides
- **Manual validation** to eliminate **false positives**, confirm findings
- **Manual testing** to find additional vulnerabilities not found by scanning tools
- **Penetration testing** through custom-designed and pre-existing **exploits** to test real severity
  - Illumant's pen testing and manual testing techniques are continually updated through research and participation in hacker forums and conferences (e.g. BlackHat, DEFCON, SANS)
- Classification of **severity** of findings
- **Remediation** recommendations
- **Benchmark** analysis of results vs industry

Targets

- Internal networks, systems, applications, services, ports, protocols:
- Web sites
- Web applications (non-credentialed testing)
  - For credentialed testing see Web Application Security Assessment (WASA)
- Servers
- VPNs
- Firewalls
- Border routers
- 100,000+ known vulnerabilities, unique vulnerabilities from custom designs, configurations and software

Methodology

Scoping:

- Illumant provides scoping worksheets
- Client provides in-scope target networks, system IPs, URLs

Enumeration/Recon:

- Port mapping (ping sweeps, connection sweeps and malformed packet sweeps) to identify target services and applications, systems, versions, and OS guesses
- Manual review of IPs, ports, and URLs to refine information about in scope target systems including function, manufacturer, OS, applications, services, and their respective versions

Vulnerability Analysis/Harvesting:

- Automated scanning of in scope target networks, systems and applications using best-of-breed commercial and open-source tools and scripts
- Multiple tools are used to provide the widest possible initial baseline for additional analysis and limit exposure to the limitations of any single tool
- 100,000+ vulnerabilities are analyzed, including all known vulnerabilities across open source vulnerability databases and commercially maintained vulnerability databases

Manual validation and manual testing:

- Expert manual review of vulnerabilities identified to confirm validity of identified vulnerabilities and discard false positives
- Additional expert manual testing to identify vulnerabilities not detected by automated scanners, often due to custom configuration, custom designs, custom applications, and use of purpose-built scripts

Penetration testing and exploitation:

- Illumant identifies and attempts all known exploits against confirmed vulnerabilities. These are limited to exploits that are non-destructive (will not corrupt data or configurations, will not cause availability issues).
- Illumant attempts to craft custom exploits targeting custom designs, custom configurations, as well as custom on off-the shelf applications

Findings:

- CASA findings include: CGI abuses, buffer overflows, default credentials, malware sweeps, SQL injection, URL injection, CSRF injection, directory traversal, auth vulnerabilities, AJAX vulnerabilities, backdoors, trojans, viruses, insecure direct object

references, security misconfiguration, sensitive data exposure, missing function level access control, buffer overflows, missing patches, vulnerable versions and many more

Reporting:

- Findings are described in the report including full technical details of each vulnerability and exploit.
- Findings are summarized to provide a high-level overview of the security posture and security rating of the target systems. Ratings are benchmarked against thousands of previous assessments.

Vulnerability Databases
Mitre.org CVE, CERT, OSVDB, Security Focus Bugtraq, NVD, Rapid7, OWASP

Tools
Qualys, Nessus, NeXpose, Saint, Metasploit, ZAP, NTO Spider, Burp Suite

Notes
Testing for the CASA is performed without credentials to test susceptibility to attack propagation by outside attackers, or insiders with lower privileges or without authorization. For credentialed testing of applications see our WASA (Web applications). For credentialed testing of other critical assets see our platform-specific reviews, e.g.: MSSA (Microsoft servers), NixSA (UNIX/Linux servers), ADSA (Active Directory), etc. For credentialed testing of the user computing environment, see our LAN Security Assessment (LANSA). These other credentialed tests include full reporting on patch levels.

LAN Security Assessment (LANSA)

Description

Internal, unfiltered vulnerability analysis and penetration testing of desktops, laptops and other LAN-based systems for validation of end-user computing system security.

Highlights

- **Scanning** to create a **baseline** of **vulnerabilities** and security risks
- **Best-of-breed** open source and commercial **vulnerability harvesting tools**
  - A cross section is used to limit exposure to the limitations of any single tool, and reap the benefits the strengths each tool provides
- **Manual validation** to eliminate **false positives**, confirm findings
- **Manual testing** to find additional vulnerabilities not found by scanning tools
- **Penetration testing** through custom-designed and pre-existing **exploits** to test real severity
  - Illumant's pen testing and manual testing techniques are continually updated through research and participation in hacker forums and conferences (e.g. BlackHat, DEFCON, SANS)
- Classification of **severity** of findings
- **Remediation** recommendations
- **Benchmark** analysis of results vs industry

Targets

- LANs, desktops, workstations, laptops, printers, LAN devices, applications, services, ports, protocols from within firewalls boundaries – unfiltered analysis:
  - Desktops
  - Workstations
  - Laptops
  - LAN servers
  - Switches
  - Printers
  - Other LAN Devices
- 100,000+ known vulnerabilities, unique vulnerabilities from custom designs, configurations and software

Methodology

Scoping:
- Illumant provides scoping worksheets
- Client provides in-scope target networks, system IPs, URLs

Enumeration/Recon:
- Port mapping (ping sweeps, connection sweeps and malformed packet sweeps) to identify target services and applications, systems, versions, and OS guesses
- Manual review of IPs, ports, URLs, to refine information about in scope target systems including function, manufacturer, OS, applications, services, and their respective versions

Vulnerability Analysis/Harvesting:
- Automated scanning of in scope target networks, systems and applications using best-of-breed commercial and open-source tools and scripts
- Credentialed testing of desktops, laptops and work stations to validate OS and application versions, and missing patches.
- Multiple tools are used to provide the widest possible initial baseline for additional analysis
- 100,000+ vulnerabilities are analyzed, including all known vulnerabilities across open source vulnerability databases and commercially maintained vulnerability databases
- End-user system vulnerabilities include: Default credentials, malware sweeps, security misconfiguration, sensitive data exposure, backdoors, trojans, viruses, vulnerable applications, out-of-date OSs, missing patches, and many more.
- For LAN servers and other devices vulnerabilities tested may also include: CGI abuses, buffer overflows, default credentials, SQL injection, URL injection, CSRF injection, directory traversal, AJAX vulnerabilities, insecure direct object references, missing function level access control, buffer overflows, etc.

Manual validation and manual testing:
- Expert manual review of vulnerabilities identified to confirm validity of identified vulnerabilities and discard false positives
- Additional expert manual testing to identify vulnerabilities not detected by automated scanners due to custom configuration, custom designs and custom applications using purpose-built scripts

Penetration testing and exploitation:
- Illumant identifies and attempts all known exploits against confirmed vulnerabilities. These are limited to exploits that are non-destructive (will not corrupt data or configurations, will not cause availability issues).
- Illumant attempts to craft custom exploits targeting custom designs, custom configurations, as well as custom on off-the shelf applications

Reporting:
- Findings are described in the report including full technical details of each vulnerability and exploit.
- Findings are summarized to provide a high-level overview of the security posture and security rating of the target systems. Ratings are benchmarked against thousands of previous assessments.

Vulnerability Databases
Mitre.org CVE, CERT, OSVDB, Security Focus Bugtraq, NVD, Rapid7, OWASP

Tools
Qualys, Nessus, NeXpose, Saint, Metasploit, ZAP, NTO Spider, Burp Suite

Notes
LAN-based systems may be numerous. Illumant specifies vulnerabilities that affect all or most systems, and calls out exceptionally vulnerable outliers, as well.
Testing of end-user systems is performed with credentials to evaluate the security within the end-user's context including patch-levels, vulnerable applications and out-of-date OSs.

Social Engineering (Soc Eng)

Description

Beyond just phishing, targets the human element through multiple attack vectors to test awareness of users to potential security threats, by performing simulated phishing, planted media, pretext calling, and social networking attacks.

Highlights	Targets
• **Social engineering** • **Simulated** attacks • **Phishing** • **Planted media** (mail, **USB-drops**, etc.) • **Pretext calling** • **Social networking** • **Tailgating** (optional) • Security **awareness** • Comparison to **baseline** of similar organizations	• Employees • Users • Managers • Departments (HR, finance, administration, customer service/support, engineering, …) • Knowledgeability about security • Awareness of security threats

Methodology

Scoping:

- Illumant gathers preliminary target list through blind enumeration on Internet (demonstrates exposure to targeted phishing)
- Illumant provide simulated attack vector scenarios with assigned targets for final review
- Client vets target list to remove sensitive personnel, and supplies additional targets as desired. Client approves simulated attack vectors

Testing:

- Illumant runs simulated attack vectors against targets per the scoping phase above
- Full response data is collected including which targets responded and all sensitive data and access that was provided as a result

Simulated attack vectors

- Phishing
  - An email is sent which is intended to deceive the target by coaxing them into following a link or opening an attachment. The link may lead to a fake page that looks legitimate which prompts the target to provide sensitive info (e.g. credentials), or may launch benign malware to simulate how an infection might be spread. Similarly an attachment when opened may deliver this benign malware as well.
  - Examples: Fake IT person sends link to fake webmail site to gather username/password, fake internship seeker sends resume which launches benign malware
- Pretext Calling
  - A phone call is placed to a target. The call script is designed to emulate a real scenario, for instance to impersonate a real caller/client, or otherwise create a compelling reason for the target to divulge sensitive info, including client data, passwords, or other sensitive info.
  - Examples: Fake client asking for info, fake IT person asking for system/password info, fake vendor asking for sensitive info
- Social Networking
  - A profile for a user is created on a social network (e.g. LinkedIn) that purports that the users belongs to the target company or a vendor of the target company. The fake profile asks for connections to the target company and then sends a message request info or requesting that they follow a link which acts like the phishing attack above
  - Examples: Fake IT manager profile for target company asks for uses to log into a fake test site to gather usernames and passwords, fake vendor profile asks for target to share info about phone or IT systems
- Planted Media
  - CDs or USBs are planted or emailed to the employees at the target company enticing the user to insert/open the media and files within. When opened, malware is launched which provides access to the employee's computer.
  - Examples: USB in parking lot contains fake salary info and when opened launches malware, CD in mail contains regulatory info for review and when opened launches malware
- Physical Security / Tailgating (optional)
  - Facilities and properties are visited
  - Attempts are made to tailgate into offices and sensitive areas,
  - Impersonation of delivery personnel or visitors, contractors, etc. is used to attempt gain unauthorized access
  - Attempts are made to identify / access unlocked or unsupervised entries

Reporting:

- All responses to simulated attacks or tracked including each target's responses, the information divulged, or the level of access provided
- Findings are summarized to provide a high-level overview of the security posture and security rating of the target systems. Ratings are benchmarked against thousands of previous assessments.

Tools
Call scripts, phishing templates, pseudo-malware (non-destructive, memory-only script that simulates malware and informs Illumant when documents are opened).

Notes
An organization may wish to test all employees or a representative sample

Wireless Security Assessment (WSA)

Description

Ensures protection against unauthorized access to wireless networks and traffic, as well as segregation of guest access from corporate networks and systems. Also identifies potential back-doors through rogue access points.

Highlights

- Enumeration of all **active SSIDs**
- Evaluation of **auth/encryption strength** for authorized wireless networks
- Assessment of **isolation of guest wireless**
- Enumeration of vulnerabilities with wireless infrastructure
- Review of **guest/user wireless** account provisioning protocols
- Identification **of rogue access points**
- Evaluation of access achievable through rogue wireless
- **Remediation recommendations**

Targets

- Authorized employee wireless networks
- Guest wireless networks/supporting infrastructure
- Special purpose wireless networks
- Point-to-point wireless networks
- Auth/encryption protocol/implementation vulnerabilities
- Network segregation issue
- Rogue access points/networks

Methodology

Scoping:
- Client provides in-scope target facilities and enumerates authorized employee, special purpose, and guest wireless networks
- Client provides credentials for accessing guest wireless
- Testing may be performed on-site and in person, or remotely via testing laptop

Enumeration:
- Illumant uses specialty wireless adapters for broadest spectrum for analysis of wireless networks, including workstation networks and point-to-point networks
- Best-of-breed wireless scanners are used to enumerate SSIDs
- Results are compared against list of authorized networks
- Neighbors networks are excluded through supplementary information and signal strength analysis

Security Analysis:
- Illumant reviews the authentication and encryption protocols of authorized networks through packet data analysis and compares them against best practices noting weaknesses.
- Illumant looks at security at various of stages: post-association, pre-authentication, and post-authentication including vulnerability analysis of supporting systems (e.g. DHCP, DNS, gateways, routers, access points, auth servers, etc.)
- Isolation of guest networks from internal resources is tested to confirm proper network segregation.
- Rogue devices are accessed when possible to test the level of exposure

Reporting:
- Findings are described in the report including full technical details of each vulnerability and exploit.

- Findings are summarized to provide a high-level overview of the security posture

Tools
CommView for WiFi, Vistumbler, InSSIDer, Kismet, NMAP, Nessus, Orinoco ABGN adapter, laptop with virtual wireless test environment

Notes
The WSA may be performed on-site or off-site via remote access to testing laptop. The latter saves on the cost of service. Remote testing may require relocation of the laptop during testing.

Physical Security Assessment (PhySA)

Description

Assessment of facilities and properties to analyze the key security measures that govern physical security that are required to control access to buildings and to protect the people and data within them.

Highlights

- **Physical security** assessment
- Review of **facilities** and **properties**
- Assessment of key **physical security measures**
- Walkthroughs of:
  - Property and facility **perimeters**
  - Review of **ingress** and **egress** points
  - Inspection of **reception**/**receiving** areas
  - Review of **badging** protocols
  - Review room/**data center access**

Targets

- Ingress/egress point access controls, alarms, locks
- badging and pass requirements
- receptionist, guard positioning/duties
- perimeter fencing
- patrolling/camera placement/lighting for monitoring

Methodology

Our Physical Security Assessment (PhySA) targets facilities and properties to analyze the key aspects that govern physical security and that are required to control access to buildings and to protect the people and data within them.

During an on-site assessment, our consultants perform physical inspections of facilities and security operations. The assessment includes an interview with relevant physical security personnel and a review of physical security policies and procedures to gain an understanding of the assets at risk, threats to these assets, and the security measure in place to mitigate these threats.

We review access controls at all egress and ingress points, including badging/pass protocols, guest access procedures, and reception/guard control, alarm systems, camera placement, lighting and patrol routes. We also review the adequacy of perimeter barriers (if applicable)
Key features include:

- Review ingress/egress point access controls, alarms, locks
- Review of badging and pass requirements
- Review of receptionist, guard positioning/duties
- Review of perimeter fencing
- Review of patrolling/camera placement/lighting for monitoring

Tools
Checklists

Notes
Physical security is the first line of defense against intruders that may wish to attack networks/data from within

Reports

The findings are compiled into confidential reports with both executive and technical summaries, as well as comprehensive actionable recommendations. In addition, we provide full technical details concerning vulnerabilities and other findings. Remediation advice is presented for the vulnerabilities that are uncovered. An "Action Items" list is generated and additional recommendations for enhancing security and efficiency are presented.

Illumant's security team will formally present the highlights of the report to The County. The presentation will contain both an executive-level overview and technical details of the state of the organization's networks. The meeting or conference call will provide an opportunity to discuss the findings in detail, as well as to discuss remediation options with Illumant's Expert Security Analysts.

Organization

Illumant has the capacity and flexibility to meet schedules, including unexpected work. We operate with lead time, but reserve additional bandwidth based on RFP bidding. We frequently receive requests for aggressive timelines which we deliver under. Our testing load is constant with multiple concurrent clients, and deadlines are consistently met.

For hourly work, Illumant can build in not to exceeds, stop/check intervals to gauge budget utilization, and uses periodic meetings to ensure projects remain on track and hours intensive issues are forecasted and mitigated in advance.

Project Schedule (Sample)

The following is a sample schedule. Illumant is a flexible security partner and may condense some of these timelines upon request. It is our intent to conduct multiple assessment components concurrently to maximize the efficiency of our assessment.

Service	Start Date	End Date	On-site/Off-site
Project Kickoff Mtg.		Monday, November 1, 2021	
EXTERNAL			
BVEA	Monday, November 1, 2021	Monday, November 8, 2021	Off-site
Deliverable (Draft)		Tuesday, November 16, 2021	
PSA	Monday, November 8, 2021	Monday, November 22, 2021	Off-site
Deliverable (Draft)		Sunday, November 28, 2021	
Soc Eng	Monday, November 1, 2021	Monday, January 3, 2022	Off-site
Deliverable (Draft)		Tuesday, January 11, 2022	
WASA	Monday, November 22, 2021	Wednesday, December 22, 2021	On-/Off-site(VPN)
Deliverable (Draft)		Tuesday, December 28, 2021	
PhySA	Monday, November 22, 2021	Friday, December 10, 2021	On-site
Deliverable (Draft)		Wednesday, December 15, 2021	
INTERNAL			
CASA+LANSA	Monday, January 3, 2022	Tuesday, January 18, 2022	On-site/Off-site
Deliverable (Draft)		Tuesday, January 25, 2022	
WSA	Monday, January 3, 2022	Tuesday, January 18, 2022	On-/Off-site(VPN)
Deliverable (Draft)		Tuesday, January 25, 2022	
ADSA	Monday, January 3, 2022	Tuesday, January 18, 2022	On-/Off-site(VPN)
Deliverable (Draft)		Tuesday, January 25, 2022	
Organizational			
RA	Monday, November 1, 2021	Wednesday, December 15, 2021	On-/Off-site
Deliverable (Draft)		Monday, December 20, 2021	
PPPA	Monday, November 1, 2021	Wednesday, December 15, 2021	On-/Off-site
Deliverable (Draft)		Monday, December 20, 2021	
STARR	Monday, November 1, 2021	Wednesday, December 15, 2021	On-/Off-site
Deliverable (Draft)		Monday, December 20, 2021	
Other			
RansomSA	Wednesday, December 15, 2021	Wednesday, December 22, 2021	On-/Off-site(VPN)
Deliverable (Draft)		Monday, January 3, 2022	
Final Assessment Deliverables		Monday, January 10, 2022	
WISP	Monday, January 10, 2022	Thursday, March 10, 2022	On-/Off-site(VPN)
Documentation Deliverable		Tuesday, March 15, 2022	

Section 4: Proposed Pricing

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "J"

PRICING PROPOSAL FORM

Each Respondent shall submit a Total Price for Cybersecurity Assessments for both the BCC and Clerk locations as indicated below. These prices shall remain firm throughout the duration of the Contract. Please enter the amount for each pickup in numerals and in words. In the event of a discrepancy between the amounts, the amount written in words shall be used as the correct bid price.

Total Price for Cybersecurity Assessment(s):

Item 1 Cybersecurity Assessment for BCC

Item 1: $ 91,968.75 (Amount in numerals)
Ninty one thousand, nine hundred and sixty eight dollars and seventy five cents. (Amount in words)

Item 2 Cybersecurity Assessment for Clerk

Item 2: $ 30,656.25 (Amount in numerals)
Thirty thousand, six hundred and fifty six dollars and twenty five cents (Amount in words)

Respondents shall type or legibly print the Total Price for each item in both numerals and words. If the County is unable to determine the proposed amount due to illegibility, the proposal may be removed from consideration for award.

Our fees are based on our consultants' level of experience and skill and the time and effort required to complete the assessment. The following section shows our rates for each project component. These rates exclude travel and out-of-pocket expenses.

All services are offered a la carte. Illumant performs our work at one flat rate, inclusive of reporting, planning, and project management efforts.

Division of Labor and Cost

Cyber Security Assessment Services	Hours	Rate/Hr.	Fees
Risk Assessment (RA) Up to 8 Interviews with IT personnel, questionnaire	40	$ 225	$ 9,000
Security Technology Architecture & Roadmap Review (STARR) Up to 8 Interviews with IT personnel, questionnaire	50	$ 225	$ 11,250
Policies Procedures and Practices Assessment (PPPA) Up to 8 Interviews, documentation review.	40	$ 225	$ 9,000
Blind Visibility and Exposure Analysis (BVEA) No assistance from client required	20	$ 225	$ 4,500
Perimeter Security Assessment (PSA) Up to 80 externally accessible systems	40	$ 225	$ 9,000
Critical Asset and LAN Security Assessment (CASA+LANSA) No Up to 3,200 internal workstations, servers, and infrastructure devices	100	$ 225	$ 22,500
Wireless Security Assessment (WSA) A representative sample of SSIDs and locations (2 SSIDs at a single location)	25	$ 225	$ 5,625
Social Engineering Assessment (Soc Eng) A representative sample of users will be chosen with the County	30	$ 225	$ 6,750
Physical Security Assessment (PhySA) Up to 2 locations on one campus	25	$ 225	$ 5,625
Web Application Security Assessment (WASA) Application testing with and without credentials	80	$ 225	$ 18,000
Active Directory Security Assessment (ADSA) Up to 4 domains	30	$ 225	$ 6,750
Ransomware Security Assessment (RansomSA) This is available for free with the purchase of a Risk Assessment and the Critical Asset and LAN Security Assessment	N/A	$ 0	$ 0
Average Total	480	$ 225	$ 108,000
Additional, Post Assessment Services	**Hours**	**Rate/Hr.**	**Fees**
Written Information Security Program Development (WISP) Controls matrix, IT policies and procedures, handbook	65	$ 225	$ 14,625
Grand Total	**650**	**$ 225**	**$ 122,625**

Free differential assessments are provided (for PSAs only) within 6 months of each initial assessment. This acts as a follow up to validate remediation efforts. Any new vulnerabilities detected during the differential assessment will also be reported.

Payment Terms

For fixed fee engagements:

A 30% retainer fee is due at the start of the engagement. A milestone payment of 50% is due upon completion of draft results. The remaining 20% is due upon delivery of the final reports. With the exception of the retainer, payments are due Net 10 days from the invoice date. Fees do not include travel and expenses.

A discount of 20% (the amount of the final payment) is offered for each service component for which a three-year contract is selected. This discount is available up until receipt of the final payment for the project. This provides the opportunity to review final deliverables before committing to a 3-year term.

For hourly services:

Fees will be billed bi-weekly on a time and materials basis payments are due Net 10 days from the invoice date. Fees do not include travel and expenses.

Section 5: References & Technical Experience

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "I"

REFERENCES & TECHNICAL EXPERIENCE

In this section, Respondents shall submit information on three (3) contracts and/or engagements successfully completed in the last five (5) calendar years of similar scope to the outline scope of services described herein. Respondents must include the type of services performed, timeframe of performance, whether or not the contract was renewed/extended, and all contact information for a point of contact at the reference agency or organization.

1. Company Name: Travis County Healthcare District (TCHD)
   Date(s) of Service: 2/25/2019-12/13/2019
   Information (Type of Service): Comprehensive technical and organizational security assessment. HIPAA primary focus,
   Primary Contact Name and Title: Marta Williams, Joint Tech Team Project Liaison
   Contact Phone Number: 512.633.9202
   Contact Email Address: marta.williams@centralhealth.net

2. Company Name: Travis County
   Date(s) of Service: 6/8/2020-11/23/2020
   Information (Type of Service): Comprehensive technical and organizational security assessment. HIPAA primary focus,
   Primary Contact Name and Title: Monisha Perryman, HIPAA Compliance & Privacy Officer
   Contact Phone Number: 512-854-6278
   Contact Email Address: monisha.perryman@traviscountytx.gov

3. Company Name: Collier County, Florida
   Date(s) of Service: Ongoing. 9/2/19-10/4/19, 10/12/20-11/15/20
   Information (Type of Service): Comprehensive technical and organizational security assessment.
   Primary Contact Name and Title: Neil Randall, Senior Network Administrator - IT Security
   Contact Phone Number: 239.252.6082
   Contact Email Address: Neil.Randall@Colliercountyfl.gov

4. Company Name: Collier County Clerk of the Circuit Court & Comptroller
   Date(s) of Service: 8/23/18-9/17/18, 5/4/2020-6/1/2020, 8/9/21-10/6/21
   Information (Type of Service): Comprehensive technical and organizational security assessment.
   Primary Contact Name and Title: Marc Tougas, Director, MIS
   Contact Phone Number: 239-252-8822
   Contact Email Address: Marc.Tougas@CollierClerk.com

5. Company Name: City of Oakland
   Date(s) of Service: Ongoing. 12/2/2020 start.
   Information (Type of Service): Comprehensive technical and organizational security assessment.
   Primary Contact Name and Title: Kevin Fong, Acting CIO
   Contact Phone Number: (510) 238-3118
   Contact Email Address: kfong@oaklandca.gov

Similar, Government Assessments
The following represent only a small sample of Illumant's Government clients, which span nearly every function and level. Please note that Illumant will not disclose any specific recommendations or outcomes related to our clients – we cannot betray the security risks our clients have, which ones they choose to mitigate or accept, or how.

Travis County Healthcare District
Illumant was hired by TCHD to perform a comprehensive HIPAA Security Risk Analysis and compliance gap analysis including assessments of numerous related healthcare entities. Illumant conducted individual risk analyses per business unit, including reviews of critical vendor and external partner security, as well as overall organization-wide security analysis. Relevant stakeholders for each unit were identified early, expectations were aligned during project planning, and Illumant offered proactive flexibility to afford meaningful security analysis in situations where unforeseeable circumstances, like critical staff turnover, inhibited planned testing. In addition to the compliance/governance work and risk assessment, comprehensive technical assessments were conducted including external and internal technical security of routers, firewalls, servers, applications, active directory, desktops, laptops and wireless networks. These assessments also included an on-site security physical security assessment.

TCHD engaged Illumant to perform additional services for the organization like assisting with business continuity planning and remote strategies.

Travis County
Illumant was hired by Travis County to perform a comprehensive HIPAA Security Risk Analysis and compliance gap analysis including assessments of numerous related departments dealing with PHI. Illumant conducted individual risk analyses per business unit, including reviews of critical vendor and external partner security, as well as overall organization-wide security

analysis. Relevant stakeholders for each unit were identified early, expectations were aligned during project planning, and Illumant offered proactive flexibility to afford meaningful security analysis in situations where unforeseeable circumstances, like critical staff turnover, inhibited planned testing. In addition to the compliance/governance work and risk assessment, comprehensive technical assessments were conducted including external and internal technical security of routers, firewalls, servers, applications, active directory, desktops, laptops and wireless networks. These assessments also included a remote physical security assessment, due to COVID 19.

The County purchased these services based on the success of the TCHD project.

Collier County Clerk

Illumant was hired by the Clerk to conduct a top-to-bottom security assessment covering all major aspects of information security at the organization. Illumant conducted a detailed risk assessment including evaluation of policies and procedures against popular security frameworks and best practices. To maximize the impact of our analysis, Illumant conducted concurrent external and internal technical security of routers, firewalls, servers, active directory, desktops, laptops and wireless networks. Illumant also performed a social engineering exercise to test employee awareness of security threats and incident handling techniques. These exercises also included an on-site physical security assessment. The improvements made to the security program following our initial assessment reduced their vulnerability landscape and improved their security posture when assessed the following year, Part of this success is due to the Purple Team approach taken to help the Clerk's staff better identify and respond to security threats in the wild, like Illumant's offensive security efforts.

During COVID, Illumant has offered hands on security training to the Clerk's IT/Security teams in lieu of physical security assessment. This training is focused on understanding and replicating offensive efforts, to identify vulnerabilities between external penetration tests.

The Clerk has renewed this contract three times.

Collier County

Illumant was hired by the County to conduct a top-to-bottom technical security assessment. Illumant conducted concurrent external and internal technical security of routers, firewalls, servers, active directory, desktops, laptops and wireless networks. Platform specific, technical configuration review were performed as a part of this assessment, as well as segmentation analyses.

The County engaged Illumant for a Three Year contract based on work with the Clerk.

City of Oakland

Illumant performed a Professional Information Systems Risk Assessment (IT Security Audit) providing an actionable security roadmap. The security assessment included risk assessment, detailed policy/procedure gap analysis for multiple overlapping frameworks, physical security assessment, penetration testing, threat modeling, and other specific, custom assessments. Illumant presented the results of the findings to both the senior City leadership, as well as other relevant stakeholders and elected officials.. The City was able to utilize the findings in Illumant's deliverables to make meaningful improvements to their security posture, budget effectively for future security work, and complete remediation efforts.

Additional City departments have engaged Illumant for assessments based on initial project's success.

Clients

Below is a partial list of Illumant's current and past clients:

Adobe Systems
Advisor Software
Ariel Investments
Bank of the Sierra
Bidz.com
Benelogic
Bessemer Trust
Bloom Energy
BlueRoads
Bowdoin College
Brocade Communications
Central Garden & Pet
CH2M Hill
Citizens Business Bank
Clark Nuber P.S.
Coherent, Inc.
CollabNet
Cornell University
County of Riverside
Danger
Disney Animation Studios
Duke University
E-Loan
EDPR
Ellipse Communications
Embarcadero Technologies
EMC Insignia
Essex Property Trust
Excelligence Learning Corporation
Foothill Independent Bank
Foothill Securities
Foundry Networks
Glatfelter
Glo
GP Bullhound
Herakles Data Center
Horizon Wind Energy
InSite Vision
Invisalign
Juniper Networks
K-Swiss
Kingston Companies
Marketo
Maxygen
Monogram Biosciences
NeoPhotonics
NetManage
Newfield Exploration
Pacific Premier Bank
Panasonic
Phoenix Technologies
Proteolix
Rainmaker Systems
Riverstone Networks
Shopping.com (eBay)
Solexa
SonicWall
Southwest Community Bank
SouthwestUSA Bank
Stanford University
Sunrise Telecom
TeleSoft Partners
The Link Group
Thomas and Betts
Titan Pharmaceuticals
Trimble
Tropian
Tyco Plastics & Adhesives
Tymphany
UCLA
UC Santa Cruz
University of North Carolina
University of California - UCSF
UT Starcom
Valley Hospital
Vineyard Bank
Virologic
VMware
Western Municipal Water District
Zhone Technologies

Section 6: Administrative Information

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "A"

AFFIDAVIT OF SOLVENCY

PERTAINING TO THE SOLVENCY OF {*insert entity name*} Illumant LLC, being of lawful age and being duly sworn I, {*insert affiant name*} B. Allens Crew, as {*insert position or title*} Sr. Solutions Advisor - Authorized Rep. (*ex: CEO, officer, president, duly authorized representative, etc.*) hereby certify under penalty of perjury that:

1. I have reviewed and am familiar with the financial status of above stated entity.
2. The above stated entity possesses adequate capital in relation to its business operations or any contemplated or undertaken transaction to timely pay its debts and liabilities (including, but not limited to, unliquidated liabilities, unmatured liabilities and contingent liabilities) as they become absolute and due.
3. The above stated entity has not, nor intends to, incur any debts and/or liabilities beyond its ability to timely pay such debts and/or liabilities as they become due.
4. I fully understand failure to make truthful disclosure of any fact or item of information contained herein may result in denial of the application, revocation of the Certificate of Public Necessity if granted and/or other action authorized by law.

The undersigned has executed this Affidavit of Solvency, in his/her capacity as a duly authorized representative of the above stated entity, and not individually, as of this 27 day of October, 2021.

Signature of Affiant

STATE OF Arizona)

COUNTY OF Maricopa)

Subscribed and sworn to before me this 27 day of October, 2021, by Billens Austin Crew who personally appeared before me at the time of notarization, and who is personally known to me or who has produced Drivers License as identification.

Notary Public

MARISABEL ACUNA
Notary Public - State of Arizona
MARICOPA COUNTY
Commission # 606866
Expires June 7, 2025

My commission expires:
06/07/25

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "B"

AFFIDAVIT

ST. JOHNS COUNTY BOARD OF COUNTY COMMISSIONERS
ST. AUGUSTINE, FLORIDA

At the time the proposal is submitted, the Respondent shall attach to his proposal a sworn statement.

The sworn statement shall be an affidavit in the following form, executed by an officer of the firm, association or corporation submitting the proposal and shall be sworn to before a person who is authorized by law to administer oaths.

STATE OF Arizona COUNTY OF Maricopa. Before me, the undersigned authority, personally appeared Billens Austin Crow who, being duly sworn, deposes and says he is Senior Solutions Advisor (Title) of ILLUMANT (Firm) the respondent submitting the attached proposal for the services covered by the RFP documents for **RFP No: 22-06; Cyber Security Assessment.**

The affiant further states that no more than one proposal for the above referenced service will be submitted from the individual, his firm or corporation under the same or different name and that such respondent has no financial interest in the firm of another respondent for the same work, that neither he, his firm, association nor corporation has either directly or indirectly entered into any agreement, participated in any collusion, or otherwise taken any action in restraint of free competitive bidding in connection with this firm's proposal on the above described service. Furthermore, neither the firm nor any of its officers are debarred from participating in public contract lettings in any other state.

(Proposer)

By Billens Crow

Sr. Solutions Advisor

(Title)

STATE OF Arizona)

COUNTY OF Maricopa

Subscribed and sworn to before me this 27 day of October, 2021, by Billens Austin Crow who personally appeared before me at the time of notarization, and who is personally known to me or who has produced Drivers Licens as identification.

M Acuna

Notary Public

MARISABEL ACUNA
Notary Public - State of Arizona
MARICOPA COUNTY
Commission # 606866
Expires June 7, 2025

My commission expires: 06/07/25

VENDOR ON ALL COUNTY SERVICES MUST EXECUTE AND ATTACH THIS AFFIDAVIT TO EACH PROPOSAL.

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "C"

CONFLICT OF INTEREST DISCLOSURE FORM

RFP Number/Description: RFP No 22-06; Cyber Security Assessment

The term "conflict of interest" refers to situations in which financial or other considerations may adversely affect, or have the appearance of adversely affecting a consultant's/contractor's professional judgment in completing work for the benefit of St. Johns County ("County"). The bias such conflicts could conceivably impart may inappropriately affect the goals, processes, methods of analysis or outcomes desired by the County.

Consultants/Contractors are expected to safeguard their ability to make objective, fair, and impartial decisions when performing work for the benefit of the County. Consultants/Contractors, therefore must there avoid situations in which financial or other considerations may adversely affect, or have the appearance of adversely affecting the Consultant's/Contractor's professional judgement when completing work for the benefit of the County.

The mere appearance of a conflict may be as serious and potentially damaging as an actual distortion of goals, processes, and methods of analysis or outcomes. Reports of conflicts based upon appearances can undermine public trust in ways that may not be adequately restored even when the mitigating facts of a situation are brought to light. Apparent conflicts, therefore, should be disclosed and evaluated with the same vigor as actual conflicts.

It is expressly understood that failure to disclose conflicts of interest as described herein may result in immediate disqualification from evaluation or immediate termination from work for the County.

statement:

☒ I hereby attest that the undersigned Respondent has no actual or potential conflict of interest due to any other clients, contracts, or property interests for completing work on the above referenced service.

☐ The undersigned Respondent, by attachment to this form, submits information which may be a potential conflict of interest due to other clients, contracts or property interests for completing work on the above referenced service.

Legal Name of Respondent: Illumant LLC

Authorized Representative(s):

Signature	Print Name/Title
[signature]	Matija Siljak, CEO
Signature	Print Name/Title

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "D"

DRUG-FREE WORKPLACE FORM

The undersigned firm, in accordance with Florida Statute 287.087 hereby certifies that

Illumant LLC does:

Name of Firm

1. Publish a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the workplace and specifying the actions that will be taken against employees for violations of such prohibition.

2. Inform employees about the danger of drug abuse in the workplace, the business' policy of maintaining a drug-free workplace, any available drug counseling, rehabilitation, employee assistance programs and the penalties that may be imposed upon employees for drug abuse violations.

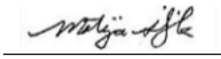
3. Give each employee engaged in providing the contractual services that are described in St. Johns County's Request for Proposal a copy of the statement specified in paragraph 1.

4. In the statement specified in paragraph 1, notify the employees that, as a condition of working on the contractual services described in paragraph 3, the employee will abide by the terms of the statement and will notify the employer of any conviction of, or plea of guilty or nolo contendere to, any violation of Florida Statute 893, as amended, or of any controlled substance law of the United States or any state, for a violation occurring in the workplace no later than five (5) days after such conviction or plea.

5. Impose a sanction on, or require the satisfactory participation in a drug abuse assistance or rehabilitation program if such is available in the employee's community by, any employee who is so convicted.

6. Consistent with applicable provisions with State or Federal law, rule, or regulation, make a good faith effort to continue to maintain a drug-free workplace through implementation of paragraphs 1 through 5.

As the person authorized to sign this statement, I certify that this firm complies fully with the above requirements.



Signature

10/26/2021

Date

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "E"

LOCAL PREFERENCE

Any Respondent that meets the criteria of a Local Business, in accordance with Section 302.25 of the SJC Purchasing Procedure Manual, must complete and sign this Attachment "E" to indicate their qualification to receive local preference. All required documentation to demonstrate that the Respondent meets all qualification criteria as a local business must be included in the submitted proposal/submittal with this Attachment "E".

In order to qualify for local preference Respondent must provide sufficient documentation to demonstrate:

- A physical, brick and mortar place of business located within the geographic boundaries of St. Johns County, with a valid mailing address, in an area zoned for the conduct of such business, from which the Vendor has operated or performed business on a day-to-day basis that is substantially similar to those specified in the solicitation for a period of at least one (1) calendar year prior to the issuance of the solicitation. No PO Boxes shall be accepted.
- Local address above must be registered as the Vendor's principal place of business with the Divisions of Corporations Florida Department of State for at least one (1) calendar year prior to the issuance of this RFP.
- Submit current and valid Local Business Tax Receipt, and must have Local Business Tax Receipts issued by the St. Johns County Tax Collector from at least one (1) calendar year prior to issuance of this RFP.
- Must qualify as a local business as shown above **AND** self-perform a minimum of fifty percent (50%) of all services under the awarded Contract, or must have a minimum of fifty percent (50%) of all services performed by qualified local businesses as sub-contractors or sub-consultants.

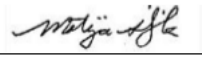
If qualifying for local preference through the use of qualified local sub-contractors or sub-consultants, Respondent must submit all required documentation to demonstrate the above requirements of all proposed sub-contractors and sub-consultants for local preference consideration with the submitted proposal.

Respondent is a Local Business as defined in Section 302.25, SJC Purchasing Procedure Manual _____

If Respondents selects this option, by signing below, Respondent certifies that the firm qualifies as a local business in accordance with the requirements stated above, OR certifies that the submitted local business proposed as sub-contractors or sub-consultants meet the requirements for local preference AND that a minimum of fifty percent (50%) of all services shall be performed by local businesses as proposed.

Respondent is **not** a Local Business as defined in Section 302.25, SJC Purchasing Procedure Manual X

If Respondent selects this option, Respondent is not seeking consideration for local preference, and is not required to submit the documentation provided above.



Signature – Authorized Respondent Representative

Matija Siljak, CEO
Printed Name & Title

10/26/2021
Date of Signature

Illumant | Security Assessment and Compliance
431 Florence Street, Suite 210, Palo Alto, California 94301
+1.650.961.5911 (main) | +1.650.961.5912 (fax)

www.illumant.com
info@illumant.com

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "F"

CERTIFICATES OF INSURANCE

Respondents shall provide certificates of insurance as part of their submittal package. Certificates of insurance shall meet or exceed the requirements as described in Part V: Contract Requirements; F. Insurance Requirements.

Failure to provide proof of current insurance coverage or ability to obtain the required coverages may result in being deemed non-responsive and removed from further consideration.

(Attach or insert copy here)

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 9/24/2021

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME: CL Central
Leavitt Pacific Insurance Brokers, Inc. License #0D79674 1570 The Alameda, Suite 101 San Jose CA 95126	PHONE (A/C, No, Ext): (408)288-6262 FAX (A/C, No): (408)298-7635 E-MAIL ADDRESS: Broker
INSURED	**INSURER(S) AFFORDING COVERAGE** / **NAIC #**
Illumant LLC 431 Florence ST STE 201 Palo Alto CA 94301	INSURER A: Sentinel Insurance Company 11000 INSURER B: Property & Casualty Insurance Company c 34690 INSURER C: Lloyd's of London R85202 INSURER D: INSURER E: INSURER F:

COVERAGES **CERTIFICATE NUMBER:** CL2192428449 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X COMMERCIAL GENERAL LIABILITY CLAIMS-MADE X OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: X POLICY PRO-JECT LOC OTHER:			57SBARH2968	1/25/2021	1/25/2022	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG Hired & Non-Owned Auto Liability	$ 2,000,000 $ 1,000,000 $ 10,000 $ 2,000,000 $ 4,000,000 $ 4,000,000 $ 2,000,000
	AUTOMOBILE LIABILITY ANY AUTO ALL OWNED AUTOS SCHEDULED AUTOS HIRED AUTOS NON-OWNED AUTOS						COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	$ $ $ $
	UMBRELLA LIAB OCCUR EXCESS LIAB CLAIMS-MADE DED RETENTION $						EACH OCCURRENCE AGGREGATE	$ $
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? Y / N (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N / A		57WBCNG0526	12/15/2020	12/15/2021	PER STATUTE OTH-ER E.L. EACH ACCIDENT E.L. DISEASE - EA EMPLOYEE E.L. DISEASE - POLICY LIMIT	$ 1,000,000 $ 1,000,000 $ 1,000,000
C	Professional Liability E&O TECH & CYBER			BSK0033496425	9/20/2021	9/20/2022	Each Claim Retention	5,000,000 10,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER

For Informational Use

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

M zcMunford/MAMUNF

ACORD 25 (2014/01)
INS025 (201401)

The ACORD name and logo are registered marks of ACORD

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "G"
CLAIMS, LIENS, LITIGATION HISTORY
(Complete and Submit)

1. Within the past 7 years, has your organization filed suit or a formal claim against an owner (as a prime or subcontractor) or been sued by or had a formal claim filed by an owner, subcontractor or supplier resulting from a construction dispute? Yes _____ No X_____ If yes, please attach additional sheet(s) to include:

   Description of every action Captions of the Litigation or Arbitration

   Amount at issue: _____ Name (s) of the attorneys representing all parties:

   Amount actually recovered, if any: _____

   Name(s) of the service owner(s)/manager(s) to include address and phone number:

2. List all pending litigation and or arbitration.
   N/A

3. List and explain all litigation and arbitration within the past seven (7) years - pending, resolved, dismissed, etc.
   N/A

4. Within the past 7 years, please list all Liens, including Federal, State and Local, which have been filed against your Company. List in detail the type of Lien, date, amount and current status of each Lien.
   N/A

5. Have you ever abandoned a job, been terminated or had a performance/surety bond called to complete a job?

   Yes _____ No X_____ If yes, please explain in detail:

6. For all claims filed against your company within the past five-(5) years, have all been resolved satisfactorily with final judgment in favor of your company within 90 days of the date the judgment became final? Yes X___ No____
   If no, please explain why? _____
   N/A

7. List the status of all pending claims currently filed against your company:
   N/A

Liquidated Damages

1. Has an owner ever withheld retainage, issued liquidated damages or made a claim against any Performance and Payment Bonds? Yes _____ No X_____ If yes, please explain in detail:

(Use additional or supplemental pages as needed)

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "K"
E-VERIFY AFFIDAVIT
Contract No. Cybersecurity Assessment

STATE OF Arizona
COUNTY OF Maricopa

I, Billens Cron (hereinafter "Affiant"), being duly authorized by and on behalf of Illumant LLC (hereinafter "Consultant/Contractor") hereby swears or affirms as follows:

1. Consultant/Contractor understands that E-Verify, authorized by Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), is a web-based system provided by the United States Department of Homeland Security, through which employers electronically confirm the employment eligibility of their employees.

2. For the duration of Contract No. Cybersecurity Assessment (hereinafter "Agreement"), in accordance with section 448.095, F.S., Consultant/Contractor shall utilize the U.S. Department of Homeland Security's E-Verify system to verify the employment eligibility of all new employees hired by the Consultant/Contractor and shall expressly require any subcontractors performing work or providing services pursuant to the Agreement to likewise utilize the U.S. Department of Homeland Security's E-Verify system to verify the employment eligibility of all new employees hired by the subcontractor.

3. Consultant/Contractor shall comply with all applicable provisions of section 448.095, F.S., and will incorporate in all subcontracts the obligation to comply with section 448.095, F.S.

4. Consultant/Contractor understands and agrees that its failure to comply with all applicable provisions of section 448.095, F.S. or its failure to ensure that all employees and subcontractors performing work under the Agreement are legally authorized to work in the United States and the State of Florida constitute a breach of the Agreement for which St. Johns County may immediately terminate the Agreement without notice and without penalty. The Consultant/Contractor further understands and agrees that in the event of such termination, Consultant/Contractor shall be liable to the St. Johns County for any costs incurred by the St. Johns County resulting from Consultant/Contractor's breach.

DATED this 27 day of October, 2021.

Signature of Affiant

Billens Cron
Printed Name of Affiant

Printed Title of Affiant

Full Legal Name of Consultant/Contractor

Sworn to (or affirmed) and subscribed before me by means of ☒ physical presence or ☐ online notarization, this 27 day of October, 2021, by {*insert name and title of Affiant*}, who is personally known to me or has produced Drivers License as identification.

MARISABEL ACUNA
Notary Public - State of Arizona
MARICOPA COUNTY
Commission # 605866
Expires June 7, 2025

Notary Public
My Commission Expires: 06/07/25

30

ADDENDUM #2

October 21, 2021

To: Prospective Respondents
From: St. Johns County Purchasing Division
Subject: RFP No: 22-06; Cyber Security Assessment

This Addendum #2 is issued to further Respondents' information and is hereby incorporated into the RFP Documents. Respondents shall incorporate any and all information, changes, clarifications and instructions provided in each Addendum into their submitted Proposal, and include a copy of each signed addendum in the submitted Proposal as instructed in the RFP Document.

Questions/Answers:

1. Is a Credential Landing page to provide analysis for users who enter credentials in-scope? YES/NO
   Answer: No.

2. Please confirm type of data to capture:
   a. Click Rate: YES/NO
   b. Credential Harvesting: YES/NO
   c. Live Payload: YES/NO
   d. Other: Please specify
   Answer: Please see clarification found in Addendum #1.

3. For the vulnerability assessment, will County utilize white-box, gray-box, or black-box testing?
   Answer: White-box testing.

4. Number of Facilities in scope?
   Answer: 2.

5. To what level should the unauthorized access be demonstrated (access to paper files, office areas, network access, obtaining equipment, etc.)?
   Answer: Network access.

6. What approach is expected for this assessment (i.e., total population or sampling)?
   Answer: Referring to Social Testing, a sample is acceptable. Referring to phishing/email testing, then a total population is expected.

7. Would it be possible or desired to perform grey box testing in conjunction with external penetration testing and DMZ architecture review?
   Answer: White Box testing is permitted.

8. Are you seeking a guided walkthrough of in-scope facilities or physical penetration testing?
   Answer: SJC prefers to have testing against physical access controls by having the awarded contractor attempt to utilize social engineering techniques to obtain access to secure areas.

9. What social engineering methods are in scope (e.g., phishing, USB drops, vishing, physical access attempts)?
   Answer: Phishing.

10. Please provide historical data for FTE staff.
    Answer: County has no historical data to provide.

11. Will USB drops be included as part of the exercise? If so, how many USBs would you like to deploy, and how many locations?
    Answer: No.

12. Please confirm the following attack vectors for a physical pentest:
a. SIte Security Architecture: YES/NO
b. Physical Perimeter Access Control: YES/NO
c. Sensitive Area Access: YES/NO
d. Document Control: YES/NO
e. Network/Device Access: YES/NO
f. Internal Sensitive Information handling: YES/NO
g. USB Device Drop: YES/NO
    Answer: a. Yes.
    b. Yes.
    c. Yes.
    d. No.
    e. Yes.
    f. No.
    g. Yes.

13. In order to properly scope the level of effort for this assessment can you provide us copies of current Security Policies, Procedures?
    Answer: None are available.

14. Can you provide any current process/volumes and/or existing methodologies in order to properly scope the level of effort for this assessment?
    Answer: None are available.

15. Can you provide documentation and/or descriptions of currently deployed policies, methodologies, controls in place for Host Based Security along with description/quantities of current operating systems, internally developed applications, and associated current tools in place for management of the various areas of assessment desired.
    Answer: None are available.

16. Will Wi-Fi testing be conducted at multiple locations? If so, how many SSIDs and which locations?
    Answer: One location (SJC Administration Building) is sufficient.

17. Will Physical Facility Breach be included as part of the exercise? If so, how many locations will be in scope?
    Answer: Yes, one (1) the SJC Administration Building.

18. For services that do not require physical presence; Can they be performed remotely? If so, can they be performed outside the Continental US?
    Answer: Yes, Respondent business can be in any location provided the can complete the required physical penetration testing.

19. Do you have an Access Control tool in place?
    Answer: Yes, we use APACS Pro by Apollo Security.

20. Can the vendor deliver a subset of the in-scope services from a location outside the United States?
    Answer: See the response to #18 above.

21. Is a physical penetration test expected, or will review of policies, and procedures for physical access be performed?
    Answer: See the response to #17 above.

22. Can you confirm that the removal of SCADA applies to the 420 items listed in the scope or has this item been renamed?
    Answer: Yes, removal of SCADA applies to the 420 items listed in the scope.

23. Attachment K must be signed and notarized, but it is written as if a contract is already in place. What should we fill in as the Contract No. or should we wait to complete this form until award?
    Answer: Respondents may either leave the contract line blank or put the project name "Cyber Security Assessment" in the space provided. You will need to complete and submit the form with your proposal.

24. Attachment J, the Pricing Proposal Form, specifies that we should provide separate pricing for the Cyber Security Assessment for both the BCC and the Clerk of Courts. However, none of the IT environment information has been provided separately for the two entities. Is it possible for your team to provide either a breakdown of the IT environment by entity, or specify a percentage by which the pricing split could be ascertained?
    Answer: The only separation between BCC and the Clerk is the number of servers (as listed in the environment details; showing two sections BCC & Clerk). The Respondents shall provide a holistic pricing component. SJC's expectation is that any time spent on each individual entity's environment would be roughly itemized; in order for the County to later divide the costs.

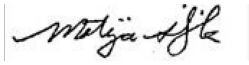
25. The approximate number of Internal/External Devices listed on page 5 of the RFP is 3,191 (excluding SCADA) but in Amendment 1 response # 31 you indicate that there are "approximately 9,500, including servers, desktops, laptops, cameras, IP security devices such as door readers, ect". For purposes of properly scoping the number of IP devices to be scanned in the vulnerability assessment can you confirm whether we should use 9,500 or the page 5 numbers?
    Answer: The number of IP devices to be scanned is 3,191.

26. When submitting the response the addendums must be include. Do you want only the page signed indicating received or the entire addendum in the response?
    Answer: Respondents may submit only the signed acknowledgement page.

27. Are travel costs included in the County's budget?
    Answer: The budget for this project is not itemized. Respondents are required to adhere to the County's travel policy as stipulated in the SJC Administrative Code Travel Policy for County Employees.

The deadline for Proposal remains the same: Thursday, October 28, 2021 at 4:00PM EDST

Acknowledgment



Signature and Date

Matija Silak

Printed Name/Title

Illumant LLC

Company Name (Print)

END OF ADDENDUM NO. 2

ADDENDUM #1

October 8, 2021

To: Prospective Respondents
From: St. Johns County Purchasing Division
Subject: RFP No: 22-06; Cyber Security Assessment

This Addendum #1 is issued to further Respondents' information and is hereby incorporated into the RFP Documents. Respondents shall incorporate any and all information, changes, clarifications and instructions provided in each Addendum into their submitted Proposal, and include a copy of each signed addendum in the submitted Proposal as instructed in the RFP Document.

Clarifications/Revisions:

1. To better define the scope of "APPLICATION TESTING" to be performed the County provides the following clarification:

   St. Johns County (SJC) is looking for basic testing of our EXTERNAL applications. The extent of this testing would be limited to approximately ten (10) applications that we have developed in-house, and NOT to third-party hosted applications. The testing of these in-house developed applications would NOT include API testing. The testing would be somewhat generic in nature, to include, standard exploits such as SQL/script injection, and known vulnerabilities in the hosting platform (Windows, IIS, .NET framework). Therefore, we would NOT expect all pages within applications, or any proprietary business logic to be tested verbosely. Due to the high number of, and extensive business/workflow knowledge required, INTERNAL applications would NOT need to be tested, but rather a few random platform exploit tests would be sufficient.

   All of our EXTERNAL web applications are written in MS.NET framework version 4.x, hosted on MS Windows IIS, and access data from a MS SQL Server DB. Our applications sometimes utilize client-side JavaScript/AJAX, but usually for user interface experience purposes only. We also commonly use Bootstrap as a responsive framework. These EXTERNAL applications are ALL web based, with no Native Windows or Native Mobile applications. Testing would occur in a LIVE production environment, and therefore, we would need to be notified of the timeline and scope of testing to take place, when the time comes.

   To be clear, we are NOT asking for source code to be evaluated, but simply spot checks on our applications for common security flaws, and basic inspection of our platforms, known exploits, patches, etc. Once again, to reiterate:

   - NO isolated Web Service testing
   - NO isolated API testing
   - NO source code evaluation
   - NOT every page or URL must be tested, simply spot checks, with documentation of what was tested.
   - NO user role testing.

2. All references to SCADA in the scope of services are hereby removed.

Questions/Answers:

1. Can you share any budgetary information about this project with us, is there any assigned budget for this project? Please specified the budget.
   Answer: The County has $160,000.00 budgeted.

2. Is there an incumbent company or organization with an advantage for this project?
   Answer: No.

3. In the Scope of Services it looks like you are looking for a variety of security related services including: security benchmarking, vulnerability assessments, penetration testing, data assessments, third-party interfaces, application penetration testing, password management auditing, access controls auditing, and security logging review. However, the requirements for the final report look to focus on penetration testing. As such, it is not 100% clear what the you are looking for, and if it is everything in the scope of services needs to be included on the final report, that is a lot of different items that are all independent of each other, and will affect the final price estimation, can you please clarify, what is need it on the SOW and if all these items need to be part of the final report as well?
   Answer: All penetration items are to be included in the final report. The remainder of the analysis is to be given in a less formal manner.

4. How many office locations and facilities are in-scope for the project?
   Answer: There are 57 remote locations that connect through various transport methods back to a DMVPN hub. In a sense, they are 1 site in 4 VRFs but they are physically diverse.

5. How many relevant departments are there from an IT or Information Security point-of-view?
   Answer: There are 2 Constitutional entities.

6. How many existing Information Security Policies and Procedures are currently implemented?
   Answer: There are minimal P&P's in place.

7. Is there a network diagram that could be shared?
   Answer: One can be shared after award and a non-disclosure agreement has been executed.

8. How many Wireless Access Points are there in total across the two organizations?
   Answer: 150.

9. Is the approximate number of partner/vendor connections 12?
   Answer: Yes.

10. How many applications and APIs are in-scope for security assessment/testing?
    Answer: With regards to external applications, perform testing on known exploits for SQL Server, IIS, to include DoS and other common attack methodology such as script and SQL injection. Due to the business specific nature of our internal applications, we would not expect individual testing on each of those 100+ applications. More of an "after hours", platform based (IIS, SQL Server, .NET, Windows) penetration and various exploit testing would be sufficient.

11. How many of the apps/APIs can be tested remotely? (Note that QA or DEV versions are necessary for security testing)
    Answer: See the response to #10 above.

12. When does the St. John's Country BCC expect the work to be started/completed?
    Answer: A schedule and timeline shall be developed after award.

13. Is there an expected period of performance once the work has started? Or can the engagement be broken into phases throughout the year long period?
    Answer: See the response to #12 above.

14. Is there a proposed budget that the City has allocated for this assessment? If so, can that be disclosed?
    Answer: See the response to #1 above.

15. Can a portion of the work be performed fully remote, apart from the physical security and SCADA phases of the assessment?
    Answer: Yes.

16. Can the work be performed outside of core working hours (9AM-5PM)?
    Answer: Yes.

17. How does the SCADA network connect with the rest of the City's network?
    Answer: See #2 in Clarifications/Revisions above.

18. How many locations will be assessed for physical security? Will the county permit after hours assessment of physical locations?
    Answer: One location. Yes, with proper scheduling.

19. How many total individuals will the social engineering testing intend to target?
    Answer: There are approximately 1,200 email accounts.

20. How many different campaigns are expected for the social engineering testing?
    Answer: Respondents should include recommendations in their RFP submission.

21. How are communications with partner billing entities conducted? (e.g., protocols, applications)
    Answer: This will be handled on a case by case basis.

22. How many sites should be included in physical security testing?
    Answer: See the response to #18 above.

23. Are there any specific social engineering attack vectors or pretexts that St. Johns County specifically expects/desires to be included in testing?
    Answer: No.

24. What language/frameworks are any custom Web applications written in?
    Answer: St. Johns County developed applications are in VB.Net.

25. What is the count of URLs for each Web application? For sites using custom API calls, how many APIs are used for each Web application?
    Answer: There are 10 external applications w/ 10 URLs. Please see #1 in Clarifications/Revisions above for additional information.

26. Will credentials be provided for Web applications to ensure exhaustive testing? (e.g., unauthenticated, authenticated user account, authenticated as administrator account)
    Answer: Yes, credentials will be provided after contract award.

27. How many external (network) points of presence will be tested?
    Answer: Two (2).

28. What types of wireless protocols are in scope for testing? (e.g., 2.4 GHz, 5 GHz, Cellular)
    Answer: 2.4/5Ghz WiFI.

29. Would the County consider electronic-only response submissions?
    Answer: No.

30. Who is providing your current cyber security services, an external vendor or delivered in-house?
    Answer: Internal, in-house.

31. Please provide the number of systems which are designated as in scope.
    Answer: Approximately 9,500. This would include servers, desktops, laptops, cameras, IP security devices such as door readers, etc.

32. Does the client want every internal application tested with full coverage of all functionality or are they looking for a cursory "low-hanging fruit" approach? With 100 internal applications a full assessment, particularly a whitebox assessment involving source code review and analysis, of each would greatly increase the amount of time required for testing to complete.
    Answer: SJC is looking for a cursory approach with emphasis on process.

33. Are there any socio-economic preference points allocated to small businesses, disadvantaged small businesses, economically disadvantaged women-owned small businesses (EDWOSB), women-owned small businesses (WOSB), and/or minority owned small businesses?
    Answer: No.

34. Is this the first time that you will contract a vendor for the services in question? If not, then would a copy of the final contract and amount of the previous successful vendor be available?
    Answer: This will be the first Cyber Security Assessment completed by SJC.

35. Given the COVID-19 pandemic, can work be performed remotely to the maximum possible extent?
    Answer: Yes.

36. For the items – "Partner Connectivity", "Interface to Partner Entities", "Evaluate Client Remote Access to External Services", "Evaluate Internal MIS Tools for Data Leakage", "Internet Usage", and "Host Based Security", are you looking for us to perform these reviews **as a part of** the network penetration tests? Or are you looking for us to perform individual reviews of each of these areas at a detailed configuration level where we review the configuration settings at a very granular level?
    Answer: These are expected to be separate.

37. Please provide the approximate number of live external IP addresses in scope?
    Answer: 80.

38. Please provide the approximate number of live internal IP addresses in scope?
    Answer: See the response to #31 above.

39. Please provide the number of web applications in scope?
    Answer: See clarification above.

40. Please provide the number of locations to be included in the wireless network penetration test? Can sampling be used?
    Answer: One (1) is sufficient as the configuration is not diverse.

41. As part of this project are you also looking for us to review your existing cybersecurity documentation (policies, plans, procedures, etc.) and provide guidance for improvement? In addition, are you looking for us to develop one or more of these from scratch?
    Answer: Yes to both.

42. Please identify if you have key cybersecurity documentation in place such as – Business Continuity Plan, Incident Response Plan, Information Security Policies and Procedures, etc.
    Answer: SJC has frameworks for all of these; but, is concerned about their efficacy.

43. Please provide a high-level overview of your remote access infrastructure in scope for review.
    Answer: Remote Access is currently a mix of legacy client Anyconnect transitioning to client based Global Protect. A single gateway and portal are in place.

44. Please provide the number and types of social engineering scenario tests that you would like us to perform.
    Answer: Respondents should document what they are proposing in their submission.

45. Please provide a high-level overview of your URL/web filtering solution infrastructure in scope for review.
    Answer: Web filtering is performed with a mix of client based and inline iBoss scanning.

46. Please provide a high-level overview of the operating systems and databases in scope for the host-based security review.
    Answer: 80% Windows, Security, 5% Linux servers, appliances, etc. Mobile is 90% iOS with 10% Android.

47. Please provide a high-level idea of the size and scope of the technical infrastructure that we would encounter.
    Answer: There are 2 main Datacenters with several small server environments at local offices. Mostly all VMware/Microsoft. Network is 80-90 routers, 400 switches, 3 WLCs all Cisco.

48. Please provide a description of the SCADA/ICS infrastructure in scope for penetration testing.
    Answer: See #2 under Clarifications/Revisions above.

49. As part of benchmarking security practices and procedures against NIST 800.53, is a governance or NIST 800-53 compliance assessment expected?
    Answer: No.

50. Concerning the Physical Access Controls Evaluation and Social Engineering, is a physical penetration test expected?
    Answer: Yes.

51. Concerning the Internet Usage portion of the engagement, what are the expectations or goals for this assessment?
    Answer: SJC has no defined goals for this assessment.

52. Are there any regulations or regulators/auditors that apply to the environments to be tested? If so, specify which testing or environment it applies to.
    Answer: Some applicability to PCI, HIPAA and CJIS.

53. Is there a date that final reports must be submitted by? If yes, please specify final report delivery date.
    Answer: TBD based upon negotiations and final schedule included in the awarded contract.

54. Please provide the number of external IP's to be tested:
    Answer: See the response to #37 above.

55. Will you require a retest of Critical/High findings for the external pentest?
    Answer: No.

56. Will you require a customer-facing report for the external pentest?
    Answer: Yes.

57. Will you require a customer facing attestation letter for the external pentest?
    Answer: No.

58. List any third-party systems or networks that are in-scope for the external pentest as well was which systems they own: NOTE: Permission must be obtained by the third-party prior to conducting any testing on these systems.
    Answer: No third-party systems are included.

59. Please provide the number of internal IP's to be tested:
    Answer: See response to #31 above.

60. Do all internal systems respond to a Ping Echo Request?
    Answer: No (approximately 95% will).

61. Will internal testing be performed remote or in-person? NOTE: If Remote, confirm that the client will allow a laptop to be connected to the internal network. The Laptop will form a VPN tunnel for assessment work to be performed remotely.
    Answer: SOME remote is acceptable.

62. Please provide the number of SSID Networks to be in-scope:
    Answer: 3.

63. Number of locations to be tested for wireless pentest, and address of each location.
    Answer: 1.

64. Number of locations to be tested for the physical pentest and address for each location in-scope:
    Answer: One (1) location. 500 San Sebastian View, St Augustine FL 32084.

65. Number of users to be in-scope for email phishing:
    Answer: See the response to #19 above.

66. Please advise type of tests required:
    Answer:
    a. Web Application: **YES**
    b. Mobile Application: Android: **NO**
    c. Mobile Application: iOS: **NO**

67. Please specify how many web/mobile applications need to be tested and specify if they are mobile or web apps:
    Answer: See #1 under Clarifications/Revisions above.

68. Describe the functionality of each application:
    Answer: See #1 under Clarifications/Revisions above.

69. List any specific concerts for each application being tested:
    Answer: See #1 under Clarifications/Revisions above.

70. What type of data is the application responsible for protecting?
    Answer: See #1 under Clarifications/Revisions above.

71. Are any of the applications to be tested custom-built, third-party hosted or COTS? If so, please specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

72. Do any of the applications utilize an application server? If so, specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

73. List any other third-party products being utilized:
    Answer: See #1 under Clarifications/Revisions above.

74. Will testing be conducted on a production environment or is a development/staging environment available?
    Answer: See #1 under Clarifications/Revisions above.

75. Specify the language each application is developed in:
    Answer: See #1 under Clarifications/Revisions above.

76. Do any of the applications rely on client-side technologies? If so, specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

77. Do the applications leverage AJAX, AngularJS, or other frameworks? If so, specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

78. List the different types of roles to be tested within the application and specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

79. Approximately how many user interface screens comprise each application?
    Answer: See #1 under Clarifications/Revisions above.

80. Do the applications interface with any single sign-on (SSO) solution? If so, specify which applications, and list what SSO solution is in place for each application.
    Answer: Yes, ADFS/Azure AD is in use only for third part cloud appliaitons (Energov, Duo, etc.)

81. Is the SSO server accessible from the internet, only internally, or restricted per application.
    Answer: Yes, https://fs.sjcfl.us server SJCADFS.

82. Is there a thick client that talks to the application? If so, please specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

83. Should the thick-client be tested?
    Answer: See #1 under Clarifications/Revisions above.

84. What language is the thick-client written in?
    Answer: See #1 under Clarifications/Revisions above.

85. Are there any system to system API's exposed by the application that you would like tested? If yes, please specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

86. How many distinct API's need to be tested?
Answer: See #1 under Clarifications/Revisions above.

87. Please provide any documentation or URL's to definition files if possible:
Answer: See #1 under Clarifications/Revisions above.

88. What OS is being tested?
Answer: See response to #46 above.

89. How many devices per OS to be tested?
Answer: See response to #46 above.

90. What OS will be tested (Windows, Linux, Mac, ect)?
Answer: See response to #46 above.

91. How many devices per OS to be tested?
Answer: See response to #46 above.

92. In your own words please describe end-goal/result from risk assessment:
Answer: SJC's goal is to identify any high risk areas that require remediation, as well as to aid in defining a baseline standard for MIS.

93. Please list all locations where traditional IT networks/infrastructure are:
Answer: There are 57 remote locations. Details will be provided after RFP is awarded. All are within St Johns County.

94. Number of dedicated security personnel per location:
Answer: 0.

95. Number of security domains (Active Directory forests) that are in place per location:
Answer: 1.

96. Number of servers (physical and virtual) that are in the infrastructure per location:
Answer: 0-20 at remote sites. The 2 Datacenters have between 20-200.

97. Will you be able to provide the following organizational information?
Answer:

a. Personnel

1. Organizational Chart: **Yes**
2. Roles and Responsibilities of IT/Security: **Yes**
3. Documented Policies & Processes: **Yes**
4. Information Security Policy: **Yes**
5. Risk Management Strategy and Plan: **Yes**
6. IR Strategy: **No**
7. Results of any previous assessments: **N/A**

b. Physical

1. Locations of sites: **Yes**

2. Physical Security responsibility overview: **Yes**

c. Network

1. Logical network diagram, data flow diagrams, any other network and communications diagrams: **Yes**
2. Security monitoring overview: **Possibly**

d. Assets

1. Asset management process - inventory of endpoints on the network: **90%**
2. Supplier and third-party partner inventory/list: **50%**
3. List of critical facilities: **Yes**

98. Have you had any formal vulnerability assessment (s) and/or Penetration Testing processes performed within the past 3 years – whether across the full BCC/Clerk operations or within separate operating units of BCC – and if so will the results of those projects be available for review?
Answer: See the response to #34 above.

99. Can you provide details regarding the number of physical locations and types of access controls that are in place in order to properly scope the level of effort for this assessment?
Answer: There are approximately 50+ locations with emphasis on the main campus which houses 70% of the users in question. Access control is currently badge controlled in all main locations with many outbuildings being a mix of keyed access and combination locks.

100. Can you provide additional documentation/information on the current # of URLs as well as deployed tools being utilized in order to properly scope the level of effort for this assessment.
Answer: See #1 under Clarifications/Revisions above.

101. In addition to the Corporate-owned devices (550) can you advise the quantity of BYOD devices in use, and can you provide documentation regarding BCC policies/controls currently in place for BYOD users. This will be helpful to properly scope the level of effort for this assessment.
Answer: There are no BYOD devices in use.

102. Can you provide additional clarification on the service scope, for instance are you requesting Web Application Testing for this category? If "yes" then can you provide answers to the following scoping items:
Answer: See #1 under Clarifications/Revisions above. Answer applies to items a – e below as well.

a. How many web site(s)/URLs would you like to assess?

b. How many pages? An example of a static page would be the front page of a web site or any of the pages referenced on the site map that remain the same. A dynamic page would be applications that are behind the static page. An example would be a built in price list, a log in, choices from a previous page, i.e., the Best Buy site where you can drill down and purchase things. Those would be dynamic pages. Are some of these pages dynamically generated from a subset of core pages?

c. Does the application require any client side applications? An example of this would be a web site that requires Flash Player, ActiveX, etc. Anything a web site user would need to download to view the web site correctly.

d. Are there different user levels? If so, how many? An example of this would be a web site that has an "Administrator" logon and also a "User" logon. If there are different user levels, do you want data integrity verified between different user levels? Do you want us to make sure one level of logon can/cannot access information intended for another level?

e. Do you want black-box (unauthenticated) or white-box (authenticated) testing?

103. SCADA devices – can you provide descriptions of what types of devices (functional, network, applications) are included within this category.
Answer: See #2 under Clarifications/Revisions above..

104. Can all SCADA devices be accessed via IP networks? If not, what network types are deployed?
Answer: See #2 under Clarifications/Revisions above.

105. How many locations are to be assessed?
Answer: See the response to #18 above.

106. Are point to point wireless systems deployed to provide connectivity between locations?
Answer: Yes, but for a handful of very small sites/hosts.

107. How many wireless access points (WAPs) are deployed?
Answer: 150.

108. Are there open access points for public/visitor access? If so, on how many WAPs?
Answer: Yes, All.

109. Are there encrypted access points for business use? If so, on how many WAPs?
Answer: Yes, All.

110. How many SSIDs does the organization have at each location?
Answer: 3 are in scope.

111. Is the organization using WEP, WPA, and/or WPA2 encryption? Which ones?
Answer: WPA2 EAP-TLS.

112. How many wireless policies, procedures, and documentation is available for review?
Answer: 0.

113. Can you describe the nature and range of access methods currently in use and to be evaluated for the various partner entities?
Answer: Remote Access for an unknown number of users, 5 Lan 2 Lan tunnels, ~10 directly connected firewall connected interconnects.

114. Are these dedicated network connections?
Answer: See the response to #113 above.

115. Have you performed any formal social engineering assessments within the past 3 years, and if so will the results of those assessments be provided?
Answer: Yes, email based only. Yes, results will be provided to awarded firm.

116. Total number of internal network IP addresses to be tested. (If providing an IP range, please indicate the estimated number of live IPs.)
Answer: See the response to #31 above.

117. How deep should testing go in the event of successful network penetration (i.e., just validation of vulnerability; network administrator access; server access, etc.)?
Answer: Validation is sufficient.

118. Are internal web-based applications/services in scope? If so, please indicate the anticipated number of web-based applications/services that may need to be assessed.
Answer: See #1 under Clarifications/Revisions above.

119. Is it desired to evaluate the strength of mobility environments (iPhones, BlackBerry, home VPN access)?
Answer: Yes, to county-owned mobile devices (90% iOS, 10% android).

120. Are corporate build/configuration standards in place for various platforms (network devices, operating systems, etc.), and if so, is it desirable to evaluate against those standards, etc. This process will determine the amount of time required to perform additional analysis and tuning of evaluation criteria.
Answer: Yes.

121. Can remote internal networks be scanned via a primary location, or would it be necessary to perform field visits to each in-scope location?
Answer: Remote networks are accessible.

122. If multiple locations need to be visited, how many locations are in scope?
Answer: N/A.

123. Are any of the internal applications a third-party provider?
Answer: See #1 under Clarifications/Revisions above.

124. Does SJC have intrusion detection capabilities? If so, is an objective of this test also to assess the SJC's intrusion detection capabilities?
Answer: No.

125. What is the total number of public-facing/external network IP addresses to be tested? (If providing an IP range, please indicate the estimated number of live IPs.)
Answer: See the response to #37 above.

126. Number of Web-based applications/ services to test (dynamic pieces of websites that users or other applications authenticate to - client portal, sales quote system).
Answer: See #1 under Clarifications/Revisions above.

127. Please confirm the approximate number of Web Servers is 35. Are these 35 Web servers in addition to the 30 live hosts?
Answer: See #1 under Clarifications/Revisions above.

128. Number of Website URLs to be tested?
Answer: See #1 under Clarifications/Revisions above.

129. Is the Web Application in scope to be tested? If so, please provide the following information:
Answer: See #1 under Clarifications/Revisions above.

    a. URL(s) (also need instance ID + IP)
    b. Links to be excluded from testing
    c. User Roles Count
    d. How many web service endpoints are there in scope?
    e. What are the number of functions per web service?
    f. Will testing be performed against a test environment or production? (test is preferred)

130. With respect to website testing, are web applications in scope, and how many are included?
Answer: See #1 under Clarifications/Revisions above.

131. How deep should testing go in the event of successful network penetration (i.e., just validation of vulnerability; network administrator access; server access, etc.)?
Answer: Validation is sufficient.

132. Are any external systems hosted by a third-party provider?
Answer: Yes, some Azure AD to Tyler Entergov and connections to cloud based apps like Invoice Cloud at Utilities.

133. Does SJC own and manage the network equipment at your external perimeter?
Answer: Yes.

134. Are there any test window restrictions for any of the test categories (Ext, Int, SE, Lock picking, Tailgating, etc.)?
Answer: None.

135. Is the target/goal of external testing similar to the internal testing goal of "attempting to connect to internal servers and other network devices to obtain accounts/passwords, acquire network information, and access SJC data"?
Answer: Yes.

136. What controls are in place for requesting, configuring, monitoring Partner Connectivity?
Answer: Controls are informal.

137. Is there a Partner Connectivity Agreement / Policy?
Answer: No.

138. How many individual Partner Connections are in scope?
Answer: See the response to #113 above.

139. Can Partner Connection be tested via a primary location, or would it be necessary to perform field visits to each in-scope location?
Answer: They can be tested from the primary location.

140. If multiple locations need to be visited, how many locations are in scope?
Answer: N/A.

141. Please confirm the number of Wireless Networks.
Answer: See the response to #110 above.

142. Please provide an estimate of the types of Wireless in use (microwave, 802.11x, proprietary, cell phone, blackberry, iPhone, Bluetooth, Point-to-Point, etc.).
Answer: 10 P2P wireless, 100 802.11x EAP-TLS clients, 500 public users, 200 cell phone users with RA.

143. Are formal wireless security policies in place?
Answer: No.

144. How many individual Partner Entities are in scope?
Answer: Only the handoff is in scope, not the partner.

145. Are these Application Interfaces (APIs), network trusts, scripted imports/exports from other systems?
Answer: Yes.

146. Can Partner Entities be tested via a primary location, or would it be necessary to perform field visits to each in-scope location?
Answer: Tested via the County.

147. If multiple locations need to be visited, how many locations are in scope?
Answer: N/A.

148. What controls are in place for requesting, configuring, monitoring remote access?
Answer: See the response to #136 above.

149. Is there a Remote Access Agreement / Policy?
Answer: Yes; can be provided after award.

150. Is this an assessment against policy, legitimate accounts, and configurations?
Answer: Yes.

151. Impersonation: If there is a person within the company you would like us to impersonate to gain access to information, please indicate who this should be. Otherwise, we will decide based on factors including tenure, position, and possible influence.
Answer: This will be determined with awarded firm.

152. Important User: We may make references to known associates or important users to influence someone's decision to provide us with information on their behalf. Please indicate who this 'important user' should be. Otherwise, we will decide based on factors including tenure, position, and possible influence.
Answer: See the response to #151 above.

153. Third-party Authorization: We may make claims that permission has already been granted by another associate for information.
Answer: Third-party authorization can be discussed after award.

154. SPAM: Do you wish for us to generate false advertisements in hopes of detecting users who decide to click on ads and hyperlinks?
Answer: Yes.

155. Spear Phishing: Through the process of sending an e-mail to users and falsely claiming to be a legitimate enterprise, we can potentially coerce a user into disclosing private information. Please indicate if this is a required assessment.
Answer: Yes.

156. Can employees log into webmail remotely? If so, what is the webmail URL?
Answer: Yes, this will be provided to the awarded firm.

157. Is email hosted internally? If not, who hosts the email services?
Answer: Internally.

158. What controls are in place for content/web filtering and alerting?
Answer: There are managerial controls by department, but should be evaluated.

159. Is there an acceptable Use / Internet Use Policy?
Answer: Yes; can be provided after award.

160. Is this an assessment against policy, configuration, and performance?
Answer: Yes, Yes, and No.

161. What Mobile Platforms are in scope?
Answer: See the response to #119 above.

162. How are Mobile devices being used for (e.g., email, two-way comms, application interfaces, GPS, mobile applications)?
Answer: All of these examples are being used.

163. What, if any, host configuration standards and procedures are in place?
Answer: There is a Mobile Iron MDM in place that should be evaluated

164. Is this assessment against policy and configuration standards?
Answer: Yes

165. How many Active Directory Trees are in use?
Answer: 2 (co/Internet); co includes 4 domains

166. Is role-based access used? How many roles?
Answer: Yes, unknown, most AD functions performed as specific domain admin.

167. Are user access audits periodically performed?
Answer: Yes, as needed or required.
168. What approach is expected for this assessment (i.e., total population or sampling)?
Answer: Respondents must submit as part of their Proposal an intended approach.

169. What, if any, password management tools are in use?
Answer: Informal and limited use of Keepass.

170. Please indicate the number of lines of code, the languages (e.g., C, C#, HTML, Web 2.0, ASP, etc.), the number of applications, etc., to help determine what is meant by "security code" review.
Answer: See #1 under Clarifications/Revisions above.

171. Are automatic source code evaluators acceptable (they are expensive!)?
Answer: See #1 under Clarifications/Revisions above.

172. Are developers available for interviews and confirmation of suspected problems?
Answer: Yes.

173. Are there policies that define system, network, and application logging configurations?
Answer: No.

174. Do any employees access systems in the BCA/Clerks office as well as other county operating systems? If so, how many employees & how many different roles?
Answer: Yes, unknown, and unknown.

175. Does St. Johns maintain an official social media presence? If so, what are the approved handles and who maintains the presence?
Answer: Yes, managed by the Public Affairs Office.

176. Are the servers located within datacenter facilities or in the cloud?
Answer: Local Datacenters with a small amount of Azure integration.

177. Does your organization have an IDS (Intrusion Detection System) or IPS (Intrusion Protection System)?
Answer: Yes.

178. Will St. John's County BCC provide the tools needed to perform the Assessments?
Answer: No.

179. Your Software Applications that were Developed Internally, What was the technology used? What is the language code of the applications?
Answer: See #1 under Clarifications/Revisions above.

180. Do these applications have public access, internal or both?
Answer: See #1 under Clarifications/Revisions above.

181. What is the timeframe you expect to get the results from this Assessment? ASAP, 1-5 months, more than five months?
Answer: This is TBD based upon negotiations and final agreement between County and awarded firm.

182. How many IP addresses are in scope for internal vulnerability assessment/penetration testing?
Answer: See the response to #31 above.

183. How many IP addresses are in scope for external vulnerability assessment/penetration testing?
Answer: See the response to #37 above.

184. Is code review in scope? If yes, what language and how many lines of code.
Answer: See #1 under Clarifications/Revisions above.

185. Are you looking for penetration testing into applications?
Answer: Yes.

186. What type of applications are in scope?
Answer: See #1 under Clarifications/Revisions above.

187. How many live web pages are in scope for testing on each application?
Answer: See #1 under Clarifications/Revisions above.

188. How many web forms (pages) that require user interaction?
Answer: See #1 under Clarifications/Revisions above.

189. What is the number and type of user roles?
Answer: Unknown, roles are normally dictated by AD user group through application.

190. If web services are to be tested, how many endpoints are in scope (i.e., number of parameters per method)?
Answer: See #1 under Clarifications/Revisions above.

191. How many users are in scope for social engineering?
Answer: 5 for direct, 1200 email users.

192. How many physical locations are to be tested?
Answer: See the response to #18 above.

193. What is the approximate total travel time between locations?
Answer: N/A.

194. How many ESSIDs are in scope at each location?
Answer: 3.

195. What is the extent of testing that you want performed on SCADA systems, since they are more sensitive? How many of these are in scope for the testing?
Answer: See #2 under Clarifications/Revisions above.

196. Is the County flexible on insurance requirements (e.g., as a small business with a largely remote workforce, we have determined that automobile insurance is not necessary within our business model)?
Answer: Proof of coverage at the required limits is necessary/required for any vehicle you are using to conduct business. If this is a personal vehicle you would provide your personal auto declaration page along with a statement signed by an officer of the corporation stating that no commercial/business vehicles are owned by the company.

197. Are there any systems currently being utilized which could be characterized as fragile (systems with tendency to crash)?
Answer: SJC has no knowledge of any such fragile systems.

198. Are there systems on the network which the client does not own, that may require additional approval to test?
Answer: No.

199. How many hosts (endpoints) are in the network and part of the scope?
Answer: See the response to #31 above.

200. Is the target environment mostly Windows based? If not, which technologies are used?
Answer: Primarily Windows based.

201. How many external IPs are in scope (local perimeter, cloud services, etc.)?
Answer: See the response to #37 above.

202. How many DNS domains are included?
Answer: Two (2); co.st-johns.fl.us and internet.co.st-johns.fl.us

203. How many web applications will need to be tested?
Answer: See #1 under Clarifications/Revisions above.

204. How many application roles will be tested (by app)?
Answer: See #1 under Clarifications/Revisions above.

205. Are any mobile applications in scope? Android vs. iOS
Answer: None that are internally developed

206. Is the source code available on request?
Answer: See #1 under Clarifications/Revisions above.

207. How many lines of code?
Answer: See #1 under Clarifications/Revisions above.

208. In what language is the application written?
Answer: See #1 under Clarifications/Revisions above.

209. For iOS, is the application available unencrypted?
Answer: N/A

210. For API Testing, how many features?
Answer: See #1 under Clarifications/Revisions above.

211. Can a swagger file be provided?
Answer: See #1 under Clarifications/Revisions above.

212. Is Social Engineering – Phishing to be included in the scope of activities?
Answer: Yes.

213. How many targets will be included in the testing?
Answer: See the response to #191 above.

214. Is Vulnerability Analysis (Vulnerability Scanning) to be included in the scope of activities?
Answer: Yes.

215. How many hosts need to be scanned/analyzed?
Answer: See the response to #31 above.

216. What is the number of distinct environments that should be evaluated (e.g. on-prem, cloud, business silos, etc.)?
Answer: Hosting is primarily on-prem with a small amount of Azure.

217. Relative to the environments to be evaluated, which environments use virtual machines and/or containers?
Answer: 10% physical and 90% Vmware.

218. Which cloud service providers are used (IaaS, SaaS & PaaS)?
Answer: Azure.

219. Please list your perimeter defense technologies currently used (e.g. Cisco ASA, CKP WAF):
Answer: Cisco ASA, Cisco Firepower, iBoss, Palo Alto RA.

220. Is your infrastructure self-managed? If not, by whom?
Answer: Self-managed.

221. For every environment (Google, AWS, Azure, etc.), please provide the following:
Answer:

    a. A network schema or logical diagrams is available upon request: **Yes**
    b. Number of regions for Azure services: **(1) one**
    c. Number of tenants in this cloud provider: **(1) one; primary domain sjcfl.us**
    d. Number of application services used in this provider: **(3) Duo, Tyler Enrgov**

222. Please describe the cloud strategy for each provider (Google, AWS, Azure, etc.), how the environment is used and its purpose.
Answer: Azure – using Azure AD (free) for use with cloud app registrations only at this time.

223. How much technical documentation is there? How many pages?
Answer: Technical documentation is available for the configuration of Tyler, Duo w/ Azure. Approx. 80 pages total.

224. How many users are in scope?
Answer: Approximately 1,200 domain users.

225. How many physical sites are in scope?
Answer: See the response to #18 above.

226. Which best describes the infrastructure: On-prem only, cloud only, or hybrid?
Answer: On-prem with Azure having a copy of AD.

227. Based on our understanding, the County's infrastructure is partially hosted on Azure. If yes, can the County provide an approximate count and type of devices/services deployed in Azure?
Answer: Only using Azure AD (free) at this time. No infrastructure is deployed in Azure.

228. Based on our understanding, the physical access reviews need to be conducted in 2 different locations (BCC and Clerk). Please confirm.
Answer: These are within the same campus.

229. Are the following services applicable to Clerk of Courts (Clerk) - Partner Connectivity, Interface to Partner Entities, Evaluate Client Remote Access to External Services and Evaluate Internal MIS Tools for Data Leakage?
Answer: No

230. Based on our understanding, the 'Partner Connectivity' service is limited to evaluating configurations of interface connection to partners, and 'Interface to Partner Entities' is limited to evaluating how controls are implemented to restrict access for the partners entities. Please confirm if our understanding is correct. If not, please explain the difference between the two in-scope services.
Answer: This is correct.

231. Can the County elaborate on the nature of activities expected to be performed as part of the following service - 'Evaluate Internal MIS Tools for Data Leakage'?
Answer: SJC MIS tools involved are various open source applications like Librenms, Oxidized, phpipam, and self-hosted github. Respondents should include in their approach how they will evaluate these tools for data leakage.

232. Does the County have a Mobile Device Management (MDM) solution installed in the County-owned mobile devices?
Answer: Yes, Mobile Iron.

233. The Scope of Services includes 'benchmarking' of the current security posture against industry standards. Is the County seeking financial as well as operational benchmarking?
Answer: No.

234. Is there an expectation that the scanning/pentesting would extend to the parties identified in the Partner Connectivity/Partner Entities section of the RFP, or do you require review of configurations/process documentation only in this space?
Answer: We require a configuration/process review only.

235. Our typical approach to pentesting would be to run basic scans and use other techniques to identify potential exploits which may succeed within your environment. We would then work with the County to prioritize these

items and run tightly controlled test on a subset of the environment. Is this acceptable to the County, or do you require full exploit testing for any vulnerability we discover?
Answer: This is acceptable.

236. Please provide a list of SCADA devices that would be included in the Vulnerability Scanning / Pen Testing exercises. If available, please provide previous scan results for these devices
Answer: See #2 under Clarifications/Revisions above.

237. Please provide details on current Social Engineering tools/studies the County currently uses.
Answer: The County currently uses Proofpoint's Security Awareness Training module.

238. For Mobile Device Security, please clarify if you are seeking a detailed review of each device or if you require a review of policies/procedures and tools in this area.
Answer: Review of policies and procedures only.

239. Please confirm the Indemnification clause identified in Item G. INDEMNIFICATION would be amended as it relates to penetration testing.
Answer: The County and the awarded firm shall come to agreement over the final provisions of the Contract, including the Indemnification language.

240. There are a few tasks that appear to require performance onsite, but will remote testing also be acceptable?
Answer: Yes.

241. Will any testing be required outside of normal business hours? I.e. evenings or weekends.
Answer: Not required.

242. This assessment will require interviews/discussions to be conducted in order to gain a more thorough understanding of the overall environment and security posture. Can an approximate number of relevant IT personnel/departments we'll need to engage for these activities be provided?
Answer: 7-10.

243. Will a selection of policies, procedures, and other relevant documentation be provided for review as part of the project?
Answer: Yes.

244. For internal testing, is a physical device permitted to be placed onsite? Alternatively, if setting up a VM is preferred, we can provide an OVA file to set up.
Answer: Either is permitted.

245. In evaluating partner connectivity, will this be addressed during the above-mentioned discussions as part of the overall architecture review/security assessment? I.e. Review of firewall rules, procedures, configurations, controls in place, etc., or is there another expectation for this task? I.e. Segmentation level testing of each partner to validate what each connection looks like. If the latter, will travel to these partner locations be required?
Answer: Review of policies and configurations is the expectation.

246. If in depth testing is expected, we are unable to perform this unless permission has been explicitly given to do so.
Answer: N/A.

247. In testing the wireless network(s), how many SSIDs and locations are in scope?
Answer: 3.

248. Is this task meant to be a full penetration test, including segmentation, or is a security review of architectural design and wireless configurations sufficient?
Answer: A full penetration test is required.

249. Is the physical access control evaluation intended to be a cooperative exercise or a stealthy endeavor?
Answer: Either is acceptable. Respondents shall submit their proposed approach as part of the Proposal, which shall be subject to final negotiations and approval by the County.

250. How many locations/buildings are in scope?
Answer: See the response to #18 above.

251. In evaluating tools for data leakage, are these host based as well as network based?
Answer: Yes.

252. Will county owned laptops and/or other devices be provided to complete some of these tasks, and if so, how many different devices need to be tested?
Answer: They can be. 1 device of each type is acceptable (laptop, mobile, etc).

253. For the social engineering component, will this consist of phishing exercises, or are other methods also requested?
Answer: We currently have a phishing test underway, we are looking for targeted testing to a small amount of users as well.

254. Is the goal of this task to test both employee awareness as well as controls in place?
Answer: Yes.

255. In evaluating the internally developed applications, is this meant to be an in-depth penetration test on each one? If so, how many user roles are in scope for each application?
Answer: See #1 under Clarifications/Revisions above.

256. Can a brief explanation of function and complexity for each application in scope be provided?
Answer: See #1 under Clarifications/Revisions above.

257. Are any APIs or other web services in scope for this project?
Answer: See #1 under Clarifications/Revisions above.

258. For Attachment H - Key Personnel, comprehensive, one-page resumes need to be provided as part of the submission. Would it be acceptable if these resumes were two-pages in length to ensure adequate experience is outlined for each of the consultants that would be part of this project?
Answer: No, resumes must be kept to one page.

259. Has this type of assessment been performed previously, and is there an estimated budget for this project?
Answer: See responses to #1 and #34 above.

260. Regarding trade secrets that will be included within the proposal submission, for ease of readability, would County accept an original hard copy of the proposal containing all required information, including information marked as "trade secret," and in addition, a separate, redacted copy of the proposal with all trade secret information redacted for release under a public records request? If yes, is it the County's preference that we include the redacted copy in a separate envelope from the original hard copy?

Answer: Respondents must comply with the requirements of Part III: Proposal Submittal Requirements, paragraph B. Trade Secrets to qualify any of the submitted information as Trade Secret or confidential.

261. Is it County's preference for vendors to include an electronic copy of the redacted proposal on the same USB drive as the original electronic copy?
Answer: See response to #272 above.

262. Within Attachment "I" on page 27 of the RFP, County states in the introductory paragraph that "respondents shall submit information on three (3) contracts and/or engagements." However, Attachment "I" contains 5 reference slots. Please confirm if County wants 3 or 5 references included within the proposal submission.
Answer: A minimum of three (3) references are required.

263. Does County have documented IT policies, procedures, standards, and guidelines in place? If so, how many?
Answer: Yes, less than ten (10).

264. Is County's IT organization centralized or decentralized?
Answer: Centralized.

265. What is County's budget for this project?
Answer: See the response to #1 above.

266. Is there an Active Directory assessment in scope? If so, how many users?
Answer: Yes, see response to #323 above.

267. How many physical locations will be included within the physical access controls evaluation?
Answer: See the response to #18 above.

268. Is an endpoint configuration review in scope? If so, how many should be tested?
Answer: Yes, one (1) of each type.

269. Is a VPN configuration review in scope? If so, how many appliances?
Answer: Yes, two (2).

270. Does County want vendors to provide copies of the engagement team's certifications as part of the proposal submission, or do they just want to know what certifications the consultants hold?
Answer: Respondents shall provide any and all documentation of the certifications for validation purposes.

271. The RFP references a comprehensive list of IT hardware and systems. Are the systems designated as "internal" currently located in a on-premise data center, a colocation data center, or a managed service (data center/cloud)?
Answer: Primarily on-prem with a small amount of Azure.

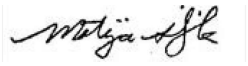
272. The RFP references multiple IT security frameworks, including NIST, OWSAP and SANS. Is there a particular standards-based control framework that St Johns county is managing against? If so, can you please provide it and its version? If Not, would a recommendation of standards-based control framework be valued as part of the assessment report?
Answer: No.

273. Is the partner connective listed a complete listing?
Answer: Yes, to the best of our knowledge.

The deadline for Questions is hereby extended to: Thursday, October 14, 2021 at 5:00PM EDST

The deadline for Proposal submittal is hereby extended to: Thursday, October 28, 2021 at 4:00PM EDST

Acknowledgment



10/26/2021

Signature and Date

Matija Siljak, CEO

Printed Name/Title

Illumant LLC

Company Name (Print)

END OF ADDENDUM NO. 1

About Illumant

Delivering confidence in all aspects of information security through assessment and penetration testing.

Illumant provides penetration testing, security assessment, awareness training, and security compliance services, to help its clients navigate the cyber-security threat and regulatory landscapes. Leveraging strategic and tactical risk management and information security expertise, Illumant partners with its clients to help them improve security, limit exposure, and achieve compliance objectives.

Illumant
431 Florence Street, Suite 210
Palo Alto, CA 94301
www.illumant.com
650-961-5911

ST. JOHNS COUNTY
BOARD OF COUNTY COMMISSIONERS

RFP NO. 22-06
REQUEST FOR PROPOSALS

CYBER SECURITY ASSESSMENT

St. Johns County Purchasing Division
500 San Sebastian View
St. Augustine FL 32084
(904) 209-0150 – Main
www.sjcfl.us/Purchasing/index.aspx

FINAL 9.10.21

TABLE OF CONTENTS

PART I: INTRODUCTION

A. TENTATIVE SCHEDULE OF EVENTS

The County proposes the tentative schedule of events below. The dates provided may change at the discretion of the County. If any modifications impact the schedule of this RFP, through and until the deadline for submitted proposals, the County will notify all interested respondents via Addendum.

Advertisement of RFP	September 14, 2021
Deadline for Questions	September 30, 2021
Issuance of Final Addendum	October 7, 2021
Proposal Submission Deadline	October 14, 2021
Evaluation of Proposals	October 28, 2021
Issue Final Contract	December 21, 2021

B. DUE DATE & LOCATION

Proposals submitted in response to this RFP must be delivered to, and received by the SJC Purchasing Department by or before **four o'clock (4:00PM EDST)** on **Thursday, October 14, 2021**. Any proposals received by the SJC Purchasing Division after this deadline will be deemed non-responsive, and shall be returned to the Respondent, unopened.

Proposals must be submitted to:

SJC Purchasing Division
500 San Sebastian View
St. Augustine, FL 32084

C. DESIGNATED POINT OF CONTACT

Any and all questions or requests for information relating to this RFP must be directed, ***in writing,*** to the following Designated Point of Contact provided below:

Designated Point of Contact Information:

April Bacon, Purchasing Buyer
SJC Purchasing Division
500 San Sebastian View
St. Augustine, FL 32084
Email: abacon@sjcfl.us

In the event the Designated Point of Contact provided above is absent or otherwise unavailable for more than three (3) business days, firms may contact Leigh A. Daniels, CPPB, Purchasing Manager at ldaniels@sjcfl.us.

Interested firms **SHALL NOT** contact any staff member of St. Johns County, including members of the Board of County Commissioners, except the above referenced individual, with regard to this RFP as stated in SJC Purchasing Code 304.6.5 "Procedures Concerning Lobbying". All inquiries will be routed to the appropriate staff member for response. Any such communication may result in disqualification from consideration for award of a contract for these services.

D. SUBMITTAL OF QUESTIONS/INQUIRIES

Any and all questions and/or inquiries related to this RFP, shall be directed, in writing, to the Designated Point of Contact as provided above, by or before **five o'clock (5:00PM) EDST** on **Thursday, September 30, 2021**. Any questions received after this deadline will not be addressed or clarified by the County, unless it is determined to be in the best interest of the County to do so. The County reserves the right to extend the deadline for submittal of proposals in order to clarify or answer questions as necessary to serve the best interest of the County.

E. ADDENDA

Any and all clarifications, answers to questions, or changes to this RFP shall be provided through a County issued Addendum, posted on www.demandstar.com. Any clarifications, answers, or changes provided in any manner other than a formally issued addendum, are to be considered "unofficial" and shall not bind the County to any requirements, terms or conditions not stated herein.

The County shall make every possible, good faith effort to issue any and all addenda no later than seven (7) days prior to the due date for proposals. Any addenda issued after this date shall be for material, necessary clarifications to the Request for Proposals, unless otherwise approved by the Purchasing Manager.

Any and all issued Addenda must be signed and included with all copies of each Respondent's submitted proposal. Failure to include any issued addendum with the submitted proposal may result in the Respondent being deemed non-responsive, and being removed from consideration for award. The County reserves the right to request from any Respondent, copies of any missing addenda, if the content included in the Addenda is not of a material nature to the merit of the submitted proposal.

F. EQUAL EMPLOYMENT OPPORTUNITY

In accordance with Federal, State and Local law, Respondents shall not discriminate against any employee or applicant for employment because of race, color, religion, sex, national origin, or handicap. The awarded firm(s) shall be required to comply with all aspects of the Americans with Disabilities Act (ADA) during the performance of the work.

G. SOLICITATION POSTPONEMENT/CANCELLATION

The County may, at its sole and absolute discretion, postpone, cancel, or re-advertise, at any time, this solicitation process for any reason, as determined by County Staff, in order to best serve the interests of St. Johns County.

H. RIGHT TO REJECT/ACCEPT

The County reserves the right to accept or reject any or all proposals, waive minor formalities, and to award to the Respondent that best serves the interest of St. Johns County.

I. COMPLIANCE WITH ST. JOHNS COUNTY PURCHASING POLICY AND PROCEDURES MANUAL

All terms and conditions of the St. Johns County Purchasing Procedure Manual are incorporated into this RFP Document by reference, and are fully binding. Respondents are required to submit their responses to this RFP, and to conduct their activities during this process in accordance with the St. Johns County Purchasing Procedure Manual. This solicitation, the subsequent evaluation, negotiations and contract award shall be in accordance with the St. Johns County Purchasing Procedure Manual. The County reserves the right to disqualify, remove from consideration, or debar as appropriate, any vendor that does not comply with the applicable requirements set forth in the St. Johns County Purchasing Procedure Manual.

J. LOCAL PREFERENCE

Per Section 302.25 of the SJC Purchasing Procedure Manual, the County shall review all submitted proposals to determine whether or not the Respondent qualifies for consideration as a Local Business. Staff shall provide the appropriate consideration of local preference to those submitted proposals, in accordance with SJC Purchasing Policy.

PART II: GENERAL REQUIREMENTS

A. GENERAL INFORMATION

The St. Johns County Board of County Commissioners (BCC) supports a local and wide area network for the Board of County Commissioners, Clerk of Courts and the Sheriff's Office.

These networks contain servers, SANs, desktop computers, laptops, software applications, wireless access points, firewalls, switches, wireless LAN controllers, VPN gateways, PKI, NPS, cameras and security access devices.

The BCC supports Internet and Intranet services, internally developed applications, Cisco Call Manager, Utility SCADA system, Mobile Device Management, Access Control System and HVAC Control System.

The Clerk of Courts (Clerk) supports countywide judicial operations primarily relegated to the Judicial Center and Judicial Datacenter. These applications and servers are related to billing, official records, licensing, and court related matters.

BCC

Device or Service	Approximate Count (Internal/External)	Notes
Servers	300/50	Virtual and physical servers, SAN devices
Internally Developed Software Applications	100/10	
Desktop/Laptop Computers	1300	
Corporate-owned Mobile Phones and Tablets	550	iOS and Android
Wireless Access Points	250 and 3 WLCs	Cisco 3402
Routers/Switches	470/6	All Cisco
Firewalls	25/4	ASA moving towards Palo Alto
Web Service APIs	10	
SCADA	420/0	Servers, desktops, and field devices

CLERK

Device or Service	Approximate Count (Internal/External)	Notes
Hypervisor Nodes	4	
Internal and DMZ Servers	112	

B. SCOPE OF SERVICES

Benchmark existing IT security practices and procedures against NIST 800-53, OWASP, SANS, and other applicable industry standards. Review the gaps and observations with MIS management and make suggestions to revise and align BCC information security standards with best practices.

Vulnerability Assessment – Perform an in-depth cybersecurity vulnerability assessment and penetration testing of BCC/SJCC/SJSO's logical and physical IT infrastructures.

Internal Network – All internal systems to include workstations, servers, switching/routing infrastructure, virtualization and storage infrastructure, and other connected IT devices. Including all (DMZ) systems to include flow controls from external to internal systems. In addition, focus on SCADA, IOT, and Building Control/Security is desired.

External Network – All external public facing systems to include firewalls, proxy, web servers, ftp servers, VPN ingress, Azure interfaces, and internally developed outward facing web applications.

Partner Connectivity – Evaluate communications methods and configurations with partner billing entities (Cogsdale, Lexis-Nexus, Sunguard/Pentamation)

Wireless Network – All wireless systems to include internal touch points from all SSID, broadcast or hidden, as well as encryption levels.

Physical Access Controls Evaluation – Determine if the current physical security is effective.

Interface to Partner Entities – Evaluate access to partner entities including City PD/FR, e911, Supervisor of Elections, State Attorney, Public Defender, School Board, Traffic, Tax, CJNET

Evaluate Client Remote Access to External Services – Citrix, VPN, RDP

Evaluate Internal MIS Tools for Data Leakage – Oper, WO, Inventory and Network tools Librenms, Oxidized, GitRepo

Social Engineering Component – evaluate social engineering efforts to verify the existence and effectiveness of procedural controls to prevent unauthorized physical and electronic access to BCC IT systems.

Internet Usage – Assess URL/web filtering and access restrictions.

Mobile Device Security – Assess all County-owned mobile devices and security policies for managing the devices and security of network connections. Assess security for BYOD devices as applicable to the County's network.

Host Based Security – Assess security of critical systems at operating system and database layers and associated identity and access management controls.

Evaluation of user rights/permissioning and assignment procedures

Evaluate MIS Teams password and management access procedures

Evaluate internally developed applications for common vulnerabilities

Evaluate Security logging practices

1. **Key Deliverables:**

- Provide detailed reports on testing and attack scenarios used, vulnerabilities discovered, including the risk rating
- Provide Executive Summaries with overall severity findings and risk exposure relatable and understandable to non-technical management as much as possible and comparison to other similarly sized entities
- Detailed explanations of the implications of findings, business impacts, and risks for each of the identified exposures with technical teams
- Remediation recommendations to close the deficiencies identified along with detailed steps (wherever/whenever applicable) to be followed while mitigating the reported deficiencies
- Penetration Testing- perform non-volatile exploit procedures designed to determine how well BCC systems can withstand up-to-date malicious exploits. Penetration testing should be performed from two perspectives:
    a. An outside attacker with no approved system access.
    b. A malicious insider who has access to the system.
    c. Evidence gathered as proof of access must not harm the confidentiality, integrity, or availability of the systems, application, and or data. Special attention should be given to areas that contain high risk data. These procedures should be performed without the knowledge of BCC IT staff.
- Security Strategy and Systems Report from evaluation of BCC firewall hardware, software, placement and

utilization. Perform an in-depth security scan and threat assessment to identify vulnerabilities. This should include, but not be limited to, port scans, host enumeration, and application/system identification.

- Recommendations of changes to current AD Security Policies
- Connections to External Partners Report - review our connection and security posture to our external partners through wide area networks, dedicated circuits, VPNs, remote clients, and remote server technologies; Assess remote access and security of network connections and data traffic between all campus locations and partner entities
- Inbound and Outbound Remote Access Strategy – evaluate administration of remote access, both inbound and outbound. Review implications associated with the level of access that has been granted to authorize users including Internet access.
- Internet Usage – evaluate how BCC secures sensitive data and applications: how we block or allow unnecessary and unauthorized websites: and the tools we use for monitoring the URLs, links and Web pages that were visited. Identify any immediate problems. Assess URL/web filtering and access restrictions.
- Endpoint Protection - evaluate the software used to prevent impact from malicious software. Perform a threat assessment to identify vulnerabilities.
- Logon Security - evaluate password policies and review current logon auditing practices.
- Reporting on ongoing RBAC and auditing procedures

2. Final Report:

The report on outcomes from the evaluation should include the following at a minimum:

- Separate reports for the BCC and Clerk organizations.
- Time tracking showing a percentage of work done for each organization (BCC and Clerk) for the purposes of individual cost distribution
- Purpose of the vulnerability assessment/Penetration test (Compliance with regulations (PCI, HIPPA, etc.), best practices.
- The company name and the names of the testers and their credentials.
- The reports should include what tools were used to perform the tests.
- The reports should detail the duration of the tests.
- Executive summaries, in fairly non-technical language that can be shared with Upper level management
- Details of the vulnerabilities that were found, and in the case of a penetration test, should include whether the consultants were able to successfully exploit the vulnerabilities.
- Details of External Penetration tests
- Details of Internal Penetration tests
- Details of Wireless Network tests
- Details of Web Application tests

- Results of any Social Engineering tests such as Phishing that were performed.
- The report should include a risk rating for each vulnerability found to aid in establishing the priority of remediation.
- If the assessment found sensitive information (PII, SSN, HIPPA info, etc.)
- Remediation steps should be included for each of the vulnerabilities found. If there is no remediation available (for example end of life devices or software) that should also be noted.
- Roadmap and priorities for planning the next steps for remediation and future prevention.

PART III: PROPOSAL SUBMITTAL REQUIREMENTS

A. RESPONDENT RESPONSIBILITIES

Respondents are responsible for any and all costs associated with developing and submitting a proposal in response to this RFP. Respondents are also solely responsible for any and all costs associated with interviews and/or presentations requested by the County. It is expressly understood, no Respondent may seek or claim any award and/or re-imbursement from the County for any expenses, costs, and/or fees (including attorneys' fees) borne by any Respondent, during the entire RFP process. Such expenses, costs, and/or fees (including attorneys' fees) are the sole responsibility of the Respondent.

All proposals received in response to this RFP shall become the property of St. Johns County and will not be returned. In the event of contract award, all documentation produced as part of the contract will become the exclusive property of St. Johns County.

By submitting a proposal, each Respondent certifies that the proposer has fully read and understands any and all instructions in this RFP, and has full knowledge of the scope, nature, and quality of work to be performed. All submitted proposals shall be binding for one hundred twenty (120) consecutive calendar days

B. TRADE SECRETS

To qualify any submitted information as Trade Secret, or confidential, the Respondent must mark each page of the submitted proposal or specific portion of a document as "trade secret." All material marked as a trade secret must be separated from all non-trade secret material, such as being submitted in a separate envelope clearly marked as "trade secret." If the County receives a public records request for a document or information that is marked and certified as a trade secret, the County shall release any information not verified as "trade secret", in accordance with applicable Public Records laws.

To invoke the provisions of Florida Statute 812.081, Trade Secrets, or other applicable law, the requesting firm must complete an Affidavit for Trade Secret Confidentiality, signed by an officer of the company, and submit the affidavit with the information classified as "Trade Secret" with other proposal documents. The affidavit must reference the applicable law or laws under which trade secret status is to be granted.

C. PUBLIC RECORDS

1. The cost of reproduction, access to, disclosure, non-disclosure, or exemption of records, data, documents, and/or materials, associated with the awarded Agreement shall be subject to the applicable provisions of the Florida Public Records Law (Chapter 119, Florida Statutes), and other applicable State and Federal provisions. Access to such public records, may not be blocked, thwarted, and/or hindered by placing the public records in the possession of a third party, or an unaffiliated party.

2. In accordance with Florida law, to the extent that Consultant's performance under the awarded Agreement constitutes an act on behalf of the County, Consultant shall comply with all requirements of Florida's Public Records Law. Specifically, if Consultant is expressly authorized, and acts on behalf of the County under the awarded Agreement, Consultant shall:

(a) Keep and maintain public records that ordinarily and necessarily would be required by the County in order to perform the Services;

(b) Upon request from the County's custodian of public records, provide the County with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost as provided in Chapter 119, Florida Statutes, or as otherwise provided by law;

(c) Ensure that public records related to this Agreement that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by applicable law for the duration of this Agreement and following completion of this Agreement if the Consultant does not transfer the records to the County; and

(d) Upon completion of the awarded Agreement, transfer, at no cost, to the County all public records in possession of the Consultant or keep and maintain public records required by the County to perform the Services.

If the Consultant transfers all public records to the County upon completion of the awarded Agreement, the Consultant shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Consultant keeps and maintains public records upon completion of the awarded Agreement, the Consultant shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the County, upon request from the County's custodian of public records, in a format that is compatible with the County's information technology systems.

Failure by the Consultant to comply with the requirements of this section shall be grounds for immediate, unilateral termination of the awarded Agreement by the County.

IF THE CONSULTANT HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO ITS DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THE AWARDED AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT:

500 San Sebastian View
St. Augustine, FL 32084
(904) 209-0805
publicrecords@sjcfl.us

D. USE OF COUNTY LOGO

Pursuant to, and consistent with, County Ordinance 92-2 and County Administrative Policy 101.3, Respondents may not manufacture, use, display, or otherwise use any facsimile or reproduction of the County Seal/Logo without express written approval of the Board of County Commissioners of St. Johns County, Florida.

Respondents shall not include the St. Johns County Seal/Logo in any part of their submitted proposal. Any proposals received by the SJC Purchasing Department, which contain the County Seal/Logo may be deemed nonresponsive to this requirement. The County reserves the right to request the submitting firm to resubmit a proposal with the County Seal/Logo removed, within twenty four (24) hours of the submittal deadline provided herein, or as necessary to serve the needs of the County.

E. CONFLICT OF INTEREST

Respondents must certify that they presently have no interest and shall acquire no interest, either directly or indirectly, which would conflict in any manner with the performance of required services as provided herein. Respondents must certify that no person having any interest shall be employed for the performance of any of the required services as provided herein.

Respondents are required to disclose to the County any and all potential conflicts of interest for any prospective

business association, interest or circumstance, the nature of work the Respondent may undertake and request an opinion from the County, whether such association, interest, or circumstance constitutes a conflict of interest.

F. PROPOSAL SUBMITTAL FORMAT

The proposal format must sufficiently address and demonstrate all required components, and follow the order of sections described below. The aim of the required format is to simplify the preparation and evaluation of the submitted proposals.

G. PROPOSAL COMPONENTS

All of the components outlined below must be included with each copy of the proposal and submitted as follows: one (1) original hard copy original only and one (1) exact electronic copy on USB drive, submitted in a sealed envelope or container labeled with Company name and RFP Number and name. Additionally, all headings, sections and sub-sections shall be identified appropriately. In order to ensure a uniform review process and to obtain the maximum degree of comparability, it is recommended that proposals be organized in the manner specified as follows:

Section 1: RFP Cover Page (Complete and Submit) and Cover Letter

Respondents shall provide a cover letter. Include the original signed cover letter with the original proposal and a copy of the cover letter with the PDF copy of the proposal. The cover letter should provide the following:

- Full legal company name, company type, and primary phone and email address,
- Physical address and mailing address (if different) (include location address of office that will perform the services under Contract),
- Names and titles of principals,
- Brief statement of company history (date of establishment, number of years in business, number of employees, etc.),
- Brief description of business philosophy, and
- Reason for interest in submitting a response to this solicitation.

Delegation of Authority

If the individual signing the required forms in the proposal is not a principal of the firm, Respondent must provide with the submitted proposal a Letter of Delegation of Authority listing agents of the Respondent authorized to negotiate on behalf of and contractually bind the Responding Firm. The Letter of Delegation of Authority must be on company letterhead, be signed by a principal of the Responding firm, and must list the authorized agents' name, title, and limit of authority.

Section 2: Qualifications

Respondents shall describe, in detail, the firm's history by providing length of time in business, business history including patterns of growth, mergers or acquisitions, number of staff, number of customers, market/vertical specializations, office locations, and length of time offering services similar to those outlined in the scope of services. In addition, provide a brief summary of the firm's overall capabilities to perform the services as outlined in the scope of services.

Respondents shall provide evidence that the firm has qualified and experienced staff to perform the scope of services by describing, in detail, the experience and qualifications of key personnel proposed to work on this project, including relevant certifications, length of time working in a cybersecurity field, areas of specialization, and experience with handling Cybersecurity Assessments.

Respondents shall complete and submit the following attachments to fully demonstrate the firm's Key Personnel's qualifications:

Attachment "H": Key Personnel – submit information to demonstrate the qualifications and experience of Key Personnel. Brief (one page) comprehensive resumes should be provided for each member listed.

Section 3: Project Approach
Respondents shall describe, in detail, any and all specific methodologies, ranking/measurement methodologies, proposed areas of focus, proposed tools, etc. that will be utilized during the Cybersecurity assessment. In addition, provide a detailed timeline, schedule, milestones, etc. associated with the different tasks and/or steps of the proposal.

Section 4: Proposed Pricing
Respondents shall submit a Total Price for Cybersecurity Assessments for both the BCC and Clerk locations as detailed in the pricing proposal included herein as **Attachment "J" – Pricing Proposal Form**, to be used for any services authorized under the awarded Contract. For the purposes of evaluation, proposed Total Prices shall be averaged and scored by the formula provided herein.

Section 5: References & Technical Experience
Respondents shall submit information on three (3) contracts and/or engagements successfully completed in the last five (5) calendar years of similar scope to the outline scope of services described herein. Respondents must include the type of services performed, timeframe of performance, whether or not the contract was renewed/extended, and all contact information for a point of contact at the reference agency or organization. This information shall be submitted on **Attachment "I"** provided herein.

Section 6: Administrative Information
Respondents shall submit the following forms:

- Attachment "A" – Affidavit of Solvency;
- Attachment "B" – St. Johns County Affidavit;
- Attachment "C" – Conflict of Interest Disclosure;
- Attachment "D" – Drug-Free Workplace Form;
- Attachment "E" – Local Preference;
- Attachment "F" – Certificate(s) of Insurance;
- Attachment "G" – Claims, Liens, litigation History; and
- Attachment "K" – E-Verify Affidavit
- All Signed Addenda (if applicable)

H. DETERMINATION OF RESPONSIVENESS

The County shall make a determination for each Respondent, as to the responsiveness of the submitted proposal to the requirements provided herein. Any Respondent who is not responsive to the requirements of this RFP may be determined non-responsive, and may be removed from consideration by the Evaluation Committee. Only those respondents who are fully responsive to the requirements herein will be evaluated for consideration of award.

The County reserves the right to waive any minor formality or irregularity in any submitted proposal. However, any missing information or document(s) that are material to the purpose of the RFP shall not be waived as a minor formality.

I. EVALUATION OF PROPOSALS

All properly submitted proposals determined to be responsive to the requirements of this RFP will be evaluated by an Evaluation Committee of no less than three (3) representatives. Evaluators will review and score the proposals individually, with no interaction or communication with any other individual. Scores and rankings will be summarized at the Public Evaluation Meeting. The highest ranked firm will be recommended for award. If the Evaluation Committee determines that additional interviews and/or presentations are necessary to make a final decision for selection, the three highest ranked firms will be notified. If required, presentations will be scored by

the Evaluation Committee as provided herein. The firms will be notified, as needed, of the required information that must be included in any presentation.

County Staff may consider any evidence available regarding financial, technical, and other abilities of a respondent, including past performance (experience) with the County prior to recommending approval of award to the St. Johns County Board of County Commissioners.

J. EVALUATION CRITERIA AND SCORING

The County will evaluate and rank respondents that submit proposals from highest to lowest based upon the specific evaluation criteria as associated points listed below.

Evidence of Respondent's qualification as a Local Business in accordance with Section 302.25 SJC Purchasing Procedure Manual. Local Preference shall be scored on a scale of 0 – 10 points. Respondents that meet all qualification criteria as a local business shall receive 10 points. Respondents that do not meet all criteria as a local business shall receive 0 points.

Evaluation Criteria:	**Maximum Possible Points per Evaluator:**
A. Qualifications	**30**
B. Project Approach	**25**
C. Proposed Pricing	**20**
D. References & Technical Experience	**15**
E. Local Preference	**10**
F. Quality of Submittal	**10**
Total Points Possible:	**110**
G. Presentations (if required):	***20***
Total Points Possible:	***130***

L. FORMULA FOR PRICING PROPOSAL:

The proposed Total Price for Cybersecurity Assessments for both the BCC and Clerk locations submitted by each Respondent shall be averaged and scored in accordance with the formula provided below. The lowest average Total Price for Cybersecurity Assessments shall receive twenty (20) points and all other average Total Price for Cybersecurity Assessments shall be scored through a pro rata distribution of points as shown below:

Vendor	Average Total Price	Percentage	By	Weight	Equals	Weighted Score***
A	$250.00	100.0	X	20	=	20
B	$275.00	90.0*	X	20	=	18
C	$300.00	83.3**	X	20	=	16.66

* Vendor B's percentage is $250.00 ÷ $275.00 = 90.0%

** Vendor C's percentage is $250.00 ÷ $300.00 = 83.3%

M. PRESENTATIONS BY FIRMS:

In the event the County determines that presentations from firms are necessary to make a final recommendation, the firms selected to make presentations will be notified by the County. Presentations will be evaluated by the Evaluation Committee, and the scores for the presentations shall be added to the scores for the proposal for each firm, to determine the Total Score for each firm. The criteria by which presentations will be scored will be provided to the firms with the above referenced notification by the County.

N. RECOMMENDATION FOR AWARD

Recommendation shall be made to the Board of County Commissioners by County Staff to enter into negotiations with the highest ranked firm as determined by the Evaluation Committee, with the intention of coming to agreement over terms, conditions, and pricing in order to award a Contract for the services described herein.

In the event that negotiations are unsuccessful and an agreement cannot be reached with the highest ranked firm, staff will cease negotiations, and begin negotiations with the next highest ranked firm. This process will continue until such time as an agreement can be reached, or the County, in its sole discretion, determines that moving to a subsequent firm would not be in the best interest of the County.

The St. Johns County Board of County Commissioners reserves the right to reject any or all proposals, waive minor formalities or award to/negotiate with the firm whose proposal best serves the interest of the County.

O. PROTEST PROCEDURES

Any Respondent adversely affected by an intended decision, or by any term, condition, or procedure or specification with respect to this Request for Proposals, shall file, with the SJC Purchasing Department, a written Notice of Protest, no later than seventy two (72) hours (excluding Saturdays, Sundays, and legal holidays for employees of St. Johns County) after the posting, either electronically, or by other means, of the notice of intended action, notice of intended award, bid tabulation, publication by posting electronically or by other means of a procedure, specification, term or condition which the person intends to protest, or the right to protest such matter shall be waived. The protest procedures may be obtained from the SJC Purchasing Department, and are included in St. Johns County's Purchasing Manual. All of the terms and conditions of the County's Purchasing Manual are incorporated into this Request for Proposals by reference, and are fully binding.

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ST. JOHNS COUNTY FLORIDA
BOARD OF COUNTY COMMISSIONERS

DATE:

CRITERIA RANKING:

RESPONDENTS	A.	B.	C.	D.	E.	F.	TOTALS
	QUALIFICATIONS 0 to 30	PROJECT APPROACH 0 to 25	PRICING 0 to 20	REFERENCES & TECHNICAL EXPERIENCE 0 to 15	LOCAL PREFERENCE 0 to 10	QUALITY OF SUBMITTAL 0 to 10	0 - 110

SIGNATURE OF RATER:_____ **PRINT NAME:**_____ **DATE:** _____

PART IV: CONTRACT REQUIREMENTS

A. CONTRACT AGREEMENT & TERM

It is anticipated the County will issue an Agreement with a term of one (1) calendar year, contingent upon satisfactory performance by the Consultant. The County reserves the right to extend this Agreement beyond the initial term, as needed, for the successful completion of the required services. Any extension of this Agreement shall not exceed one (1) calendar year, unless approved by the County Administrator, or designee, shall be at the option of the County, must be in writing, and agreed to by both parties providing that satisfactory performance has been maintained by the Consultant, there is availability of appropriated funds, and that the County has a continued need for the services.

The County may consider extending any executed Agreement under mutually acceptable terms and conditions. However, the County is under no obligation to extend any executed Agreement. Moreover, it is expressly understood that the option of renewal and/or extension is exercisable only by the County, and only upon the County's determination of satisfactory performance of any executed Agreement, including specifically, the Scope of Work/Services. Any contract renewal will be upon mutual agreement by all parties and based upon the availability of funds and the need for services.

In the event that an Agreement is attached to the RFP, such attached Agreement is for discussion purposes only, and not necessarily reflective of any Agreement that may be ultimately entered into by the County. In the event that an Agreement is not attached to the RFP, it is expressly understood that the Board of County Commissioner's (Board's) preference/selection of any proposal does not constitute an award of an Agreement with the County. It is anticipated that subsequent to the Board's preference/selection of any proposal, negotiations will follow between the County and the selected Respondent. It is further expressly understood that no contractual relationship exists with the County until an Agreement has been executed by both the County and the selected Respondent. The County reserves the right to delete, add to, or modify one or more components of the selected Respondent's proposal in order to accommodate changed or evolving circumstances that the County may have encountered since the issuance of the RFP.

B. PERFORMANCE REVIEW

At any point in time during the term of the Agreement with the awarded firm(s), County Staff may review records of performance to ensure that the awarded firm is continuing to provide sufficient financial support, equipment and organization as prescribed herein. The County may place said contract on probationary status and implement termination procedures if the County determines that an awarded firm no longer possesses the financial support, equipment and organization which would have been necessary during the RFP evaluation period in order to comply with this demonstration of competency section.

C. TERMINATION

Failure on the part of the Consultant to comply with any portion of the duties and obligations under the awarded Agreement shall be cause for termination. If the Consultant fails to perform any aspect of the responsibilities described herein or as designated in the contract, St. Johns County shall provide written notification stating any and all items of non-compliance. The Consultant shall then have seven (7) consecutive calendar days to correct any and all items of non-compliance. If the items of non-compliance are not corrected, or acceptable corrective action, as approved by the County, has not been taken within the seven (7) consecutive calendar days, the Agreement may be terminated by St. Johns County for cause, upon giving seven (7) consecutive calendar days written notice to the Consultant.

In addition to the above, the County may terminate the Agreement at any time, without cause, upon thirty (30) days written notice to the Consultant.

D. GOVERNING LAWS & REGULATIONS

It shall be the responsibility of the Consultant to be familiar and comply with any and all federal, state, and local laws, ordinances, rules and regulations relevant to the services to be performed under this Contract. The Agreement shall be governed by the laws of the State of Florida and St. Johns County both as to interpretation and performance.

E. LICENSES, PERMITS & CERTIFICATIONS

The Consultant shall be responsible for acquiring and maintaining any and all necessary licenses, permits, and/or certifications required to perform the work described herein throughout the duration of the Agreement. The Consultant shall be solely responsible for paying any and all fines, penalties or fees assessed to the County, or the Consultant, for any lapse in require licenses, permits, or certifications required for any portion of the work.

F. INSURANCE REQUIREMENTS

The Consultant shall not commence work under the awarded Agreement until he/she has obtained all insurance required under this section and such insurance has been approved by the County. All insurance policies shall be issued by companies authorized to do business under the laws of the State of Florida. The Consultant shall furnish proof of Insurance to the County prior to the commencement of operations. The Certificate(s) shall clearly indicate the Consultant has obtained insurance of the type, amount, and classification as required by contract and that no material change or cancellation of the insurance shall be effective without thirty (30) days prior written notice to the County. Certificates shall specifically include the County as Additional Insured for all lines of coverage except Workers' Compensation and Professional Liability. A copy of the endorsement must accompany the certificate. Compliance with the foregoing requirements shall not relieve the Consultant of its liability and obligations under the awarded Agreement.

Certificate Holder Address: St. Johns County, a political subdivision of the State of Florida
500 San Sebastian View
St. Augustine, FL 32084

The Consultant shall maintain throughout the duration of the Agreement, Comprehensive General Liability Insurance with minimum limits of $1,000,000 per occurrence, $2,000,000 aggregate, to protect the Consultant from claims for damages for bodily injury, including wrongful death, as well as from claims of property damages which may arise from any operations under this contract, whether such operations be by the Consultant or by anyone directly employed by or contracting with the Consultant.

The Consultant shall maintain throughout the duration of the Agreement, Professional Liability or Errors and Omissions Insurance (sometimes termed Technology Professional Liability Tech E&O) with minimum limits of $1,000,000, if applicable.

The Consultant shall maintain throughout the duration of the Agreement, Cyber Liability Insurance with minimum limits of $1,000,000, if applicable.

The Consultant shall maintain throughout the duration of the Agreement, Comprehensive Automobile Liability Insurance with minimum limits of $300,000 combined single limit for bodily injury and property damage liability to protect the Consultant from claims for damages for bodily injury, including the ownership, use, or maintenance of owned and non-owned automobiles, including rented/hired automobiles whether such operations be by the Consultant or by anyone directly or indirectly employed by a Consultant.

The Consultant shall maintain throughout the duration of the Agreement, adequate Workers' Compensation Insurance in at least such amounts as are required by the law for all of its employees per Florida Statute 440.02.

In the event of unusual circumstances, the County Administrator or his designee may adjust these insurance requirements.

G. INDEMNIFICATION

To the fullest extent permitted by law, the Consultant shall indemnify, defend, and hold harmless St. Johns County, Florida, and employees from and against liability, claims, damages, losses and expenses, including attorney's fees, arising out of or resulting from performance of the Work, provided that such liability, claims, damage, loss or expense is attributable to bodily injury, sickness, disease or death, or injury to or destruction to tangible property (other than the Work itself) including loss of use resulting there from, but only to the extent caused in whole or in part by negligent

acts or omissions of the Consultant, a Sub-Consultant, or anyone directly or indirectly employed by them or anyone for whose acts they may be liable, regardless of whether or not such liability, claim, damage, loss or expense is caused in part by a party indemnified hereunder.

In claims against any person or entity indemnified under this Paragraph by an employee of the Consultant, a Sub-Consultant, any one directly or indirectly employed by them or anyone for whose acts they may be liable, the indemnification obligation under this Paragraph shall not be limited by a limitation on amount or type of damages, compensation or benefits payable by or for the Consultant or a Sub-Consultant under workers' compensation acts, disability benefits acts or other employee benefit acts.

H. EMPLOYMENT ELIGIBILITY AND MANDATORY USE OF E-VERIFY

As a condition precedent to entering into the awarded Agreement, and in accordance with section 448.095, F.S., Consultant and its sub-consultants shall register with and use the E-Verify system to verify the work authorization status of all employees hired on or after January 1, 2021.

a. Consultant shall require each of its sub-consultants to provide Consultant with an affidavit stating that the sub-consultant does not employ, contract with, or subcontract with an unauthorized alien. Consultant shall maintain a copy of such affidavit for the duration of the awarded Agreement.

b. The County, Consultant, or any sub-consultant who has a good faith belief that a person or entity with which it is contracting has knowingly violated section 448.09(1), F.S. or these provisions regarding employment eligibility shall terminate the contract with the person or entity.

c. The County, upon good faith belief that a sub-consultant knowingly violated these provisions regarding employment eligibility, but Consultant otherwise complied, shall promptly notify Consultant and Consultant shall immediately terminate the contract with the sub-consultant.

d. The County and Consultant hereby acknowledge and mutually agree that, a contract terminated pursuant to these provisions regarding employment eligibility is not a breach of contract and may not be considered as such. Any contract terminated pursuant to these provisions regarding employment eligibility may be challenged in accordance with section 448.095(2)(d), F.S.

e. Consultant acknowledges that, in the event that the County terminates the awarded Agreement for Consultant's breach of these provisions regarding employment eligibility, then Consultant may not be awarded a public contract for at least one (1) year after such termination. Consultant further acknowledges that Consultant is liable for any additional costs incurred by the County as a result of the County's termination of this Agreement for breach of these provisions regarding employment eligibility.

f. Consultant shall incorporate in all subcontracts made pursuant to the awarded Agreement the provisions contained herein regarding employment eligibility.

I. FORCE MAJEURE

If awarded on the basis of this proposal, the undersigned pledges to provide the services as specified in the Proposal and County Specifications barring any delays due to strikes, fires, transportation difficulties or other causes beyond the control of the undersigned.

PART V: – ATTACHMENTS/FORMS

COVER PAGE

SUBMIT ONE (1) ORIGINAL HARD-COPY AND ONE (1) EXACT ELECTRONIC PDF COPY ON A USB DRIVE IN A SEALED ENVELOPE OR CONTAINER TO:

PURCHASING DIVISION
ST. JOHNS COUNTY
500 SAN SEBASTIAN VIEW
ST. AUGUSTINE FLORIDA 32084

COMPANY NAME: _____

CONTACT NAME & TITLE: _____

CONTACT PHONE NUMBER: _____

CONTACT EMAIL ADDRESS: _____

DATE: _____

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "A"

AFFIDAVIT OF SOLVENCY

PERTAINING TO THE SOLVENCY OF {***insert entity name***}_____, being of lawful age and being duly sworn I, {***insert affiant name***}_____, as {***insert position or title***}_____ _____ ***(****ex: CEO, officer, president, duly authorized representative, etc.)* hereby certify under penalty of perjury that:

1. I have reviewed and am familiar with the financial status of above stated entity.

2. The above stated entity possesses adequate capital in relation to its business operations or any contemplated or undertaken transaction to timely pay its debts and liabilities (including, but not limited to, unliquidated liabilities, unmatured liabilities and contingent liabilities) as they become absolute and due.

3. The above stated entity has not, nor intends to, incur any debts and/or liabilities beyond its ability to timely pay such debts and/or liabilities as they become due.

4. I fully understand failure to make truthful disclosure of any fact or item of information contained herein may result in denial of the application, revocation of the Certificate of Public Necessity if granted and/or other action authorized by law.

The undersigned has executed this Affidavit of Solvency, in his/her capacity as a duly authorized representative of the above stated entity, and not individually, as of this ____day of _____, 20____.

_____
Signature of Affiant

STATE OF_____)

COUNTY OF_____)

Subscribed and sworn to before me this _____ day of _____, 20____, by _____ who personally appeared before me at the time of notarization, and who is personally known to me or who has produced
_____ as identification.

_____
Notary Public

My commission expires:
_____

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "B"

AFFIDAVIT

ST. JOHNS COUNTY BOARD OF COUNTY COMMISSIONERS
ST. AUGUSTINE, FLORIDA

At the time the proposal is submitted, the Respondent shall attach to his proposal a sworn statement.

The sworn statement shall be an affidavit in the following form, executed by an officer of the firm, association or corporation submitting the proposal and shall be sworn to before a person who is authorized by law to administer oaths.

STATE OF_____COUNTY OF _____. Before me, the undersigned authority, personally appeared_____ who, being duly sworn, deposes and says he is _____(Title) of _____(Firm) the respondent submitting the attached proposal for the services covered by the RFP documents for **RFP No: 22-06; Cyber Security Assessment**.

The affiant further states that no more than one proposal for the above referenced service will be submitted from the individual, his firm or corporation under the same or different name and that such respondent has no financial interest in the firm of another respondent for the same work, that neither he, his firm, association nor corporation has either directly or indirectly entered into any agreement, participated in any collusion, or otherwise taken any action in restraint of free competitive bidding in connection with this firm's proposal on the above described service. Furthermore, neither the firm nor any of its officers are debarred from participating in public contract lettings in any other state.

_____
(Proposer)

By_____

_____
(Title)

STATE OF_____)

COUNTY OF_____)

Subscribed and sworn to before me this _____ day of _____, 20____, by _____ who personally appeared before me at the time of notarization, and who is personally known to me or who has produced _____ as identification.

_____
Notary Public

My commission expires: _____

_____

VENDOR ON ALL COUNTY SERVICES MUST EXECUTE AND ATTACH THIS AFFIDAVIT TO EACH PROPOSAL.

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "C"

CONFLICT OF INTEREST DISCLOSURE FORM

RFP Number/Description: RFP No 22-06; Cyber Security Assessment

The term "conflict of interest" refers to situations in which financial or other considerations may adversely affect, or have the appearance of adversely affecting a consultant's/contractor's professional judgment in completing work for the benefit of St. Johns County ("County"). The bias such conflicts could conceivably impart may inappropriately affect the goals, processes, methods of analysis or outcomes desired by the County.

Consultants/Contractors are expected to safeguard their ability to make objective, fair, and impartial decisions when performing work for the benefit of the County. Consultants/Contractors, therefore must there avoid situations in which financial or other considerations may adversely affect, or have the appearance of adversely affecting the Consultant's/Contractor's professional judgement when completing work for the benefit of the County.

The mere appearance of a conflict may be as serious and potentially damaging as an actual distortion of goals, processes, and methods of analysis or outcomes. Reports of conflicts based upon appearances can undermine public trust in ways that may not be adequately restored even when the mitigating facts of a situation are brought to light. Apparent conflicts, therefore, should be disclosed and evaluated with the same vigor as actual conflicts.

It is expressly understood that failure to disclose conflicts of interest as described herein may result in immediate disqualification from evaluation or immediate termination from work for the County.

Please check the appropriate statement:

☐ I hereby attest that the undersigned Respondent has no actual or potential conflict of interest due to any other clients, contracts, or property interests for completing work on the above referenced service.

☐ The undersigned Respondent, by attachment to this form, submits information which may be a potential conflict of interest due to other clients, contracts or property interests for completing work on the above referenced service.

Legal Name of Respondent: _____

Authorized Representative(s): _____ _____

Signature Print Name/Title

_____ _____

Signature Print Name/Title

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "D"

DRUG-FREE WORKPLACE FORM

The undersigned firm, in accordance with Florida Statute 287.087 hereby certifies that

_____ does:
Name of Firm

1. Publish a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the workplace and specifying the actions that will be taken against employees for violations of such prohibition.

2. Inform employees about the danger of drug abuse in the workplace, the business' policy of maintaining a drug-free workplace, any available drug counseling, rehabilitation, employee assistance programs and the penalties that may be imposed upon employees for drug abuse violations.

3. Give each employee engaged in providing the contractual services that are described in St. Johns County's Request for Proposal a copy of the statement specified in paragraph 1.

4. In the statement specified in paragraph 1, notify the employees that, as a condition of working on the contractual services described in paragraph 3, the employee will abide by the terms of the statement and will notify the employer of any conviction of, or plea of guilty or nolo contendere to, any violation of Florida Statute 893, as amended, or of any controlled substance law of the United States or any state, for a violation occurring in the workplace no later than five (5) days after such conviction or plea.

5. Impose a sanction on, or require the satisfactory participation in a drug abuse assistance or rehabilitation program if such is available in the employee's community by, any employee who is so convicted.

6. Consistent with applicable provisions with State or Federal law, rule, or regulation, make a good faith effort to continue to maintain a drug-free workplace through implementation of paragraphs 1 through 5.

As the person authorized to sign this statement, I certify that this firm complies fully with the above requirements.

_____
Signature

_____
Date

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "E"

LOCAL PREFERENCE

Any Respondent that meets the criteria of a Local Business, in accordance with Section 302.25 of the SJC Purchasing Procedure Manual, must complete and sign this Attachment "E" to indicate their qualification to receive local preference. All required documentation to demonstrate that the Respondent meets all qualification criteria as a local business must be included in the submitted proposal/submittal with this Attachment "E".

In order to qualify for local preference Respondent must provide sufficient documentation to demonstrate:

- A physical, brick and mortar place of business located within the geographic boundaries of St. Johns County, with a valid mailing address, in an area zoned for the conduct of such business, from which the Vendor has operated or performed business on a day-to-day basis that is substantially similar to those specified in the solicitation for a period of at least one (1) calendar year prior to the issuance of the solicitation. No PO Boxes shall be accepted.
- Local address above must be registered as the Vendor's principal place of business with the Divisions of Corporations Florida Department of State for at least one (1) calendar year prior to the issuance of this RFP.
- Submit current and valid Local Business Tax Receipt, and must have Local Business Tax Receipts issued by the St. Johns County Tax Collector from at least one (1) calendar year prior to issuance of this RFP.
- Must qualify as a local business as shown above **AND** self-perform a minimum of fifty percent (50%) of all services under the awarded Contract, or must have a minimum of fifty percent (50%) of all services performed by qualified local businesses as sub-contractors or sub-consultants.

If qualifying for local preference through the use of qualified local sub-contractors or sub-consultants, Respondent must submit all required documentation to demonstrate the above requirements of all proposed sub-contractors and sub-consultants for local preference consideration with the submitted proposal.

Respondent is a Local Business as defined in Section 302.25, SJC Purchasing Procedure Manual _____

If Respondents selects this option, by signing below, Respondent certifies that the firm qualifies as a local business in accordance with the requirements stated above, OR certifies that the submitted local business proposed as sub-contractors or sub-consultants meet the requirements for local preference AND that a minimum of fifty percent (50%) of all services shall be performed by local businesses as proposed.

Respondent is **not** a Local Business as defined in Section 302.25, SJC Purchasing Procedure Manual _____

If Respondent selects this option, Respondent is not seeking consideration for local preference, and is not required to submit the documentation provided above.

_____

Signature – Authorized Respondent Representative

_____

Printed Name & Title

_____

Date of Signature

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "F"

CERTIFICATES OF INSURANCE

Respondents shall provide certificates of insurance as part of their submittal package. Certificates of insurance shall meet or exceed the requirements as described in Part V: Contract Requirements; F. Insurance Requirements.

Failure to provide proof of current insurance coverage or ability to obtain the required coverages may result in being deemed non-responsive and removed from further consideration.

(Attach or insert copy here)

ATTACHMENT "G"
CLAIMS, LIENS, LITIGATION HISTORY
(Complete and Submit)

1. Within the past 7 years, has your organization filed suit or a formal claim against an owner (as a prime or subcontractor) or been sued by or had a formal claim filed by an owner, subcontractor or supplier resulting from a construction dispute? Yes _____ No _____ If yes, please attach additional sheet(s) to include:

   Description of every action Captions of the Litigation or Arbitration

   Amount at issue: _____ Name (s) of the attorneys representing all parties:
   _____
   Amount actually recovered, if any: _____

   Name(s) of the service owner(s)/manager(s) to include address and phone number:
   _____

2. List all pending litigation and or arbitration.
   _____

3. List and explain all litigation and arbitration within the past seven (7) years - pending, resolved, dismissed, etc.
   _____

4. Within the past 7 years, please list all Liens, including Federal, State and Local, which have been filed against your Company. List in detail the type of Lien, date, amount and current status of each Lien.
   _____
   _____
   _____

5. Have you ever abandoned a job, been terminated or had a performance/surety bond called to complete a job?

   Yes _____ No _____ If yes, please explain in detail:
   _____
   _____

6. For all claims filed against your company within the past five-(5) years, have all been resolved satisfactorily with final judgment in favor of your company within 90 days of the date the judgment became final? Yes ____ No____
   If no, please explain why? _____
   _____
   _____

7. List the status of all pending claims currently filed against your company:
   _____
   _____

Liquidated Damages

1. Has an owner ever withheld retainage, issued liquidated damages or made a claim against any Performance and Payment Bonds? Yes _____ No _____ If yes, please explain in detail:
   _____
   _____

(Use additional or supplemental pages as needed)

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "H"

KEY PERSONNEL LIST

In the space below, list all qualified personnel who are permanent employees of the company that may be utilized to perform any aspect of the required services. Attach brief but comprehensive resumes for each staff member listed below.

Employee Name	Employee Title	# Years Employed	Total # Yrs. Experience

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "I"

REFERENCES & TECHNICAL EXPERIENCE

In this section, Respondents shall submit information on three (3) contracts and/or engagements successfully completed in the last five (5) calendar years of similar scope to the outline scope of services described herein. Respondents must include the type of services performed, timeframe of performance, whether or not the contract was renewed/extended, and all contact information for a point of contact at the reference agency or organization.

1. Company Name: _____

   Date(s) of Service: _____

   Information (Type of Service): _____

   _____

   Primary Contact Name and Title: _____

   Contact Phone Number: _____

   Contact Email Address: _____

* *

2. Company Name: _____

   Date(s) of Service: _____

   Information (Type of Service): _____

   _____

   Primary Contact Name and Title: _____

   Contact Phone Number: _____

   Contact Email Address: _____

* *

3. Company Name: _____

   Date(s) of Service: _____

   Information (Type of Service): _____

   _____

   Primary Contact Name and Title: _____

   Contact Phone Number: _____

   Contact Email Address: _____

* *

4. Company Name: ____

   Date(s) of Service: ____

   Information (Type of Service): ____

   ____

   Primary Contact Name and Title: ____

   Contact Phone Number: ____

   Contact Email Address: ____

* *

5. Company Name: ____

   Date(s) of Service: ____

   Information (Type of Service): ____

   ____

   Primary Contact Name and Title: ____

   Contact Phone Number: ____

   Contact Email Address: ____

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "J"

PRICING PROPOSAL FORM

Each Respondent shall submit a Total Price for Cybersecurity Assessments for both the BCC and Clerk locations as indicated below. These prices shall remain firm throughout the duration of the Contract. Please enter the amount for each pickup in numerals and in words. In the event of a discrepancy between the amounts, the amount written in words shall be used as the correct bid price.

Total Price for Cybersecurity Assessment(s):

Item 1 Cybersecurity Assessment for BCC

Item 1: $ _____ (Amount in numerals)
_____ (Amount in words)

Item 2 Cybersecurity Assessment for Clerk

Item 2: $ _____ (Amount in numerals)
_____ (Amount in words)

Respondents shall type or legibly print the Total Price for each item in both numerals and words. If the County is unable to determine the proposed amount due to illegibility, the proposal may be removed from consideration for award.

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

ATTACHMENT "K"
E-VERIFY AFFIDAVIT
Contract No._____

STATE OF _____
COUNTY OF _____

I, _____ (hereinafter "Affiant"), being duly authorized by and on behalf of _____(hereinafter "Consultant/Contractor") hereby swears or affirms as follows:

1. Consultant/Contractor understands that E-Verify, authorized by Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), is a web-based system provided by the United States Department of Homeland Security, through which employers electronically confirm the employment eligibility of their employees.

2. For the duration of Contract No. _____ (hereinafter "Agreement"), in accordance with section 448.095, F.S., Consultant/Contractor shall utilize the U.S. Department of Homeland Security's E-Verify system to verify the employment eligibility of all new employees hired by the Consultant/Contractor and shall expressly require any subcontractors performing work or providing services pursuant to the Agreement to likewise utilize the U.S. Department of Homeland Security's E-Verify system to verify the employment eligibility of all new employees hired by the subcontractor.

3. Consultant/Contractor shall comply with all applicable provisions of section 448.095, F.S., and will incorporate in all subcontracts the obligation to comply with section 448.095, F.S.

4. Consultant/Contractor understands and agrees that its failure to comply with all applicable provisions of section 448.095, F.S. or its failure to ensure that all employees and subcontractors performing work under the Agreement are legally authorized to work in the United States and the State of Florida constitute a breach of the Agreement for which St. Johns County may immediately terminate the Agreement without notice and without penalty. The Consultant/Contractor further understands and agrees that in the event of such termination, Consultant/Contractor shall be liable to the St. Johns County for any costs incurred by the St. Johns County resulting from Consultant/Contractor's breach.

DATED this _____ day of _____, 20____.

_____
Signature of Affiant

_____
Printed Name of Affiant

_____
Printed Title of Affiant

_____
Full Legal Name of Consultant/Contractor

Sworn to (or affirmed) and subscribed before me by means of ☐ physical presence or ☐ online notarization, this _____ day of _____, 20____, by {*insert name and title of Affiant*}, who is personally known to me or has produced_____ _____ as identification.

_____
Notary Public
My Commission Expires:_____

OPTIONAL CHECKLIST

SECTION	PROPOSAL COMPONENTS	CHECK BOX
Section 1	Cover Page & Cover Letter	
Section 2	Qualifications	
	Attachment "H" – Key Personnel List	
Section 3	Project Approach	
Section 4	Proposed Pricing	
	Attachment "J" – Pricing Proposal Form	
Section 5	References & Technical Experience	
	Attachment "I" – References & Technical Experience	
Section 6	Administrative Information	
	Attachment "A" – Affidavit of Solvency	
	Attachment "B" – St. Johns County Affidavit	
	Attachment "C" – Conflict of Interest Disclosure Form	
	Attachment "D" – Drug-Free Workplace Form	
	Attachment "E" – Local Preference Form	
	Attachment "F" – Certificates of Insurance	
	Attachment "G" – Claims, Liens, Litigation History	
	Attachment "K" – E-Verify Affidavit	
	Acknowledged (signed) Addenda (as posted)	

RFP NO: 22-06; CYBER SECURITY ASSESSMENT

SEALED RFP MAILING LABEL

Cut along the outer border and affix this label to your sealed bid envelope to identify it as a "Sealed RFP"

SEALED RFP • DO NOT OPEN

SEALED RFP #:	**RFP NO. 22-06**
RFP TITLE:	**CYBER SECURITY ASSESSMENT**
DUE DATE/TIME:	**Thursday, October 14, 2021** **No Later Than 4:00 P.M. EST**
SUBMITTED BY:	
	Company Name
	Company Address
	Company Address
DELIVER TO:	St. Johns County Purchasing 500 San Sebastian View St St. Augustine, FL 32084

END OF DOCUMENT

ADDENDUM #1

October 8, 2021

To: Prospective Respondents
From: St. Johns County Purchasing Division
Subject: RFP No: 22-06; Cyber Security Assessment

This Addendum #1 is issued to further Respondents' information and is hereby incorporated into the RFP Documents. Respondents shall incorporate any and all information, changes, clarifications and instructions provided in each Addendum into their submitted Proposal, and include a copy of each signed addendum in the submitted Proposal as instructed in the RFP Document.

Clarifications/Revisions:

1. To better define the scope of "APPLICATION TESTING" to be performed the County provides the following clarification:

   St. Johns County (SJC) is looking for basic testing of our EXTERNAL applications. The extent of this testing would be limited to approximately ten (10) applications that we have developed in-house, and NOT to third-party hosted applications. The testing of these in-house developed applications would NOT include API testing. The testing would be somewhat generic in nature, to include, standard exploits such as SQL/script injection, and known vulnerabilities in the hosting platform (Windows, IIS, .NET framework). Therefore, we would NOT expect all pages within applications, or any proprietary business logic to be tested verbosely. Due to the high number of, and extensive business/workflow knowledge required, INTERNAL applications would NOT need to be tested, but rather a few random platform exploit tests would be sufficient.

   All of our EXTERNAL web applications are written in MS.NET framework version 4.x, hosted on MS Windows IIS, and access data from a MS SQL Server DB. Our applications sometimes utilize client-side JavaScript/AJAX, but usually for user interface experience purposes only. We also commonly use Bootstrap as a responsive framework. These EXTERNAL applications are ALL web based, with no Native Windows or Native Mobile applications. Testing would occur in a LIVE production environment, and therefore, we would need to be notified of the timeline and scope of testing to take place, when the time comes.

   To be clear, we are NOT asking for source code to be evaluated, but simply spot checks on our applications for common security flaws, and basic inspection of our platforms, known exploits, patches, etc. Once again, to reiterate:

   - NO isolated Web Service testing
   - NO isolated API testing
   - NO source code evaluation
   - NOT every page or URL must be tested, simply spot checks, with documentation of what was tested.
   - NO user role testing.

2. All references to SCADA in the scope of services are hereby removed.

Questions/Answers:

1. Can you share any budgetary information about this project with us, is there any assigned budget for this project? Please specified the budget.
   Answer: The County has $160,000.00 budgeted.

2. Is there an incumbent company or organization with an advantage for this project?
   Answer: No.

3. In the Scope of Services it looks like you are looking for a variety of security related services including: security benchmarking, vulnerability assessments, penetration testing, data assessments, third-party interfaces, application penetration testing, password management auditing, access controls auditing, and security logging review. However, the requirements for the final report look to focus on penetration testing. As such, it is not 100% clear what the you are looking for, and if it is everything in the scope of services needs to be included on the final report, that is a lot of different items that are all independent of each other, and will affect the final price estimation, can you please clarify, what is need it on the SOW and if all these items need to be part of the final report as well?
   Answer: All penetration items are to be included in the final report. The remainder of the analysis is to be given in a less formal manner.

4. How many office locations and facilities are in-scope for the project?
   Answer: There are 57 remote locations that connect through various transport methods back to a DMVPN hub. In a sense, they are 1 site in 4 VRFs but they are physically diverse.

5. How many relevant departments are there from an IT or Information Security point-of-view?
   Answer: There are 2 Constitutional entities.

6. How many existing Information Security Policies and Procedures are currently implemented?
   Answer: There are minimal P&P's in place.

7. Is there a network diagram that could be shared?
   Answer: One can be shared after award and a non-disclosure agreement has been executed.

8. How many Wireless Access Points are there in total across the two organizations?
   Answer: 150.

9. Is the approximate number of partner/vendor connections 12?
   Answer: Yes.

10. How many applications and APIs are in-scope for security assessment/testing?
    Answer: With regards to external applications, perform testing on known exploits for SQL Server, IIS, to include DoS and other common attack methodology such as script and SQL injection. Due to the business specific nature of our internal applications, we would not expect individual testing on each of those 100+ applications. More of an "after hours", platform based (IIS, SQL Server, .NET, Windows) penetration and various exploit testing would be sufficient.

11. How many of the apps/APIs can be tested remotely? (Note that QA or DEV versions are necessary for security testing)
    Answer: See the response to #10 above.

12. When does the St. John's Country BCC expect the work to be started/completed?
    Answer: A schedule and timeline shall be developed after award.

13. Is there an expected period of performance once the work has started? Or can the engagement be broken into phases throughout the year long period?
    Answer: See the response to #12 above.

14. Is there a proposed budget that the City has allocated for this assessment? If so, can that be disclosed?
    Answer: See the response to #1 above.

15. Can a portion of the work be performed fully remote, apart from the physical security and SCADA phases of the assessment?
    Answer: Yes.

16. Can the work be performed outside of core working hours (9AM-5PM)?
    Answer: Yes.

17. How does the SCADA network connect with the rest of the City's network?
    Answer: See #2 in Clarifications/Revisions above.

18. How many locations will be assessed for physical security? Will the county permit after hours assessment of physical locations?
    Answer: One location. Yes, with proper scheduling.

19. How many total individuals will the social engineering testing intend to target?
    Answer: There are approximately 1,200 email accounts.

20. How many different campaigns are expected for the social engineering testing?
    Answer: Respondents should include recommendations in their RFP submission.

21. How are communications with partner billing entities conducted? (e.g., protocols, applications)
    Answer: This will be handled on a case by case basis.

22. How many sites should be included in physical security testing?
    Answer: See the response to #18 above.

23. Are there any specific social engineering attack vectors or pretexts that St. Johns County specifically expects/desires to be included in testing?
    Answer: No.

24. What language/frameworks are any custom Web applications written in?
    Answer: St. Johns County developed applications are in VB.Net.

25. What is the count of URLs for each Web application? For sites using custom API calls, how many APIs are used for each Web application?
    Answer: There are 10 external applications w/ 10 URLs. Please see #1 in Clarifications/Revisions above for additional information.

26. Will credentials be provided for Web applications to ensure exhaustive testing? (e.g., unauthenticated, authenticated user account, authenticated as administrator account)
    Answer: Yes, credentials will be provided after contract award.

27. How many external (network) points of presence will be tested?
    Answer: Two (2).

28. What types of wireless protocols are in scope for testing? (e.g., 2.4 GHz, 5 GHz, Cellular)
    Answer: 2.4/5Ghz WiFI.

29. Would the County consider electronic-only response submissions?
    Answer: No.

30. Who is providing your current cyber security services, an external vendor or delivered in-house?
    Answer: Internal, in-house.

31. Please provide the number of systems which are designated as in scope.
    Answer: Approximately 9,500. This would include servers, desktops, laptops, cameras, IP security devices such as door readers, etc.

32. Does the client want every internal application tested with full coverage of all functionality or are they looking for a cursory "low-hanging fruit" approach? With 100 internal applications a full assessment, particularly a whitebox assessment involving source code review and analysis, of each would greatly increase the amount of time required for testing to complete.
    Answer: SJC is looking for a cursory approach with emphasis on process.

33. Are there any socio-economic preference points allocated to small businesses, disadvantaged small businesses, economically disadvantaged women-owned small businesses (EDWOSB), women-owned small businesses (WOSB), and/or minority owned small businesses?
    Answer: No.

34. Is this the first time that you will contract a vendor for the services in question? If not, then would a copy of the final contract and amount of the previous successful vendor be available?
    Answer: This will be the first Cyber Security Assessment completed by SJC.

35. Given the COVID-19 pandemic, can work be performed remotely to the maximum possible extent?
    Answer: Yes.

36. For the items – “Partner Connectivity”, “Interface to Partner Entities”, “Evaluate Client Remote Access to External Services”, “Evaluate Internal MIS Tools for Data Leakage”, “Internet Usage”, and “Host Based Security”, are you looking for us to perform these reviews **as a part of** the network penetration tests? Or are you looking for us to perform individual reviews of each of these areas at a detailed configuration level where we review the configuration settings at a very granular level?
    Answer: These are expected to be separate.

37. Please provide the approximate number of live external IP addresses in scope?
    Answer: 80.

38. Please provide the approximate number of live internal IP addresses in scope?
    Answer: See the response to #31 above.

39. Please provide the number of web applications in scope?
    Answer: See clarification above.

40. Please provide the number of locations to be included in the wireless network penetration test? Can sampling be used?
    Answer: One (1) is sufficient as the configuration is not diverse.

41. As part of this project are you also looking for us to review your existing cybersecurity documentation (policies, plans, procedures, etc.) and provide guidance for improvement? In addition, are you looking for us to develop one or more of these from scratch?
    Answer: Yes to both.

42. Please identify if you have key cybersecurity documentation in place such as – Business Continuity Plan, Incident Response Plan, Information Security Policies and Procedures, etc.
    Answer: SJC has frameworks for all of these; but, is concerned about their efficacy.

43. Please provide a high-level overview of your remote access infrastructure in scope for review.
    Answer: Remote Access is currently a mix of legacy client Anyconnect transitioning to client based Global Protect. A single gateway and portal are in place.

44. Please provide the number and types of social engineering scenario tests that you would like us to perform.
    Answer: Respondents should document what they are proposing in their submission.

45. Please provide a high-level overview of your URL/web filtering solution infrastructure in scope for review.
    Answer: Web filtering is performed with a mix of client based and inline iBoss scanning.

46. Please provide a high-level overview of the operating systems and databases in scope for the host-based security review.
    Answer: 80% Windows, Security, 5% Linux servers, appliances, etc. Mobile is 90% iOS with 10% Android.

47. Please provide a high-level idea of the size and scope of the technical infrastructure that we would encounter.
    Answer: There are 2 main Datacenters with several small server environments at local offices. Mostly all VMware/Microsoft. Network is 80-90 routers, 400 switches, 3 WLCs all Cisco.

48. Please provide a description of the SCADA/ICS infrastructure in scope for penetration testing.
    Answer: See #2 under Clarifications/Revisions above.

49. As part of benchmarking security practices and procedures against NIST 800.53, is a governance or NIST 800-53 compliance assessment expected?
    Answer: No.

50. Concerning the Physical Access Controls Evaluation and Social Engineering, is a physical penetration test expected?
    Answer: Yes.

51. Concerning the Internet Usage portion of the engagement, what are the expectations or goals for this assessment?
    Answer: SJC has no defined goals for this assessment.

52. Are there any regulations or regulators/auditors that apply to the environments to be tested? If so, specify which testing or environment it applies to.
    Answer: Some applicability to PCI, HIPAA and CJIS.

53. Is there a date that final reports must be submitted by? If yes, please specify final report delivery date.
    Answer: TBD based upon negotiations and final schedule included in the awarded contract.

54. Please provide the number of external IP's to be tested:
    Answer: See the response to #37 above.

55. Will you require a retest of Critical/High findings for the external pentest?
    Answer: No.

56. Will you require a customer-facing report for the external pentest?
    Answer: Yes.

57. Will you require a customer facing attestation letter for the external pentest?
    Answer: No.

58. List any third-party systems or networks that are in-scope for the external pentest as well was which systems they own: NOTE: Permission must be obtained by the third-party prior to conducting any testing on these systems.
    Answer: No third-party systems are included.

59. Please provide the number of internal IP's to be tested:
    Answer: See response to #31 above.

60. Do all internal systems respond to a Ping Echo Request?
    Answer: No (approximately 95% will).

61. Will internal testing be performed remote or in-person? NOTE: If Remote, confirm that the client will allow a laptop to be connected to the internal network. The Laptop will form a VPN tunnel for assessment work to be performed remotely.
    Answer: SOME remote is acceptable.

62. Please provide the number of SSID Networks to be in-scope:
    Answer: 3.

63. Number of locations to be tested for wireless pentest, and address of each location.
    Answer: 1.

64. Number of locations to be tested for the physical pentest and address for each location in-scope:
    Answer: One (1) location. 500 San Sebastian View, St Augustine FL 32084.

65. Number of users to be in-scope for email phishing:
    Answer: See the response to #19 above.

66. Please advise type of tests required:
    Answer:
    a. Web Application: **YES**
    b. Mobile Application: Android: **NO**
    c. Mobile Application: iOS: **NO**

67. Please specify how many web/mobile applications need to be tested and specify if they are mobile or web apps:
    Answer: See #1 under Clarifications/Revisions above.

68. Describe the functionality of each application:
    Answer: See #1 under Clarifications/Revisions above.

69. List any specific concerts for each application being tested:
    Answer: See #1 under Clarifications/Revisions above.

70. What type of data is the application responsible for protecting?
    Answer: See #1 under Clarifications/Revisions above.

71. Are any of the applications to be tested custom-built, third-party hosted or COTS? If so, please specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

72. Do any of the applications utilize an application server? If so, specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

73. List any other third-party products being utilized:
    Answer: See #1 under Clarifications/Revisions above.

74. Will testing be conducted on a production environment or is a development/staging environment available?
    Answer: See #1 under Clarifications/Revisions above.

75. Specify the language each application is developed in:
    Answer: See #1 under Clarifications/Revisions above.

76. Do any of the applications rely on client-side technologies? If so, specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

77. Do the applications leverage AJAX, AngularJS, or other frameworks? If so, specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

78. List the different types of roles to be tested within the application and specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

79. Approximately how many user interface screens comprise each application?
    Answer: See #1 under Clarifications/Revisions above.

80. Do the applications interface with any single sign-on (SSO) solution? If so, specify which applications, and list what SSO solution is in place for each application.
    Answer: Yes, ADFS/Azure AD is in use only for third part cloud appliaitons (Energov, Duo, etc.)

81. Is the SSO server accessible from the internet, only internally, or restricted per application.
    Answer: Yes, https://fs.sjcfl.us server SJCADFS.

82. Is there a thick client that talks to the application? If so, please specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

83. Should the thick-client be tested?
    Answer: See #1 under Clarifications/Revisions above.

84. What language is the thick-client written in?
    Answer: See #1 under Clarifications/Revisions above.

85. Are there any system to system API's exposed by the application that you would like tested? If yes, please specify which applications.
    Answer: See #1 under Clarifications/Revisions above.

86. How many distinct API's need to be tested?
Answer: See #1 under Clarifications/Revisions above.

87. Please provide any documentation or URL's to definition files if possible:
Answer: See #1 under Clarifications/Revisions above.

88. What OS is being tested?
Answer: See response to #46 above.

89. How many devices per OS to be tested?
Answer: See response to #46 above.

90. What OS will be tested (Windows, Linux, Mac, ect)?
Answer: See response to #46 above.

91. How many devices per OS to be tested?
Answer: See response to #46 above.

92. In your own words please describe end-goal/result from risk assessment:
Answer: SJC's goal is to identify any high risk areas that require remediation, as well as to aid in defining a baseline standard for MIS.

93. Please list all locations where traditional IT networks/infrastructure are:
Answer: There are 57 remote locations. Details will be provided after RFP is awarded. All are within St Johns County.

94. Number of dedicated security personnel per location:
Answer: 0.

95. Number of security domains (Active Directory forests) that are in place per location:
Answer: 1.

96. Number of servers (physical and virtual) that are in the infrastructure per location:
Answer: 0-20 at remote sites. The 2 Datacenters have between 20-200.

97. Will you be able to provide the following organizational information?
Answer:

a. Personnel

1. Organizational Chart: **Yes**
2. Roles and Responsibilities of IT/Security: **Yes**
3. Documented Policies & Processes: **Yes**
4. Information Security Policy: **Yes**
5. Risk Management Strategy and Plan: **Yes**
6. IR Strategy: **No**
7. Results of any previous assessments: **N/A**

b. Physical

1. Locations of sites: **Yes**

2. Physical Security responsibility overview: **Yes**

c. Network

1. Logical network diagram, data flow diagrams, any other network and communications diagrams: **Yes**
2. Security monitoring overview: **Possibly**

d. Assets

1. Asset management process - inventory of endpoints on the network: **90%**
2. Supplier and third-party partner inventory/list: **50%**
3. List of critical facilities: **Yes**

98. Have you had any formal vulnerability assessment (s) and/or Penetration Testing processes performed within the past 3 years – whether across the full BCC/Clerk operations or within separate operating units of BCC – and if so will the results of those projects be available for review?
Answer: See the response to #34 above.

99. Can you provide details regarding the number of physical locations and types of access controls that are in place in order to properly scope the level of effort for this assessment?
Answer: There are approximately 50+ locations with emphasis on the main campus which houses 70% of the users in question. Access control is currently badge controlled in all main locations with many outbuildings being a mix of keyed access and combination locks.

100. Can you provide additional documentation/information on the current # of URLs as well as deployed tools being utilized in order to properly scope the level of effort for this assessment.
Answer: See #1 under Clarifications/Revisions above.

101. In addition to the Corporate-owned devices (550) can you advise the quantity of BYOD devices in use, and can you provide documentation regarding BCC policies/controls currently in place for BYOD users. This will be helpful to properly scope the level of effort for this assessment.
Answer: There are no BYOD devices in use.

102. Can you provide additional clarification on the service scope, for instance are you requesting Web Application Testing for this category? If "yes" then can you provide answers to the following scoping items:
Answer: See #1 under Clarifications/Revisions above. Answer applies to items a – e below as well.

a. How many web site(s)/URLs would you like to assess?

b. How many pages? An example of a static page would be the front page of a web site or any of the pages referenced on the site map that remain the same. A dynamic page would be applications that are behind the static page. An example would be a built in price list, a log in, choices from a previous page, i.e., the Best Buy site where you can drill down and purchase things. Those would be dynamic pages. Are some of these pages dynamically generated from a subset of core pages?

c. Does the application require any client side applications? An example of this would be a web site that requires Flash Player, ActiveX, etc. Anything a web site user would need to download to view the web site correctly.

d. Are there different user levels? If so, how many? An example of this would be a web site that has an "Administrator" logon and also a "User" logon. If there are different user levels, do you want data integrity verified between different user levels? Do you want us to make sure one level of logon can/cannot access information intended for another level?

e. Do you want black-box (unauthenticated) or white-box (authenticated) testing?

103. SCADA devices – can you provide descriptions of what types of devices (functional, network, applications) are included within this category.
Answer: See #2 under Clarifications/Revisions above..

104. Can all SCADA devices be accessed via IP networks? If not, what network types are deployed?
Answer: See #2 under Clarifications/Revisions above.

105. How many locations are to be assessed?
Answer: See the response to #18 above.

106. Are point to point wireless systems deployed to provide connectivity between locations?
Answer: Yes, but for a handful of very small sites/hosts.

107. How many wireless access points (WAPs) are deployed?
Answer: 150.

108. Are there open access points for public/visitor access? If so, on how many WAPs?
Answer: Yes, All.

109. Are there encrypted access points for business use? If so, on how many WAPs?
Answer: Yes, All.

110. How many SSIDs does the organization have at each location?
Answer: 3 are in scope.

111. Is the organization using WEP, WPA, and/or WPA2 encryption? Which ones?
Answer: WPA2 EAP-TLS.

112. How many wireless policies, procedures, and documentation is available for review?
Answer: 0.

113. Can you describe the nature and range of access methods currently in use and to be evaluated for the various partner entities?
Answer: Remote Access for an unknown number of users, 5 Lan 2 Lan tunnels, ~10 directly connected firewall connected interconnects.

114. Are these dedicated network connections?
Answer: See the response to #113 above.

115. Have you performed any formal social engineering assessments within the past 3 years, and if so will the results of those assessments be provided?
Answer: Yes, email based only. Yes, results will be provided to awarded firm.

116. Total number of internal network IP addresses to be tested. (If providing an IP range, please indicate the estimated number of live IPs.)
Answer: See the response to #31 above.

117. How deep should testing go in the event of successful network penetration (i.e., just validation of vulnerability; network administrator access; server access, etc.)?
Answer: Validation is sufficient.

118. Are internal web-based applications/services in scope? If so, please indicate the anticipated number of web-based applications/services that may need to be assessed.
Answer: See #1 under Clarifications/Revisions above.

119. Is it desired to evaluate the strength of mobility environments (iPhones, BlackBerry, home VPN access)?
Answer: Yes, to county-owned mobile devices (90% iOS, 10% android).

120. Are corporate build/configuration standards in place for various platforms (network devices, operating systems, etc.), and if so, is it desirable to evaluate against those standards, etc. This process will determine the amount of time required to perform additional analysis and tuning of evaluation criteria.
Answer: Yes.

121. Can remote internal networks be scanned via a primary location, or would it be necessary to perform field visits to each in-scope location?
Answer: Remote networks are accessible.

122. If multiple locations need to be visited, how many locations are in scope?
Answer: N/A.

123. Are any of the internal applications a third-party provider?
Answer: See #1 under Clarifications/Revisions above.

124. Does SJC have intrusion detection capabilities? If so, is an objective of this test also to assess the SJC's intrusion detection capabilities?
Answer: No.

125. What is the total number of public-facing/external network IP addresses to be tested? (If providing an IP range, please indicate the estimated number of live IPs.)
Answer: See the response to #37 above.

126. Number of Web-based applications/ services to test (dynamic pieces of websites that users or other applications authenticate to - client portal, sales quote system).
Answer: See #1 under Clarifications/Revisions above.

127. Please confirm the approximate number of Web Servers is 35. Are these 35 Web servers in addition to the 30 live hosts?
Answer: See #1 under Clarifications/Revisions above.

128. Number of Website URLs to be tested?
Answer: See #1 under Clarifications/Revisions above.

129. Is the Web Application in scope to be tested? If so, please provide the following information:
Answer: See #1 under Clarifications/Revisions above.

    a. URL(s) (also need instance ID + IP)
    b. Links to be excluded from testing
    c. User Roles Count
    d. How many web service endpoints are there in scope?
    e. What are the number of functions per web service?
    f. Will testing be performed against a test environment or production? (test is preferred)

130. With respect to website testing, are web applications in scope, and how many are included?
Answer: See #1 under Clarifications/Revisions above.

131. How deep should testing go in the event of successful network penetration (i.e., just validation of vulnerability; network administrator access; server access, etc.)?
Answer: Validation is sufficient.

132. Are any external systems hosted by a third-party provider?
Answer: Yes, some Azure AD to Tyler Entergov and connections to cloud based apps like Invoice Cloud at Utilities.

133. Does SJC own and manage the network equipment at your external perimeter?
Answer: Yes.

134. Are there any test window restrictions for any of the test categories (Ext, Int, SE, Lock picking, Tailgating, etc.)?
Answer: None.

135. Is the target/goal of external testing similar to the internal testing goal of "attempting to connect to internal servers and other network devices to obtain accounts/passwords, acquire network information, and access SJC data"?
Answer: Yes.

136. What controls are in place for requesting, configuring, monitoring Partner Connectivity?
Answer: Controls are informal.

137. Is there a Partner Connectivity Agreement / Policy?
Answer: No.

138. How many individual Partner Connections are in scope?
Answer: See the response to #113 above.

139. Can Partner Connection be tested via a primary location, or would it be necessary to perform field visits to each in-scope location?
Answer: They can be tested from the primary location.

140. If multiple locations need to be visited, how many locations are in scope?
Answer: N/A.

141. Please confirm the number of Wireless Networks.
Answer: See the response to #110 above.

142. Please provide an estimate of the types of Wireless in use (microwave, 802.11x, proprietary, cell phone, blackberry, iPhone, Bluetooth, Point-to-Point, etc.).
Answer: 10 P2P wireless, 100 802.11x EAP-TLS clients, 500 public users, 200 cell phone users with RA.

143. Are formal wireless security policies in place?
Answer: No.

144. How many individual Partner Entities are in scope?
Answer: Only the handoff is in scope, not the partner.

145. Are these Application Interfaces (APIs), network trusts, scripted imports/exports from other systems?
Answer: Yes.

146. Can Partner Entities be tested via a primary location, or would it be necessary to perform field visits to each in-scope location?
Answer: Tested via the County.

147. If multiple locations need to be visited, how many locations are in scope?
Answer: N/A.

148. What controls are in place for requesting, configuring, monitoring remote access?
Answer: See the response to #136 above.

149. Is there a Remote Access Agreement / Policy?
Answer: Yes; can be provided after award.

150. Is this an assessment against policy, legitimate accounts, and configurations?
Answer: Yes.

151. Impersonation: If there is a person within the company you would like us to impersonate to gain access to information, please indicate who this should be. Otherwise, we will decide based on factors including tenure, position, and possible influence.
Answer: This will be determined with awarded firm.

152. Important User: We may make references to known associates or important users to influence someone's decision to provide us with information on their behalf. Please indicate who this 'important user' should be. Otherwise, we will decide based on factors including tenure, position, and possible influence.
Answer: See the response to #151 above.

153. Third-party Authorization: We may make claims that permission has already been granted by another associate for information.
Answer: Third-party authorization can be discussed after award.

154. SPAM: Do you wish for us to generate false advertisements in hopes of detecting users who decide to click on ads and hyperlinks?
Answer: Yes.

155. Spear Phishing: Through the process of sending an e-mail to users and falsely claiming to be a legitimate enterprise, we can potentially coerce a user into disclosing private information. Please indicate if this is a required assessment.
Answer: Yes.

156. Can employees log into webmail remotely? If so, what is the webmail URL?
Answer: Yes, this will be provided to the awarded firm.

157. Is email hosted internally? If not, who hosts the email services?
Answer: Internally.

158. What controls are in place for content/web filtering and alerting?
Answer: There are managerial controls by department, but should be evaluated.

159. Is there an acceptable Use / Internet Use Policy?
Answer: Yes; can be provided after award.

160. Is this an assessment against policy, configuration, and performance?
Answer: Yes, Yes, and No.

161. What Mobile Platforms are in scope?
Answer: See the response to #119 above.

162. How are Mobile devices being used for (e.g., email, two-way comms, application interfaces, GPS, mobile applications)?
Answer: All of these examples are being used.

163. What, if any, host configuration standards and procedures are in place?
Answer: There is a Mobile Iron MDM in place that should be evaluated

164. Is this assessment against policy and configuration standards?
Answer: Yes

165. How many Active Directory Trees are in use?
Answer: 2 (co/Internet); co includes 4 domains

166. Is role-based access used? How many roles?
Answer: Yes, unknown, most AD functions performed as specific domain admin.

167. Are user access audits periodically performed?
Answer: Yes, as needed or required.
168. What approach is expected for this assessment (i.e., total population or sampling)?
Answer: Respondents must submit as part of their Proposal an intended approach.

169. What, if any, password management tools are in use?
Answer: Informal and limited use of Keepass.

170. Please indicate the number of lines of code, the languages (e.g., C, C#, HTML, Web 2.0, ASP, etc.), the number of applications, etc., to help determine what is meant by "security code" review.
Answer: See #1 under Clarifications/Revisions above.

171. Are automatic source code evaluators acceptable (they are expensive!)?
Answer: See #1 under Clarifications/Revisions above.

172. Are developers available for interviews and confirmation of suspected problems?
Answer: Yes.

173. Are there policies that define system, network, and application logging configurations?
Answer: No.

174. Do any employees access systems in the BCA/Clerks office as well as other county operating systems? If so, how many employees & how many different roles?
Answer: Yes, unknown, and unknown.

175. Does St. Johns maintain an official social media presence? If so, what are the approved handles and who maintains the presence?
Answer: Yes, managed by the Public Affairs Office.

176. Are the servers located within datacenter facilities or in the cloud?
Answer: Local Datacenters with a small amount of Azure integration.

177. Does your organization have an IDS (Intrusion Detection System) or IPS (Intrusion Protection System)?
Answer: Yes.

178. Will St. John's County BCC provide the tools needed to perform the Assessments?
Answer: No.

179. Your Software Applications that were Developed Internally, What was the technology used? What is the language code of the applications?
Answer: See #1 under Clarifications/Revisions above.

180. Do these applications have public access, internal or both?
Answer: See #1 under Clarifications/Revisions above.

181. What is the timeframe you expect to get the results from this Assessment? ASAP, 1-5 months, more than five months?
Answer: This is TBD based upon negotiations and final agreement between County and awarded firm.

182. How many IP addresses are in scope for internal vulnerability assessment/penetration testing?
Answer: See the response to #31 above.

183. How many IP addresses are in scope for external vulnerability assessment/penetration testing?
Answer: See the response to #37 above.

184. Is code review in scope? If yes, what language and how many lines of code.
Answer: See #1 under Clarifications/Revisions above.

185. Are you looking for penetration testing into applications?
Answer: Yes.

186. What type of applications are in scope?
Answer: See #1 under Clarifications/Revisions above.

187. How many live web pages are in scope for testing on each application?
Answer: See #1 under Clarifications/Revisions above.

188. How many web forms (pages) that require user interaction?
Answer: See #1 under Clarifications/Revisions above.

189. What is the number and type of user roles?
Answer: Unknown, roles are normally dictated by AD user group through application.

190. If web services are to be tested, how many endpoints are in scope (i.e., number of parameters per method)?
Answer: See #1 under Clarifications/Revisions above.

191. How many users are in scope for social engineering?
Answer: 5 for direct, 1200 email users.

192. How many physical locations are to be tested?
Answer: See the response to #18 above.

193. What is the approximate total travel time between locations?
Answer: N/A.

194. How many ESSIDs are in scope at each location?
Answer: 3.

195. What is the extent of testing that you want performed on SCADA systems, since they are more sensitive? How many of these are in scope for the testing?
Answer: See #2 under Clarifications/Revisions above.

196. Is the County flexible on insurance requirements (e.g., as a small business with a largely remote workforce, we have determined that automobile insurance is not necessary within our business model)?
Answer: Proof of coverage at the required limits is necessary/required for any vehicle you are using to conduct business. If this is a personal vehicle you would provide your personal auto declaration page along with a statement signed by an officer of the corporation stating that no commercial/business vehicles are owned by the company.

197. Are there any systems currently being utilized which could be characterized as fragile (systems with tendency to crash)?
Answer: SJC has no knowledge of any such fragile systems.

198. Are there systems on the network which the client does not own, that may require additional approval to test?
Answer: No.

199. How many hosts (endpoints) are in the network and part of the scope?
Answer: See the response to #31 above.

200. Is the target environment mostly Windows based? If not, which technologies are used?
Answer: Primarily Windows based.

201. How many external IPs are in scope (local perimeter, cloud services, etc.)?
Answer: See the response to #37 above.

202. How many DNS domains are included?
Answer: Two (2); co.st-johns.fl.us and internet.co.st-johns.fl.us

203. How many web applications will need to be tested?
Answer: See #1 under Clarifications/Revisions above.

204. How many application roles will be tested (by app)?
Answer: See #1 under Clarifications/Revisions above.

205. Are any mobile applications in scope? Android vs. iOS
Answer: None that are internally developed

206. Is the source code available on request?
Answer: See #1 under Clarifications/Revisions above.

207. How many lines of code?
Answer: See #1 under Clarifications/Revisions above.

208. In what language is the application written?
Answer: See #1 under Clarifications/Revisions above.

209. For iOS, is the application available unencrypted?
Answer: N/A

210. For API Testing, how many features?
Answer: See #1 under Clarifications/Revisions above.

211. Can a swagger file be provided?
Answer: See #1 under Clarifications/Revisions above.

212. Is Social Engineering – Phishing to be included in the scope of activities?
Answer: Yes.

213. How many targets will be included in the testing?
Answer: See the response to #191 above.

214. Is Vulnerability Analysis (Vulnerability Scanning) to be included in the scope of activities?
Answer: Yes.

215. How many hosts need to be scanned/analyzed?
Answer: See the response to #31 above.

216. What is the number of distinct environments that should be evaluated (e.g. on-prem, cloud, business silos, etc.)?
Answer: Hosting is primarily on-prem with a small amount of Azure.

217. Relative to the environments to be evaluated, which environments use virtual machines and/or containers?
Answer: 10% physical and 90% Vmware.

218. Which cloud service providers are used (IaaS, SaaS & PaaS)?
Answer: Azure.

219. Please list your perimeter defense technologies currently used (e.g. Cisco ASA, CKP WAF):
Answer: Cisco ASA, Cisco Firepower, iBoss, Palo Alto RA.

220. Is your infrastructure self-managed? If not, by whom?
Answer: Self-managed.

221. For every environment (Google, AWS, Azure, etc.), please provide the following:
Answer:

    a. A network schema or logical diagrams is available upon request: **Yes**
    b. Number of regions for Azure services: **(1) one**
    c. Number of tenants in this cloud provider: **(1) one; primary domain sjcfl.us**
    d. Number of application services used in this provider: **(3) Duo, Tyler Enrgov**

222. Please describe the cloud strategy for each provider (Google, AWS, Azure, etc.), how the environment is used and its purpose.
Answer: Azure – using Azure AD (free) for use with cloud app registrations only at this time.

223. How much technical documentation is there? How many pages?
Answer: Technical documentation is available for the configuration of Tyler, Duo w/ Azure. Approx. 80 pages total.

224. How many users are in scope?
Answer: Approximately 1,200 domain users.

225. How many physical sites are in scope?
Answer: See the response to #18 above.

226. Which best describes the infrastructure: On-prem only, cloud only, or hybrid?
Answer: On-prem with Azure having a copy of AD.

227. Based on our understanding, the County's infrastructure is partially hosted on Azure. If yes, can the County provide an approximate count and type of devices/services deployed in Azure?
Answer: Only using Azure AD (free) at this time. No infrastructure is deployed in Azure.

228. Based on our understanding, the physical access reviews need to be conducted in 2 different locations (BCC and Clerk). Please confirm.
Answer: These are within the same campus.

229. Are the following services applicable to Clerk of Courts (Clerk) - Partner Connectivity, Interface to Partner Entities, Evaluate Client Remote Access to External Services and Evaluate Internal MIS Tools for Data Leakage?
Answer: No

230. Based on our understanding, the 'Partner Connectivity' service is limited to evaluating configurations of interface connection to partners, and 'Interface to Partner Entities' is limited to evaluating how controls are implemented to restrict access for the partners entities. Please confirm if our understanding is correct. If not, please explain the difference between the two in-scope services.
Answer: This is correct.

231. Can the County elaborate on the nature of activities expected to be performed as part of the following service - 'Evaluate Internal MIS Tools for Data Leakage'?
Answer: SJC MIS tools involved are various open source applications like Librenms, Oxidized, phpipam, and self-hosted github. Respondents should include in their approach how they will evaluate these tools for data leakage.

232. Does the County have a Mobile Device Management (MDM) solution installed in the County-owned mobile devices?
Answer: Yes, Mobile Iron.

233. The Scope of Services includes 'benchmarking' of the current security posture against industry standards. Is the County seeking financial as well as operational benchmarking?
Answer: No.

234. Is there an expectation that the scanning/pentesting would extend to the parties identified in the Partner Connectivity/Partner Entities section of the RFP, or do you require review of configurations/process documentation only in this space?
Answer: We require a configuration/process review only.

235. Our typical approach to pentesting would be to run basic scans and use other techniques to identify potential exploits which may succeed within your environment. We would then work with the County to prioritize these

items and run tightly controlled test on a subset of the environment. Is this acceptable to the County, or do you require full exploit testing for any vulnerability we discover?
Answer: This is acceptable.

236. Please provide a list of SCADA devices that would be included in the Vulnerability Scanning / Pen Testing exercises. If available, please provide previous scan results for these devices
Answer: See #2 under Clarifications/Revisions above.

237. Please provide details on current Social Engineering tools/studies the County currently uses.
Answer: The County currently uses Proofpoint's Security Awareness Training module.

238. For Mobile Device Security, please clarify if you are seeking a detailed review of each device or if you require a review of policies/procedures and tools in this area.
Answer: Review of policies and procedures only.

239. Please confirm the Indemnification clause identified in Item G. INDEMNIFICATION would be amended as it relates to penetration testing.
Answer: The County and the awarded firm shall come to agreement over the final provisions of the Contract, including the Indemnification language.

240. There are a few tasks that appear to require performance onsite, but will remote testing also be acceptable?
Answer: Yes.

241. Will any testing be required outside of normal business hours? I.e. evenings or weekends.
Answer: Not required.

242. This assessment will require interviews/discussions to be conducted in order to gain a more thorough understanding of the overall environment and security posture. Can an approximate number of relevant IT personnel/departments we'll need to engage for these activities be provided?
Answer: 7-10.

243. Will a selection of policies, procedures, and other relevant documentation be provided for review as part of the project?
Answer: Yes.

244. For internal testing, is a physical device permitted to be placed onsite? Alternatively, if setting up a VM is preferred, we can provide an OVA file to set up.
Answer: Either is permitted.

245. In evaluating partner connectivity, will this be addressed during the above-mentioned discussions as part of the overall architecture review/security assessment? I.e. Review of firewall rules, procedures, configurations, controls in place, etc., or is there another expectation for this task? I.e. Segmentation level testing of each partner to validate what each connection looks like. If the latter, will travel to these partner locations be required?
Answer: Review of policies and configurations is the expectation.

246. If in depth testing is expected, we are unable to perform this unless permission has been explicitly given to do so.
Answer: N/A.

247. In testing the wireless network(s), how many SSIDs and locations are in scope?
Answer: 3.

248. Is this task meant to be a full penetration test, including segmentation, or is a security review of architectural design and wireless configurations sufficient?
Answer: A full penetration test is required.

249. Is the physical access control evaluation intended to be a cooperative exercise or a stealthy endeavor?
Answer: Either is acceptable. Respondents shall submit their proposed approach as part of the Proposal, which shall be subject to final negotiations and approval by the County.

250. How many locations/buildings are in scope?
Answer: See the response to #18 above.

251. In evaluating tools for data leakage, are these host based as well as network based?
Answer: Yes.

252. Will county owned laptops and/or other devices be provided to complete some of these tasks, and if so, how many different devices need to be tested?
Answer: They can be. 1 device of each type is acceptable (laptop, mobile, etc).

253. For the social engineering component, will this consist of phishing exercises, or are other methods also requested?
Answer: We currently have a phishing test underway, we are looking for targeted testing to a small amount of users as well.

254. Is the goal of this task to test both employee awareness as well as controls in place?
Answer: Yes.

255. In evaluating the internally developed applications, is this meant to be an in-depth penetration test on each one? If so, how many user roles are in scope for each application?
Answer: See #1 under Clarifications/Revisions above.

256. Can a brief explanation of function and complexity for each application in scope be provided?
Answer: See #1 under Clarifications/Revisions above.

257. Are any APIs or other web services in scope for this project?
Answer: See #1 under Clarifications/Revisions above.

258. For Attachment H - Key Personnel, comprehensive, one-page resumes need to be provided as part of the submission. Would it be acceptable if these resumes were two-pages in length to ensure adequate experience is outlined for each of the consultants that would be part of this project?
Answer: No, resumes must be kept to one page.

259. Has this type of assessment been performed previously, and is there an estimated budget for this project?
Answer: See responses to #1 and #34 above.

260. Regarding trade secrets that will be included within the proposal submission, for ease of readability, would County accept an original hard copy of the proposal containing all required information, including information marked as "trade secret," and in addition, a separate, redacted copy of the proposal with all trade secret information redacted for release under a public records request? If yes, is it the County's preference that we include the redacted copy in a separate envelope from the original hard copy?

Answer: Respondents must comply with the requirements of Part III: Proposal Submittal Requirements, paragraph B. Trade Secrets to qualify any of the submitted information as Trade Secret or confidential.

261. Is it County's preference for vendors to include an electronic copy of the redacted proposal on the same USB drive as the original electronic copy?
Answer: See response to #272 above.

262. Within Attachment "I" on page 27 of the RFP, County states in the introductory paragraph that "respondents shall submit information on three (3) contracts and/or engagements." However, Attachment "I" contains 5 reference slots. Please confirm if County wants 3 or 5 references included within the proposal submission.
Answer: A minimum of three (3) references are required.

263. Does County have documented IT policies, procedures, standards, and guidelines in place? If so, how many?
Answer: Yes, less than ten (10).

264. Is County's IT organization centralized or decentralized?
Answer: Centralized.

265. What is County's budget for this project?
Answer: See the response to #1 above.

266. Is there an Active Directory assessment in scope? If so, how many users?
Answer: Yes, see response to #323 above.

267. How many physical locations will be included within the physical access controls evaluation?
Answer: See the response to #18 above.

268. Is an endpoint configuration review in scope? If so, how many should be tested?
Answer: Yes, one (1) of each type.

269. Is a VPN configuration review in scope? If so, how many appliances?
Answer: Yes, two (2).

270. Does County want vendors to provide copies of the engagement team's certifications as part of the proposal submission, or do they just want to know what certifications the consultants hold?
Answer: Respondents shall provide any and all documentation of the certifications for validation purposes.

271. The RFP references a comprehensive list of IT hardware and systems. Are the systems designated as "internal" currently located in a on-premise data center, a colocation data center, or a managed service (data center/cloud)?
Answer: Primarily on-prem with a small amount of Azure.

272. The RFP references multiple IT security frameworks, including NIST, OWSAP and SANS. Is there a particular standards-based control framework that St Johns county is managing against? If so, can you please provide it and its version? If Not, would a recommendation of standards-based control framework be valued as part of the assessment report?
Answer: No.

273. Is the partner connective listed a complete listing?
Answer: Yes, to the best of our knowledge.

The deadline for Questions is hereby extended to: Thursday, October 14, 2021 at 5:00PM EDST

The deadline for Proposal submittal is hereby extended to: Thursday, October 28, 2021 at 4:00PM EDST

Acknowledgment

_____

Signature and Date

_____

Printed Name/Title

_____

Company Name (Print)

END OF ADDENDUM NO. 1

ADDENDUM #2

October 21, 2021

To: Prospective Respondents
From: St. Johns County Purchasing Division
Subject: RFP No: 22-06; Cyber Security Assessment

This Addendum #2 is issued to further Respondents' information and is hereby incorporated into the RFP Documents. Respondents shall incorporate any and all information, changes, clarifications and instructions provided in each Addendum into their submitted Proposal, and include a copy of each signed addendum in the submitted Proposal as instructed in the RFP Document.

Questions/Answers:

1. Is a Credential Landing page to provide analysis for users who enter credentials in-scope? YES/NO
   Answer: No.

2. Please confirm type of data to capture:
   a. Click Rate: YES/NO
   b. Credential Harvesting: YES/NO
   c. Live Payload: YES/NO
   d. Other: Please specify
   Answer: Please see clarification found in Addendum #1.

3. For the vulnerability assessment, will County utilize white-box, gray-box, or black-box testing?
   Answer: White-box testing.

4. Number of Facilities in scope?
   Answer: 2.

5. To what level should the unauthorized access be demonstrated (access to paper files, office areas, network access, obtaining equipment, etc.)?
   Answer: Network access.

6. What approach is expected for this assessment (i.e., total population or sampling)?
   Answer: Referring to Social Testing, a sample is acceptable. Referring to phishing/email testing, then a total population is expected.

7. Would it be possible or desired to perform grey box testing in conjunction with external penetration testing and DMZ architecture review?
   Answer: White Box testing is permitted.

8. Are you seeking a guided walkthrough of in-scope facilities or physical penetration testing?
   Answer: SJC prefers to have testing against physical access controls by having the awarded contractor attempt to utilize social engineering techniques to obtain access to secure areas.

9. What social engineering methods are in scope (e.g., phishing, USB drops, vishing, physical access attempts)?
   Answer: Phishing.

10. Please provide historical data for FTE staff.
    Answer: County has no historical data to provide.

11. Will USB drops be included as part of the exercise? If so, how many USBs would you like to deploy, and how many locations?
    Answer: No.

12. Please confirm the following attack vectors for a physical pentest:
a. SIte Security Architecture: YES/NO
b. Physical Perimeter Access Control: YES/NO
c. Sensitive Area Access: YES/NO
d. Document Control: YES/NO
e. Network/Device Access: YES/NO
f. Internal Sensitive Information handling: YES/NO
g. USB Device Drop: YES/NO
    Answer: a. Yes.
    b. Yes.
    c. Yes.
    d. No.
    e. Yes.
    f. No.
    g. Yes.

13. In order to properly scope the level of effort for this assessment can you provide us copies of current Security Policies, Procedures?
    Answer: None are available.

14. Can you provide any current process/volumes and/or existing methodologies in order to properly scope the level of effort for this assessment?
    Answer: None are available.

15. Can you provide documentation and/or descriptions of currently deployed policies, methodologies, controls in place for Host Based Security along with description/quantities of current operating systems, internally developed applications, and associated current tools in place for management of the various areas of assessment desired.
    Answer: None are available.

16. Will Wi-Fi testing be conducted at multiple locations? If so, how many SSIDs and which locations?
    Answer: One location (SJC Administration Building) is sufficient.

17. Will Physical Facility Breach be included as part of the exercise? If so, how many locations will be in scope?
    Answer: Yes, one (1) the SJC Administration Building.

18. For services that do not require physical presence; Can they be performed remotely? If so, can they be performed outside the Continental US?
    Answer: Yes, Respondent business can be in any location provided the can complete the required physical penetration testing.

19. Do you have an Access Control tool in place?
    Answer: Yes, we use APACS Pro by Apollo Security.

20. Can the vendor deliver a subset of the in-scope services from a location outside the United States?
    Answer: See the response to #18 above.

21. Is a physical penetration test expected, or will review of policies, and procedures for physical access be performed?
    Answer: See the response to #17 above.

22. Can you confirm that the removal of SCADA applies to the 420 items listed in the scope or has this item been renamed?
    Answer: Yes, removal of SCADA applies to the 420 items listed in the scope.

23. Attachment K must be signed and notarized, but it is written as if a contract is already in place. What should we fill in as the Contract No. or should we wait to complete this form until award?
    Answer: Respondents may either leave the contract line blank or put the project name "Cyber Security Assessment" in the space provided. You will need to complete and submit the form with your proposal.

24. Attachment J, the Pricing Proposal Form, specifies that we should provide separate pricing for the Cyber Security Assessment for both the BCC and the Clerk of Courts. However, none of the IT environment information has been provided separately for the two entities. Is it possible for your team to provide either a breakdown of the IT environment by entity, or specify a percentage by which the pricing split could be ascertained?
    Answer: The only separation between BCC and the Clerk is the number of servers (as listed in the environment details; showing two sections BCC & Clerk). The Respondents shall provide a holistic pricing component. SJC's expectation is that any time spent on each individual entity's environment would be roughly itemized; in order for the County to later divide the costs.

25. The approximate number of Internal/External Devices listed on page 5 of the RFP is 3,191 (excluding SCADA) but in Amendment 1 response # 31 you indicate that there are "approximately 9,500, including servers, desktops, laptops, cameras, IP security devices such as door readers, ect". For purposes of properly scoping the number of IP devices to be scanned in the vulnerability assessment can you confirm whether we should use 9,500 or the page 5 numbers?
    Answer: The number of IP devices to be scanned is 3,191.

26. When submitting the response the addendums must be include. Do you want only the page signed indicating received or the entire addendum in the response?
    Answer: Respondents may submit only the signed acknowledgement page.

27. Are travel costs included in the County's budget?
    Answer: The budget for this project is not itemized. Respondents are required to adhere to the County's travel policy as stipulated in the SJC Administrative Code Travel Policy for County Employees.

The deadline for Proposal remains the same: Thursday, October 28, 2021 at 4:00PM EDST

Acknowledgment

_____
Signature and Date

_____
Printed Name/Title

_____
Company Name (Print)

END OF ADDENDUM NO. 2