



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at wvOASIS.gov. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at WVPurchasing.gov with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header 5

List View

General Information

Contact | Default Values | Discount | Document Information | Clarification Request

Procurement Folder: 1369290

SO Doc Code: CRFQ

Procurement Type: Central Master Agreement

SO Dept: 0705

Vendor ID: 000000181088 

SO Doc ID: LOT2400000009

Legal Name: ADVIZEX TECHNOLOGIES LLC

Published Date: 3/21/24

Alias/DBA:

Close Date: 3/28/24

Total Bid: \$59,810.00


Close Time: 13:30

Response Date: 03/28/2024 

Status: Closed

Response Time: 10:01

Solicitation Description: Network Penetration Testing and Cybersecurity Assessments

Responded By User ID: landru2 

Total of Header Attachments: 5

Total of All Attachments: 5

First Name: Scott

Last Name: Hess

Email: shess@advizex.com

Phone: 4406221089

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	External Network Penetration Testing				12297.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Website Penetration Testing				10421.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Internal/Client-Side Network Penetration Testing				22297.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Wireless Penetration Testing				14795.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

EXHIBIT A - Pricing Page

Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	\$1,537.13	\$12,297.00
2	4.2	Website Penetration Testing	8	\$1,302.63	\$10,421.00
3	4.3	Internal/Client-Side Network Penetration Testing	8	\$2,787.13	\$22,297.00
4	4.4	Wireless Penetration Testing	8	\$1,849.38	\$14,795.00
TOTAL BID AMOUNT					\$59,810.00

Please note the following information is being captured for auditing purposes and is an estimate for evaluation only

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

Any product or service not on the Agency provided Pricing Page will not be allowable.

The state cannot accept alternate pricing pages, failure to use Exhibit A Pricing Page could lead to disqualification of vendors bid.

Vendor Name:	Advizex Technologies, LLC
Vendor Address:	680 Andersen Drive, Foster Plaza 10, 2nd Floor, Pittsburgh, PA 15220
Email Address:	mmunoz@advizex.com
Phone Number:	304-615-3301
Fax Number:	216-901-1447
Signature and Date:	<i>Mika Munoz</i>

GENERAL TERMS AND CONDITIONS:

1. CONTRACTUAL AGREEMENT: Issuance of an Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance by the State of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

2. DEFINITIONS: As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

2.1. "Agency" or "Agencies" means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

2.2. "Bid" or "Proposal" means the vendors submitted response to this solicitation.

2.3. "Contract" means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

2.4. "Director" means the Director of the West Virginia Department of Administration, Purchasing Division.

2.5. "Purchasing Division" means the West Virginia Department of Administration, Purchasing Division.

2.6. "Award Document" means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

2.7. "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

2.8. "State" means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

2.9. "Vendor" or "Vendors" means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.



3. CONTRACT TERM; RENEWAL; EXTENSION: The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

Term Contract

Initial Contract Term: The Initial Contract Term will be for a period of ONE (1) _____ . The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

Renewal Term: This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to Three (3) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

Alternate Renewal Term – This contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

Delivery Order Limitations: In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

Fixed Period Contract: This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within _____ days.

Fixed Period Contract with Renewals: This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within _____ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that:

the contract will continue for _____ years;

the contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's Office (Attorney General approval is as to form only).

One-Time Purchase: The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

Construction/Project Oversight: This Contract becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and continues until the project for which the vendor is providing oversight is complete.

Other: Contract Term specified in _____

4. AUTHORITY TO PROCEED: Vendor is authorized to begin performance of this contract on the date of encumbrance listed on the front page of the Award Document unless either the box for "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked in Section 3 above. If either "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked, Vendor must not begin work until it receives a separate notice to proceed from the State. The notice to proceed will then be incorporated into the Contract via change order to memorialize the official date that work commenced.

5. QUANTITIES: The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

Open End Contract: Quantities listed in this Solicitation/Award Document are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

Service: The scope of the service to be provided will be more clearly defined in the specifications included herewith.

Combined Service and Goods: The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.



One-Time Purchase: This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

Construction: This Contract is for construction activity more fully defined in the specifications.

6. EMERGENCY PURCHASES: The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One-Time Purchase contract.

7. REQUIRED DOCUMENTS: All of the items checked in this section must be provided to the Purchasing Division by the Vendor as specified:

LICENSE(S) / CERTIFICATIONS / PERMITS: In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a form acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

See Section 3. QUALIFICATIONS of the Specifications

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.



8. INSURANCE: The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether that insurance requirement is listed in this section.

Vendor must maintain:

Commercial General Liability Insurance in at least an amount of: \$1,000,000.00 per occurrence.

Automobile Liability Insurance in at least an amount of: \$1,000,000.00 per occurrence.

Professional/Malpractice/Errors and Omission Insurance in at least an amount of: \$1,000,000.00 per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

Commercial Crime and Third Party Fidelity Insurance in an amount of: _____ per occurrence.

Cyber Liability Insurance in an amount of: \$1,000,000.00 per occurrence.

Builders Risk Insurance in an amount equal to 100% of the amount of the Contract.

Pollution Insurance in an amount of: _____ per occurrence.

Aircraft Liability in an amount of: _____ per occurrence.



9. WORKERS' COMPENSATION INSURANCE: Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

10. VENUE: All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.

11. LIQUIDATED DAMAGES: This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

_____ for _____.

Liquidated Damages Contained in the Specifications.

Liquidated Damages Are Not Included in this Contract.

12. ACCEPTANCE: Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

13. PRICING: The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

14. PAYMENT IN ARREARS: Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software maintenance, licenses, or subscriptions may be paid annually in advance.

15. PAYMENT METHODS: Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

16. TAXES: The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.



17. ADDITIONAL FEES: Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia, included in the Contract, or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

18. FUNDING: This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.

19. CANCELLATION: The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.b.

20. TIME: Time is of the essence regarding all matters of time and performance in this Contract.

21. APPLICABLE LAW: This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code, or West Virginia Code of State Rules is void and of no effect.

22. COMPLIANCE WITH LAWS: Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

23. ARBITRATION: Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

24. MODIFICATIONS: This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

25. WAIVER: The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

26. SUBSEQUENT FORMS: The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

27. ASSIGNMENT: Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

28. WARRANTY: The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

29. STATE EMPLOYEES: State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

30. PRIVACY, SECURITY, AND CONFIDENTIALITY: The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in www.state.wv.us/admin/purchase/privacy.



31. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

32. LICENSING: In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

33. ANTITRUST: In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

34. VENDOR NON-CONFLICT: Neither Vendor nor its representatives are permitted to have any interest, nor shall they acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency.



35. VENDOR RELATIONSHIP: The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

36. INDEMNIFICATION: The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

37. NO DEBT CERTIFICATION: In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. By submitting a bid, or entering into a contract with the State, Vendor is affirming that (1) for construction contracts, the Vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

38. CONFLICT OF INTEREST: Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.



39. REPORTS: Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at purchasing.division@wv.gov.

40. BACKGROUND CHECK: In accordance with W. Va. Code § 15-2D-3, the State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

41. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS: Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code § 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code § 5A-3-56. As used in this section:

- a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.
- b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process.
- c. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:
 1. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars (\$2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or
 2. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.



42. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL: In Accordance with W. Va. Code § 5-19-1 et seq., and W. Va. CSR § 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars (\$50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a "substantial labor surplus area", as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

43. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE: W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least \$1 million, the Vendor must submit to the Agency a disclosure of interested parties prior to beginning work under this Contract. Additionally, the Vendor must submit a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-work interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.



44. PROHIBITION AGAINST USED OR REFURBISHED: Unless expressly permitted in the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

45. VOID CONTRACT CLAUSES: This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

46. ISRAEL BOYCOTT: Bidder understands and agrees that, pursuant to W. Va. Code § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.



Advizex

Cyber Security Penetration Testing

December 7, 2023

Prepared for The Example Client

Table of Contents

Cyber Security Penetration Testing.....	3
Planning Phase.....	3
Tools Used for Testing	3
Reconnaissance	4
External Target IP Addresses Provided.....	4
Enumeration Phase.....	5
Scanning Phase.....	8
External Vulnerabilities Found.....	8
External Vulnerabilities by Criticality	8
Top Ten External Vulnerabilities by Cumulative Risk.....	9
Top External Vulnerabilities by Type	10
Financial Client Internal Vulnerabilities Found	11
Financial Client Internal Vulnerabilities by Criticality	11
Top Ten Internal Financial Client Vulnerabilities by Critical Risk.....	12
Top Internal Financial Client Vulnerabilities by Type	13
Location Two Internal Vulnerabilities Found	14
Location Two Internal Vulnerabilities by Criticality	14
Top Ten Location Two Internal Vulnerabilities by Critical Risk.....	15
Top Location Two Internal Vulnerabilities by Type.....	16
External Vulnerabilities – Critical	17
External Vulnerabilities – High	17
Vulnerabilities – Medium	17
Financial Client Internal Vulnerabilities – Critical	27
Financial Client Internal Vulnerabilities – High.....	38
Financial Client Internal Vulnerabilities – Medium	38
Location Two Internal Vulnerabilities – Critical	39
Location Two Internal Vulnerabilities – High.....	41
Location Two Internal Vulnerabilities – Medium	41
External Exploitation Phase	42
Audio Codes Access	42
Cisco Benign Certain Exploit	43
Internal Exploitation Phase.....	45
Financial Client Internal Network Server Screenshot.....	45
FirstChoice Internal Network Server Screenshot	46
UPS Network Management	48
Enviromon.net SensorHawk	49
Email Phishing Testing.....	50
Wi-Fi Security Testing	52
External Retest	56
Overall Severity.....	56
Addendum A- Work Effort Matrix.....	57
Addendum B - External/Internal Vulnerability Testing Detail.....	58

Cyber Security Penetration Testing

A Cyber Security Internal and External Penetration Test was conducted at Medical Specialties Distribution from October 4, 2023 to November 30, 2023. Advizex utilized the Open Source Security Testing Methodology Manual (OSTMM) Standard for Penetration. The standard consists of Five Phases: Planning, Reconnaissance, Enumeration, Scanning and Exploitation. The testing was performed by Jeff Jones, Certified Ethical Hacker and CISSP.

Planning Phase

Tools Used for Testing

We used a combination of manual and automated testing. Most the software that we use for testing is available freely on the internet. We utilize open source to mimic what an actual "hacker" would attempt to use. We also use professional grade commercial software to act as verifier. We run multiple tests all system to corroborate and validate our findings.

The following software was used in our testing.

- Metasploit Framework Command Line Interface
- Nessus Professional Feed Software
- NMAP Port Scanning Software
- SQLMAP SQL Injection Tool
- Angry IP Scanner
- Open Source Situational Software

Exploit Attempts

We attempted to exploit all vulnerabilities that we could identify to prove or disprove the existence of the exploit.

Methodologies used in this attempt consisting of:

- Buffer Overflow Attempts
- Backdoors
- Information Disclosures
- Password Brute Forcing and Guessing
- HTTP Source Code Examination and Testing
- SQL Injection
- Cross Site Scripting

Enumeration Phase

It is this phase we try to make active connections to the target system and then try collecting more details information using queries etc. The goal is to get more details information about the target that needs to be compromised. In this case we found the following External TCP Ports open.

IP Address	Open Ports
[REDACTED]	80, 443
[REDACTED]	22
[REDACTED]	443
[REDACTED]	222, 5061, 8082, 8090
[REDACTED]	222, 8081,8090
[REDACTED]	None
[REDACTED]	None
[REDACTED]	222, 5061, 8081, 8090
[REDACTED]	None
[REDACTED]	443
[REDACTED]	21, 1723, 8080
[REDACTED]	13,21,22,23,37,110,111,427,512,513,514,1334,3000,5988,5989,32769,32770,32774
[REDACTED]	None
[REDACTED]	443
[REDACTED]	22
[REDACTED]	None
[REDACTED]	None
[REDACTED]	22
[REDACTED]	None
[REDACTED]	None
[REDACTED]	22
[REDACTED]	22
[REDACTED]	22
[REDACTED]	22
[REDACTED]	80,443
[REDACTED]	21,22,990
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443

IP Address	Open Ports
[REDACTED]	80,443
[REDACTED]	80
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	25
[REDACTED]	80,443
[REDACTED]	22, 80
[REDACTED]	22, 80
[REDACTED]	22, 80
[REDACTED]	443
[REDACTED]	80,443
[REDACTED]	21,22,990
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	80,443
[REDACTED]	443
[REDACTED]	443
[REDACTED]	8080
[REDACTED]	22
[REDACTED]	None
[REDACTED]	22
[REDACTED]	22, 23
[REDACTED]	None
[REDACTED]	22
[REDACTED]	222
[REDACTED]	222

IP Address	Open Ports
[REDACTED]	22
[REDACTED]	22
[REDACTED]	22, 23
[REDACTED]	22
[REDACTED]	13,21,22,23,37,110,111,427,512,513,514,1334,3000,5988,5989,32769,32770,32774
[REDACTED]	22, 23
[REDACTED]	22
[REDACTED]	22, 21
[REDACTED]	222
[REDACTED]	222

Internally, on both Client and Location Two Internal Network all ports were open.

CONFIDENTIAL

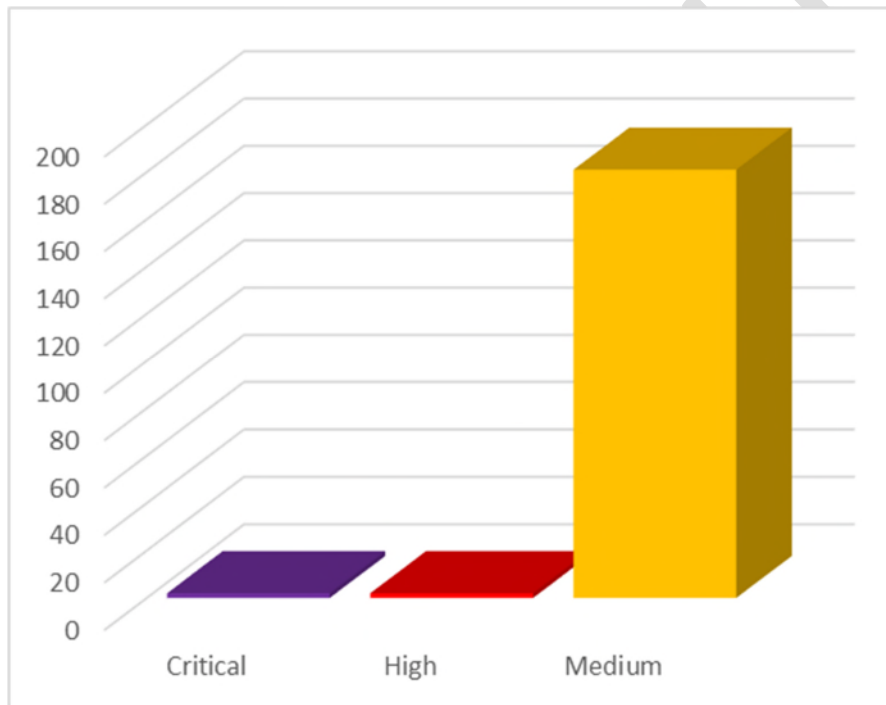
Scanning Phase

The Next Phase of our OSTMM Penetration Testing Framework is known as the Scanning Phase. During this phase, we attempt to identify hosts with the potential for exploitation. Again, we utilize a variety of tools as mentioned above.

External Vulnerabilities Found

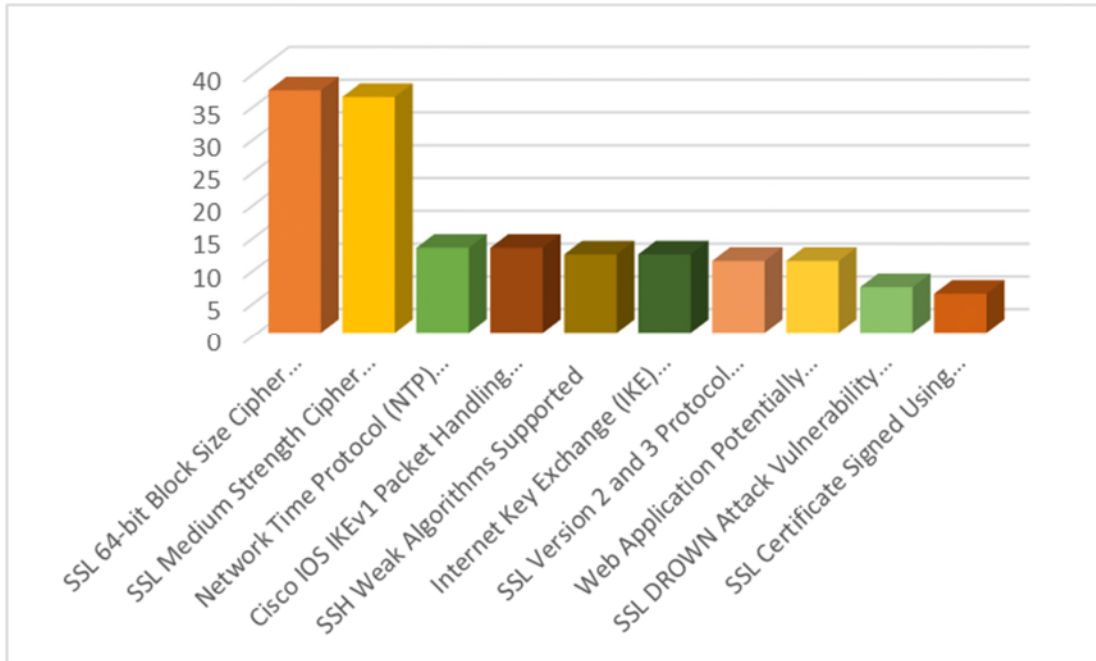
A Vulnerability Assessment/Scan was conducted on the internet exposed devices located on Financial Client's Network. A Total of 85 Internet Host were found, of these 63 or 74 Percent of all devices contained a potential exploit that was rated medium or higher. A total of 2 **Critical**, 2 **High** and 181 **Medium** vulnerabilities were found. Vulnerability Scanning was conducted over a period of 3 business days.

External Vulnerabilities by Criticality



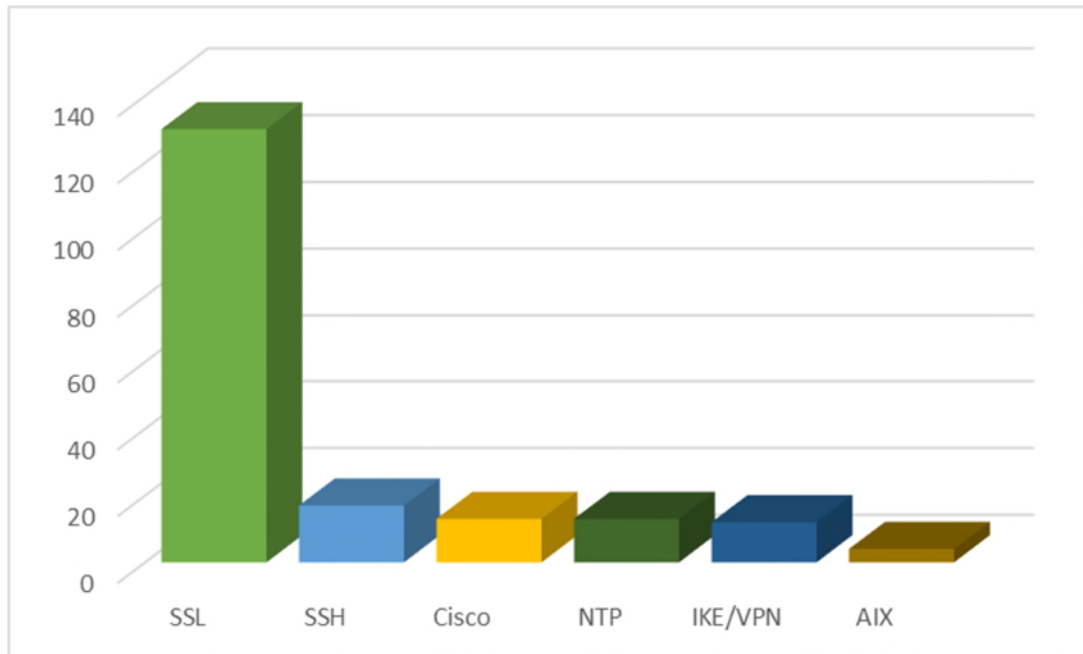
Risk	Count
Critical	2
High	2
Medium	181

Top Ten External Vulnerabilities by Cumulative Risk



Vulnerability	Hosts
SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	37
SSL Medium Strength Cipher Suites Supported	36
Network Time Protocol (NTP) Mode 6 Scanner	13
Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)	13
SSH Weak Algorithms Supported	12
Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	12
SSL Version 2 and 3 Protocol Detection	11
Web Application Potentially Vulnerable to Clickjacking	11
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened encryption)	7
SSL Certificate Signed Using Weak Hashing Algorithm	6

Top External Vulnerabilities by Type

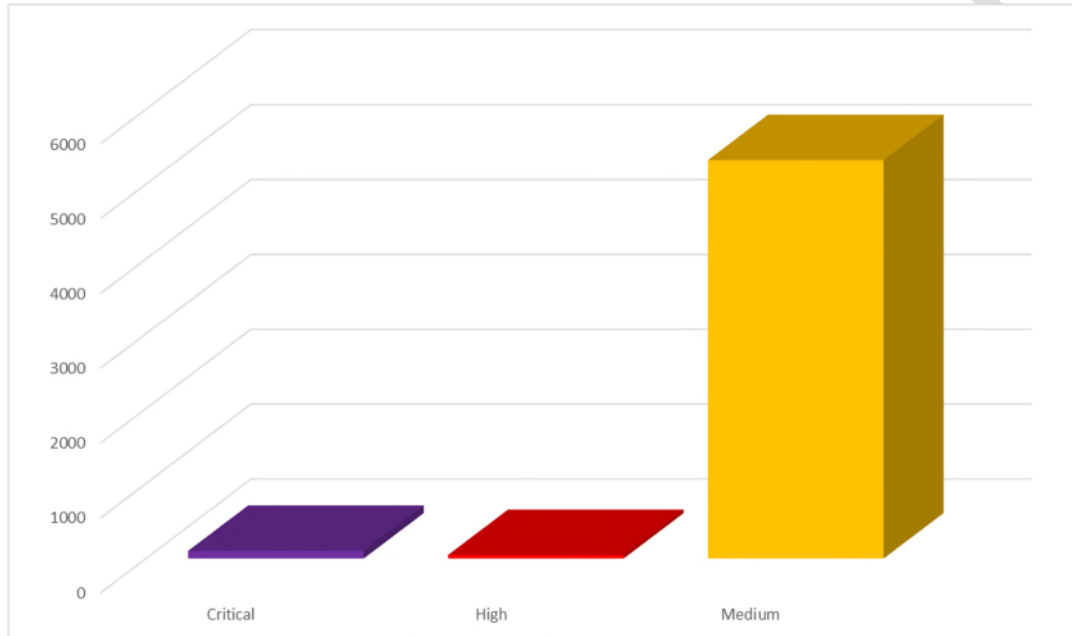


Service Type	Count
SSL	130
SSH	17
Cisco	13
NTP	13
IKE/VPN	12
AIX	4

Financial Client Internal Vulnerabilities Found

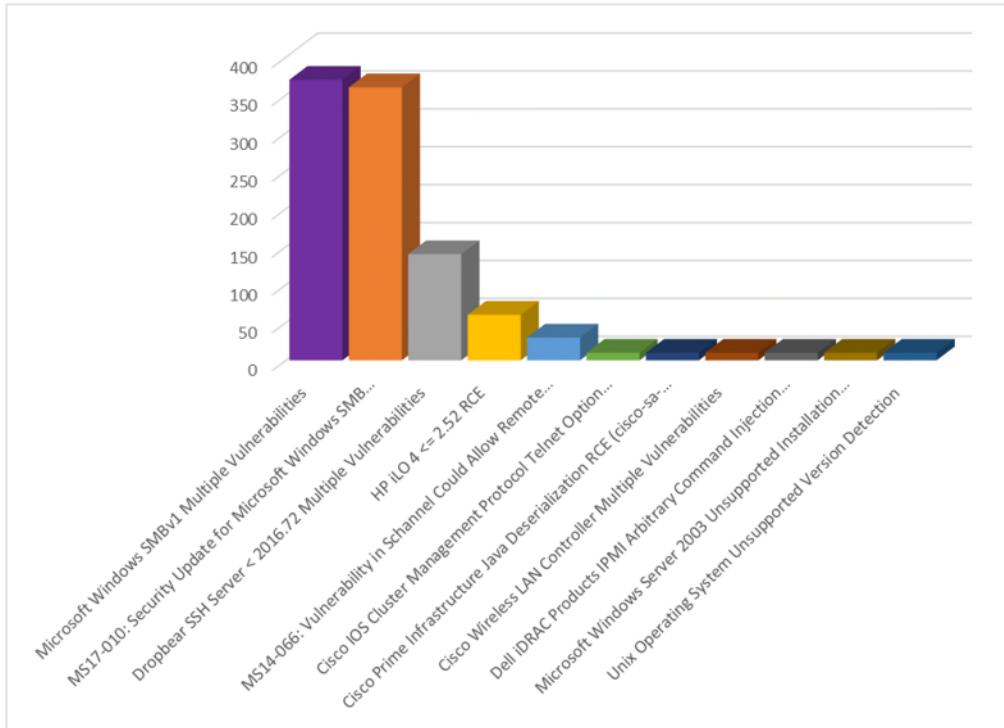
A Vulnerability Assessment/Scan was conducted on the internal devices located on Financial Client's Internal Network. A Total of 720 Internal Hosts were found of these 606 or 84 Percent of all devices contained a potential exploit that was rated medium or higher. A total of 102 **Critical**, 47 **High** and 5321 **Medium** vulnerabilities were found. Internal Vulnerability Scanning was conducted over a period of 2 business days.

Financial Client Internal Vulnerabilities by Criticality



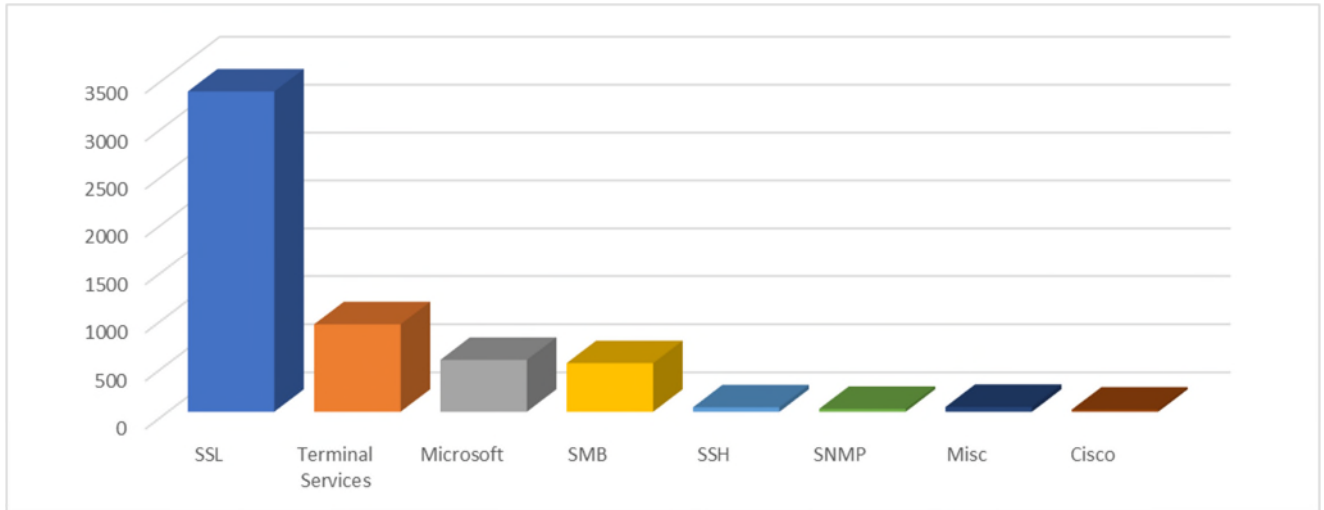
Severity	Count
Critical	102
High	47
Medium	5321

Top Ten Internal Financial Client Vulnerabilities by Critical Risk



Vulnerability	CVSS
Microsoft Windows SMBv1 Multiple Vulnerabilities	370
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	360
Dropbear SSH Server < 2016.72 Multiple Vulnerabilities	140
HP iLO 4 <= 2.52 RCE	60
MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	30
Cisco IOS Cluster Management Protocol Telnet Option Handling RCE (cisco-sa-20170317-cmp)	10
Cisco Prime Infrastructure Java Deserialization RCE (cisco-sa-20160406-remcode)	10
Cisco Wireless LAN Controller Multiple Vulnerabilities	10
Dell iDRAC Products IPMI Arbitrary Command Injection Vulnerability	10
Microsoft Windows Server 2003 Unsupported Installation Detection (ERRATICGOPHER)	10
Unix Operating System Unsupported Version Detection	10

Top Internal Financial Client Vulnerabilities by Type

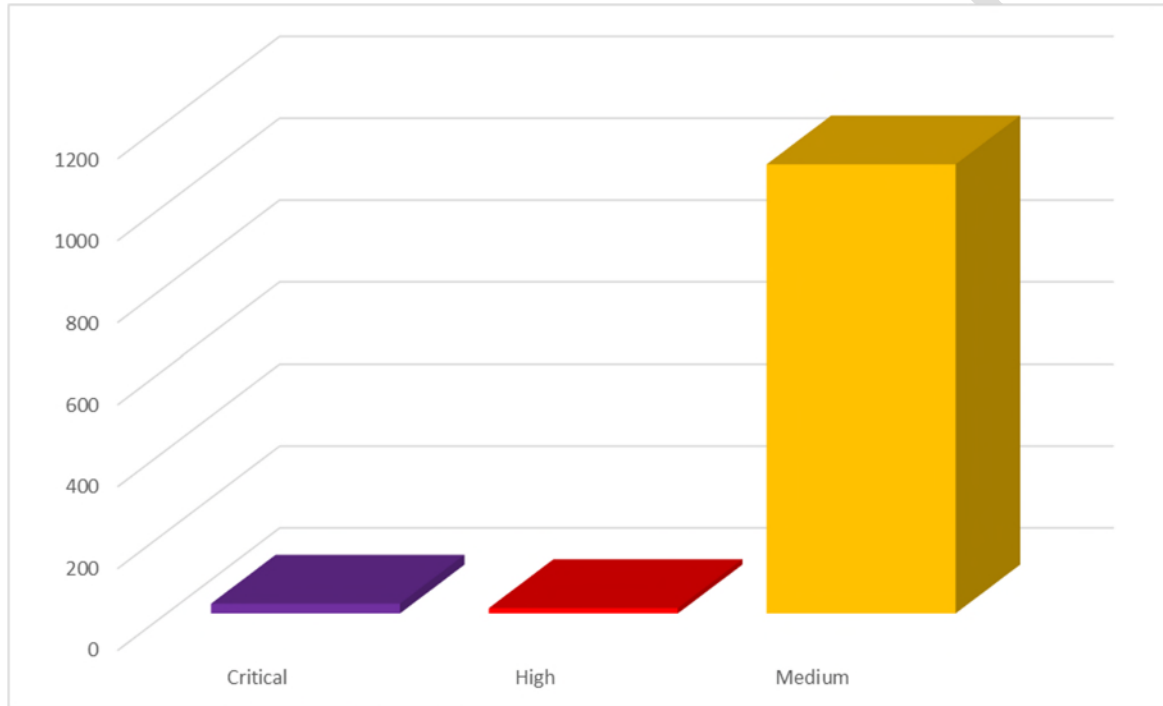


Type	Count
SSL	3339
Terminal Services	908
Microsoft	539
SMB	505
SSH	46
SNMP	30
Misc.	50
Cisco	22

Location Two Internal Vulnerabilities Found

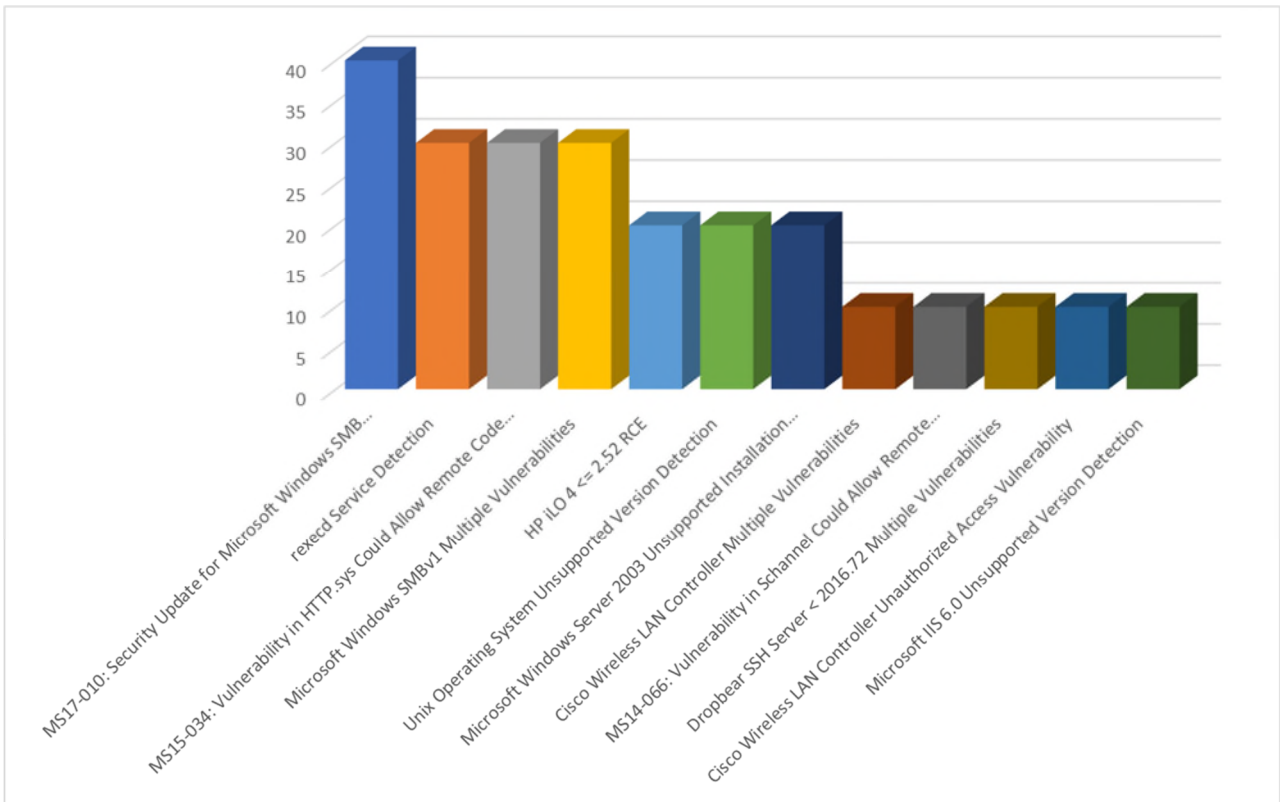
A Vulnerability Assessment/Scan was conducted on the internal devices located on Location Two's Network. A Total of 316 Internal Hosts were found, of these 165 or 52 Percent of all devices contained a potential exploit that was rated medium or higher. A total of 24 **Critical**, 13 **High** and 1096 **Medium** vulnerabilities were found. Vulnerability Scanning was conducted over a period of 3 business days.

Location Two Internal Vulnerabilities by Criticality



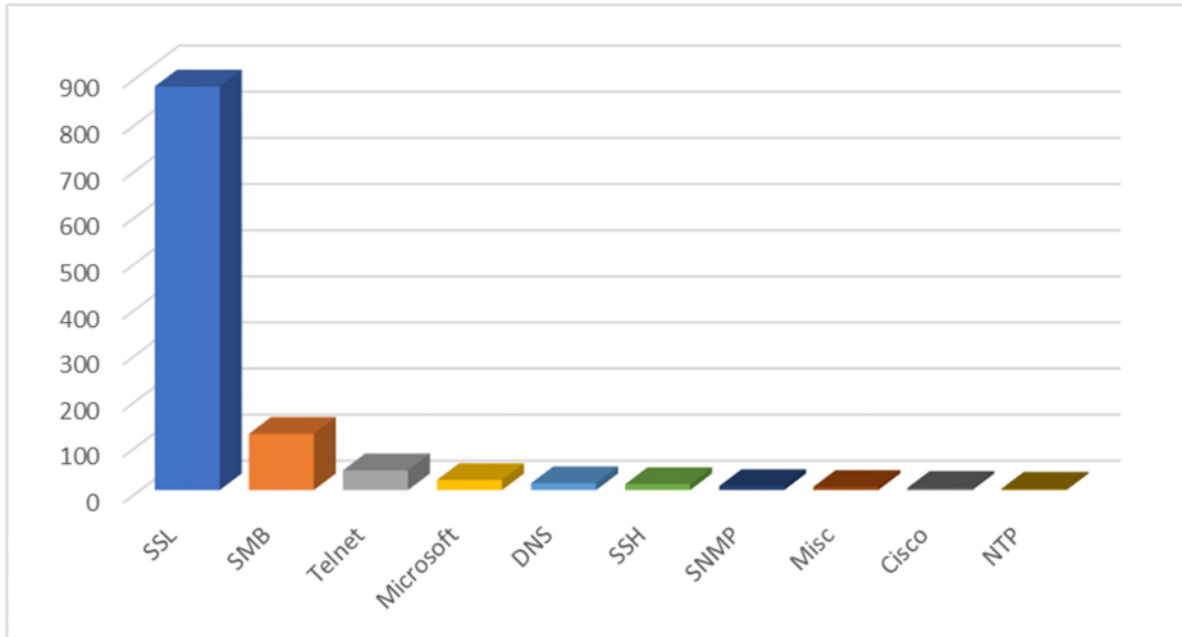
Severity	Count
Critical	24
High	13
Medium	1096

Top Ten Location Two Internal Vulnerabilities by Critical Risk



Vulnerability	CVSS
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya)	40
rexecd Service Detection	30
MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	30
Microsoft Windows SMBv1 Multiple Vulnerabilities	30
HP iLO 4 <= 2.52 RCE	20
Unix Operating System Unsupported Version Detection	20
Microsoft Windows Server 2003 Unsupported Installation Detection (ERRATICGOPHER)	20
Cisco Wireless LAN Controller Multiple Vulnerabilities	10
MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	10
Dropbear SSH Server < 2016.72 Multiple Vulnerabilities	10
Cisco Wireless LAN Controller Unauthorized Access Vulnerability	10
Microsoft IIS 6.0 Unsupported Version Detection	10

Top Location Two Internal Vulnerabilities by Type



Type	Count
SSL	875
SMB	122
Telnet	43
Microsoft	22
DNS	15
SSH	13
SNMP	9
Misc.	7
Cisco	5
NTP	3

External Vulnerabilities – Critical

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	512	rexecd Service Detection
10	Critical	[REDACTED]	tcp	512	rexecd Service Detection

External Vulnerabilities – High

CVSS	Risk	Host	Protocol	Port	Name
7.5	High	[REDACTED]	tcp	513	rlogin Service Detection
7.5	High	[REDACTED]	tcp	513	rlogin Service Detection

Vulnerabilities – Medium

CVSS	Risk	Host	Protocol	Port	Name
7.5	High	[REDACTED]	tcp	513	rlogin Service Detection
6.4	Medium	[REDACTED]	tcp	5061	SSL Certificate Cannot Be Trusted
6.4	Medium	[REDACTED]	tcp	5061	SSL Self-Signed Certificate
6.4	Medium	[REDACTED]	tcp	443	SSL Certificate Cannot Be Trusted
6.4	Medium	[REDACTED]	tcp	7980	SSL Certificate Cannot Be Trusted
6.4	Medium	[REDACTED]	tcp	443	SSL Self-Signed Certificate
6.4	Medium	[REDACTED]	tcp	443	SSL Certificate Cannot Be Trusted
6.4	Medium	[REDACTED]	tcp	25	SSL Certificate Cannot Be Trusted
6.4	Medium	[REDACTED]	tcp	25	SSL Self-Signed Certificate

CVSS	Risk	Host	Protocol	Port	Name
6.4	Medium	[REDACTED]	tcp	443	SSL Self-Signed Certificate
5.8	Medium	[REDACTED]	tcp	23	Unencrypted Telnet Server
5.8	Medium	[REDACTED]	tcp	23	Unencrypted Telnet Server
5	Medium	[REDACTED]	udp	123	Network Time Protocol (NTP) Mode 6 Scanner
5	Medium	[REDACTED]	udp	500	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)
5	Medium	[REDACTED]	udp	123	Network Time Protocol (NTP) Mode 6 Scanner
5	Medium	[REDACTED]	udp	500	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
5	Medium	[REDACTED]	udp	500	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)
5	Medium	[REDACTED]	udp	123	Network Time Protocol (NTP) Mode 6 Scanner
5	Medium	[REDACTED]	udp	123	Network Time Protocol (NTP) Mode 6 Scanner
5	Medium	[REDACTED]	udp	500	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
5	Medium	[REDACTED]	udp	500	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)
5	Medium	[REDACTED]	udp	500	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
5	Medium	[REDACTED]	udp	500	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)
5	Medium	[REDACTED]	udp	123	Network Time Protocol (NTP) Mode 6 Scanner
5	Medium	[REDACTED]	tcp	9510	SSL Version 2 and 3 Protocol Detection
5	Medium	[REDACTED]	tcp	9510	SSL Medium Strength Cipher Suites Supported

CVSS	Risk	Host	Protocol	Port	Name
5	Medium	[REDACTED]	tcp	9510	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	udp	123	Network Time Protocol (NTP) Mode 6 Scanner
5	Medium	[REDACTED]	tcp	7980	SSL Version 2 and 3 Protocol Detection
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	7980	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	udp	500	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	7980	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	udp	500	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	udp	500	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
5	Medium	[REDACTED]	udp	500	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)
5	Medium	[REDACTED]	udp	123	Network Time Protocol (NTP) Mode 6 Scanner
5	Medium	[REDACTED]	udp	500	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
5	Medium	[REDACTED]	udp	500	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)
5	Medium	[REDACTED]	udp	123	Network Time Protocol (NTP) Mode 6 Scanner
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported

CVSS	Risk	Host	Protocol	Port	Name
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	udp	123	Network Time Protocol (NTP) Mode 6 Scanner
5	Medium	[REDACTED]	udp	500	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
5	Medium	[REDACTED]	udp	500	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)
5	Medium	[REDACTED]	udp	500	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
5	Medium	[REDACTED]	udp	500	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)
5	Medium	[REDACTED]	udp	123	Network Time Protocol (NTP) Mode 6 Scanner
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported

CVSS	Risk	Host	Protocol	Port	Name
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	Microsoft Exchange Client Access Server Information Disclosure
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Version 2 and 3 Protocol Detection
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Version 2 and 3 Protocol Detection
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	Microsoft Exchange Client Access Server Information Disclosure
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	25	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	25	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Version 2 and 3 Protocol Detection
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Version 2 and 3 Protocol Detection
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported

CVSS	Risk	Host	Protocol	Port	Name
5	Medium		tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium		tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium		tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium		tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium		tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium		tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium		tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium		tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium		tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium		tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium		tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium		tcp	443	SSL Version 2 and 3 Protocol Detection
5	Medium		tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium		tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium		tcp	443	SSL Version 2 and 3 Protocol Detection
5	Medium		tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium		tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium		tcp	443	SSL Version 2 and 3 Protocol Detection
5	Medium		tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium		tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium		tcp	443	SSL Version 2 and 3 Protocol Detection
5	Medium		tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium		tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium		tcp	443	SSL Version 2 and 3 Protocol Detection
5	Medium		tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium		tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium		tcp	443	SSL Medium Strength Cipher Suites Supported

CVSS	Risk	Host	Protocol	Port	Name
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL Medium Strength Cipher Suites Supported
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	tcp	443	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
5	Medium	[REDACTED]	udp	500	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
5	Medium	[REDACTED]	udp	500	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredialled check)
5	Medium	[REDACTED]	udp	123	Network Time Protocol (NTP) Mode 6 Scanner
5	Medium	[REDACTED]	udp	500	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
5	Medium	[REDACTED]	udp	500	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredialled check)
5	Medium	[REDACTED]	udp	123	Network Time Protocol (NTP) Mode 6 Scanner
5	Medium	[REDACTED]	udp	500	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
5	Medium	[REDACTED]	udp	500	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredialled check)
5	Medium	[REDACTED]	udp	123	Network Time Protocol (NTP) Mode 6 Scanner

CVSS	Risk	Host	Protocol	Port	Name
5	Medium	[REDACTED]	udp	500	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
5	Medium	[REDACTED]	udp	500	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)
4.3	Medium	[REDACTED]	tcp	222	SSH Weak Algorithms Supported
4.3	Medium	[REDACTED]	tcp	222	SSH Weak Algorithms Supported
4.3	Medium	[REDACTED]	tcp	222	SSH Weak Algorithms Supported
4.3	Medium	[REDACTED]	tcp	22	SSH Weak Algorithms Supported
4.3	Medium	[REDACTED]	tcp	9510	SSL Weak Cipher Suites Supported
4.3	Medium	[REDACTED]	tcp	9510	SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE)
4.3	Medium	[REDACTED]	tcp	443	SSL Weak Cipher Suites Supported
4.3	Medium	[REDACTED]	tcp	11162	Web Application Potentially Vulnerable to Clickjacking
4.3	Medium	[REDACTED]	tcp	7980	Web Application Potentially Vulnerable to Clickjacking
4.3	Medium	[REDACTED]	tcp	28309	SSH Weak Algorithms Supported
4.3	Medium	[REDACTED]	tcp	830	SSH Weak Algorithms Supported
4.3	Medium	[REDACTED]	tcp	8081	Web Application Potentially Vulnerable to Clickjacking
4.3	Medium	[REDACTED]	tcp	22	SSH Weak Algorithms Supported
4.3	Medium	[REDACTED]	tcp	443	SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE)
4.3	Medium	[REDACTED]	tcp	22	SSH Weak Algorithms Supported
4.3	Medium	[REDACTED]	tcp	22	SSH Weak Algorithms Supported
4.3	Medium	[REDACTED]	tcp	22	SSH Weak Algorithms Supported
4.3	Medium	[REDACTED]	tcp	443	SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE)
4.3	Medium	[REDACTED]	tcp	443	Web Application Potentially Vulnerable to Clickjacking

CVSS	Risk	Host	Protocol	Port	Name
4.3	Medium	[REDACTED]	tcp	443	Web Application Potentially Vulnerable to Clickjacking
4.3	Medium	[REDACTED]	tcp	443	Web Application Potentially Vulnerable to Clickjacking
4.3	Medium	[REDACTED]	tcp	443	Web Application Potentially Vulnerable to Clickjacking
4.3	Medium	[REDACTED]	tcp	443	Web Application Potentially Vulnerable to Clickjacking
4.3	Medium	[REDACTED]	tcp	80	Web Application Potentially Vulnerable to Clickjacking
4.3	Medium	[REDACTED]	tcp	443	Web Application Potentially Vulnerable to Clickjacking
4.3	Medium	[REDACTED]	tcp	443	Web Application Potentially Vulnerable to Clickjacking
4.3	Medium	[REDACTED]	tcp	22	SSH Weak Algorithms Supported
4.3	Medium	[REDACTED]	tcp	222	SSH Weak Algorithms Supported
4	Medium	[REDACTED]	tcp	22	SSH Protocol Version 1 Session Key Retrieval
4	Medium	[REDACTED]	tcp	22	SSH Protocol Version 1 Session Key Retrieval
4	Medium	[REDACTED]	tcp	443	SSL Certificate Signed Using Weak Hashing Algorithm
4	Medium	[REDACTED]	tcp	22	SSH Protocol Version 1 Session Key Retrieval
4	Medium	[REDACTED]	tcp	443	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened Encryption)
4	Medium	[REDACTED]	tcp	25	SSL Certificate Signed Using Weak Hashing Algorithm
4	Medium	[REDACTED]	tcp	443	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened Encryption)
4	Medium	[REDACTED]	tcp	443	SSL Certificate Signed Using Weak Hashing Algorithm
4	Medium	[REDACTED]	tcp	443	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened Encryption)
4	Medium	[REDACTED]	tcp	443	SSL Certificate Signed Using Weak Hashing Algorithm
4	Medium	[REDACTED]	tcp	443	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened Encryption)
4	Medium	[REDACTED]	tcp	443	SSL Certificate Signed Using Weak Hashing Algorithm
4	Medium	[REDACTED]	tcp	443	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened Encryption)

CVSS	Risk	Host	Protocol	Port	Name
4	Medium	[REDACTED]	tcp	443	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened Encryption)
4	Medium	[REDACTED]	tcp	443	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened Encryption)
4	Medium	[REDACTED]	tcp	443	SSL Certificate Signed Using Weak Hashing Algorithm
4	Medium	[REDACTED]	tcp	22	SSH Protocol Version 1 Session Key Retrieval
4	Medium	[REDACTED]	tcp	22	SSH Protocol Version 1 Session Key Retrieval

CONFIDENTIAL

Financial Client Internal Vulnerabilities – Critical

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	████████	tcp	443	Cisco Prime Infrastructure Java Deserialization RCE (cisco-sa-20160406-remcode)
10	Critical	████████	tcp	0	Unix Operating System Unsupported Version Detection
10	Critical	████████	tcp	443	Dell iDRAC Products IPMI Arbitrary Command Injection Vulnerability
10	Critical	████████	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	████████	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	████████	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	████████	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	████████	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	████████	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	████████	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	████████	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	████████	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	████████	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	3389	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	0	Cisco IOS Cluster Management Protocol Telnet Option Handling RCE (cisco-sa-20170317-cmp)
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	0	Cisco Wireless LAN Controller Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	3389	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	3389	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	0	Microsoft Windows Server 2003 Unsupported Installation Detection (ERRATICGOPHER)

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	443	HP iLO 4 <= 2.52 RCE
10	Critical	[REDACTED]	tcp	80	HP iLO 4 <= 2.52 RCE
10	Critical	[REDACTED]	tcp	443	HP iLO 4 <= 2.52 RCE
10	Critical	[REDACTED]	tcp	80	HP iLO 4 <= 2.52 RCE
10	Critical	[REDACTED]	tcp	443	HP iLO 4 <= 2.52 RCE
10	Critical	[REDACTED]	tcp	80	HP iLO 4 <= 2.52 RCE
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities

Financial Client Internal Vulnerabilities – High

See Attached HTML and Excel Reports

Financial Client Internal Vulnerabilities – Medium

See Attached HTML and Excel Reports

CONFIDENTIAL

Location Two Internal Vulnerabilities – Critical

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	512	rexecd Service Detection
10	Critical	[REDACTED]	tcp	0	Unix Operating System Unsupported Version Detection
10	Critical	[REDACTED]	tcp	3389	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
10	Critical	[REDACTED]	tcp	80	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)
10	Critical	[REDACTED]	tcp	0	Microsoft Windows Server 2003 Unsupported Installation Detection (ERRATICGOPHER)
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	443	HP iLO 4 <= 2.52 RCE
10	Critical	[REDACTED]	tcp	80	HP iLO 4 <= 2.52 RCE
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	80	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)
10	Critical	[REDACTED]	tcp	22	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	80	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	0	Microsoft Windows Server 2003 Unsupported Installation Detection (ERRATICGOPHER)
10	Critical	[REDACTED]	tcp	445	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
10	Critical	[REDACTED]	tcp	80	Microsoft IIS 6.0 Unsupported Version Detection
10	Critical	[REDACTED]	tcp	445	Microsoft Windows SMBv1 Multiple Vulnerabilities
10	Critical	[REDACTED]	tcp	512	rexecd Service Detection
10	Critical	[REDACTED]	tcp	0	Unix Operating System Unsupported Version Detection
10	Critical	[REDACTED]	tcp	512	rexecd Service Detection

CVSS	Risk	Host	Protocol	Port	Name
10	Critical	[REDACTED]	tcp	0	Cisco Wireless LAN Controller Unauthorized Access Vulnerability
10	Critical	[REDACTED]	tcp	0	Cisco Wireless LAN Controller Multiple Vulnerabilities

Location Two Internal Vulnerabilities – High

See Attached HTML and Excel Reports

Location Two Internal Vulnerabilities – Medium

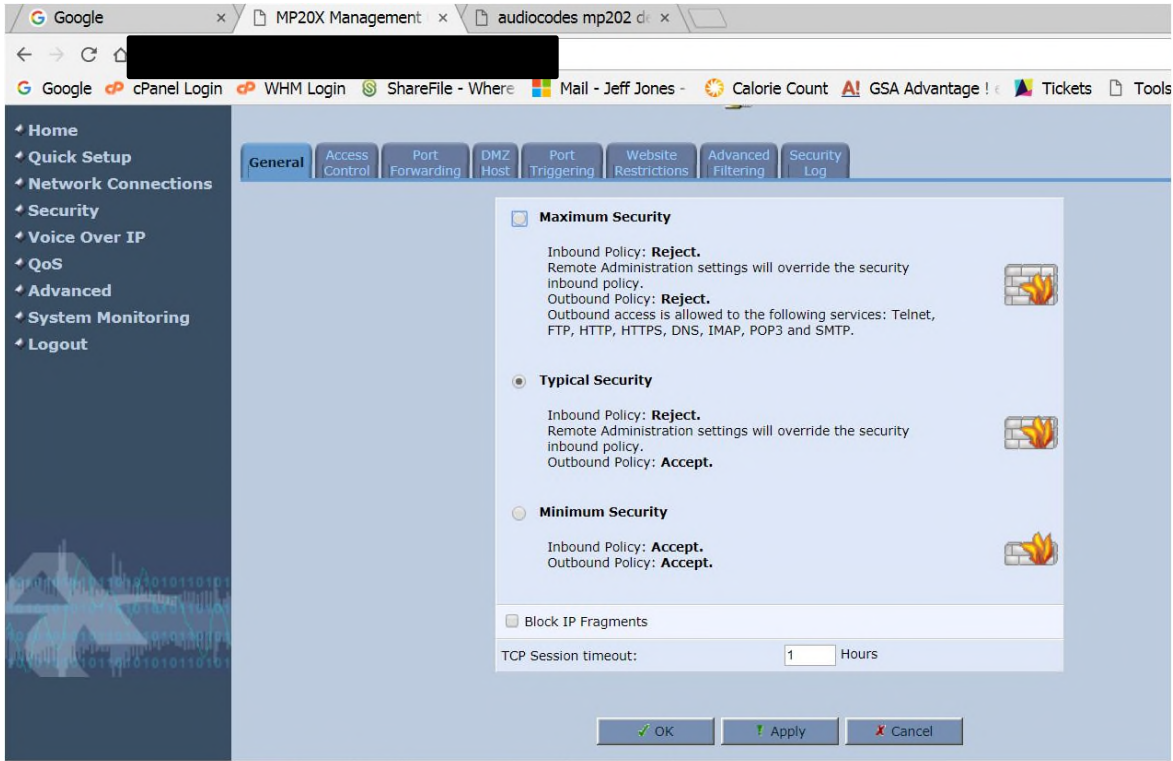
See Attached HTML and Excel Reports

CONFIDENTIAL

External Exploitation Phase

During this phase, we try to exploit any known found vulnerabilities. Multiple exploits were found and are demonstrated as follows.

Audio Codes Access



By using the Default Username and Password we were able to login to the device and gain administrative access as demonstrated by the screenshot.

Cisco Benign Certain Exploit

A vulnerability in Internet Key Exchange version 1 (IKEv1) packet processing code in Cisco IOS, Cisco IOS XE, and Cisco IOS XR Software could allow an unauthenticated, remote attacker to retrieve memory contents, which could lead to the disclosure of confidential information.

The vulnerability is due to insufficient condition checks in the part of the code that handles IKEv1 security negotiation requests. An attacker could exploit this vulnerability by sending a crafted IKEv1 packet to an affected device configured to accept IKEv1 security negotiation requests. A successful exploit could allow the attacker to retrieve memory contents, which could lead to the disclosure of confidential information.

We confirmed the existence of the exploit utilizing an open source hacking framework known as Metasploit.

```
msf auxiliary(cisco_ike_benigncertain) > unset RHOSTS
Unsetting RHOSTS...

[*] Scanned 14 of 14 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(cisco_ike_benigncertain) > []
```

We tested this vulnerability and attempted to exploit. The exploit is available in the wild. This was the result.

```
root@HP-ProBook-6470b:~# ./bc-id -t [REDACTED] -I sendpacket-lg2.raw
Connection established.

Opening input file sendpacket-lg2.raw....

WARNING: this payload is greater than 2528 bytes.

If this payload is sent to a target running 6.1.(x) or earlier, the target
will crash *immediately*; you will *not* receive a response packet.

If this payload is sent to a target running 6.2.(x) or later, the target
will crash shortly afterwards, but you should receive a response packet.

Do you want to continue? [y/n]: n

Bailing out ...

root@HP-ProBook-6470b:~# █
```

We did not continue because we did not want to crash the system.

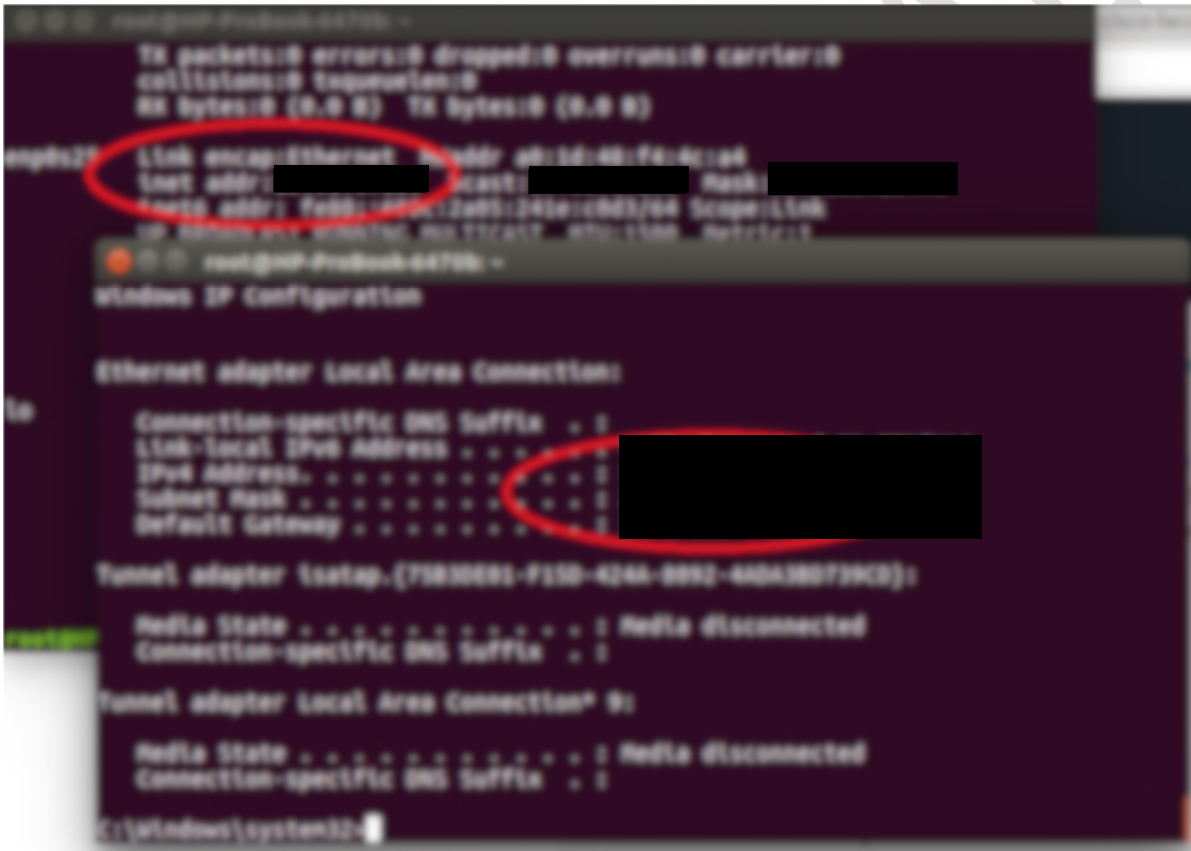
CONFIDENTIAL

Internal Exploitation Phase

Administrative Server Access

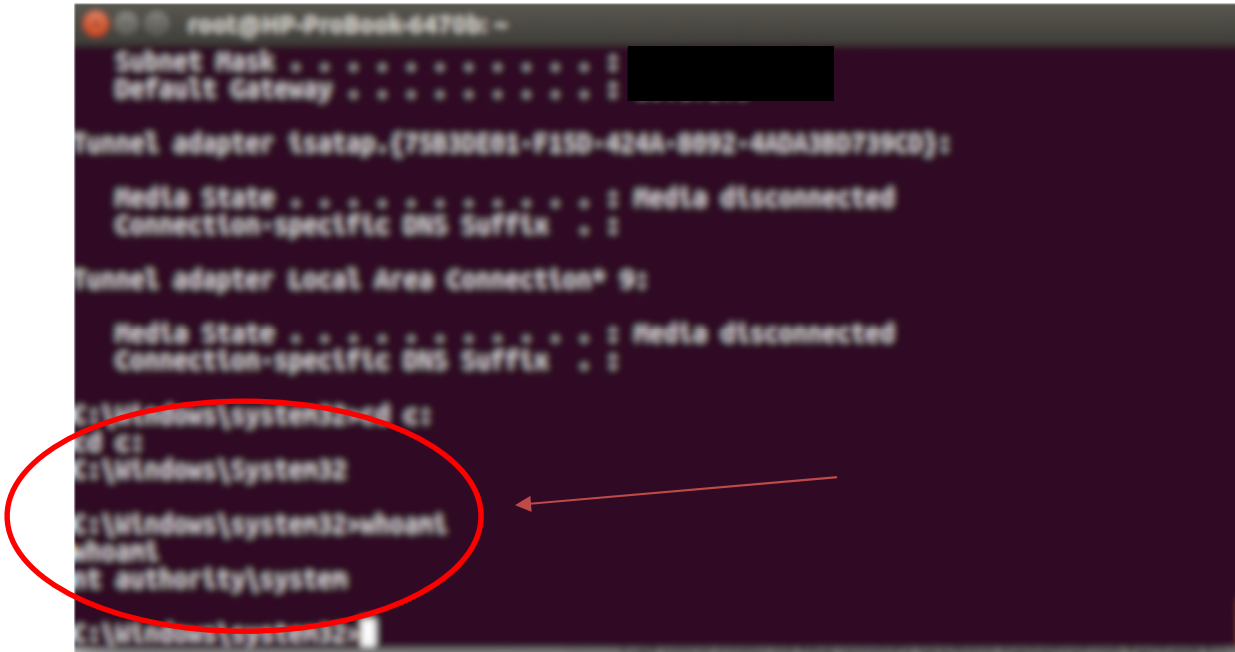
We gained administrative access to Servers both on the Financial Client and Location Two Internal Networks. The exploit known as Eternal Blue is an exploit generally believed to be developed by the U.S. National Security Agency (NSA). It was leaked by the Shadow Brokers hacker group on April 14, 2017, and was used as part of the worldwide WannaCry ransomware attack and the Petya cyberattack.

Financial Client Internal Network Server Screenshot



As demonstrated our IP Address is displayed on the background screenshot and the victim server is displayed at the forefront.

The screen shot below demonstrates that we have administrative access.



FirstChoice Internal Network Server Screenshot

Both exploits were performed using the Metasploit Exploitation Framework and the screen shot below demonstrates the beginning of the attack.



Once again, a screenshot from the FirstChoice Internal Network.

```
root@HP-ProBook-6470b: ~
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . :
    IPv4 Address. . . . . :
    Subnet Mask . . . . . :
    Default Gateway . . . . . :

Tunnel adapter Local Area Connection* 9:

    Media State . . . . . : Media disconnected
```

The screenshot below shows a directory listing of the FirstChoice Server and a “whoami” command demonstrates administrative access.

```
root@HP-ProBook-6470b: ~
07/13/2009 07:41 PM          59,392 wslshlp.dll
01/13/2013 12:09 PM          522,752 XpsOdiConverter.dll
01/13/2013 11:05 AM       1,492,432 XpsPrint.dll
11/20/2010 07:27 AM          229,888 XpsFasterService.dll
11/20/2010 07:27 AM       3,008,000 XpsServices.dll
07/13/2009 07:41 PM       1,576,448 Xpswvc.dll
06/10/2009 03:03 PM           4,041 wizard.dtd
07/13/2009 07:39 PM           42,496 wizard.exe
07/13/2009 07:41 PM          432,640 wizardr.dll
07/13/2009 07:41 PM          101,888 wreg.dll
07/13/2009 07:41 PM          201,216 wstpdul.dll
07/13/2009 07:41 PM          129,536 wstpdul2.dll
07/03/2013 11:04 PM      <DIR>      sh-CN
07/03/2013 11:04 PM      <DIR>      sh-MK
07/03/2013 11:04 PM      <DIR>      sh-TW
11/20/2010 07:27 PM          366,080 zipfldr.dll
2387 File(s) 2,104,493,693 bytes
90 Dir(s) 276,721,894,948 bytes free

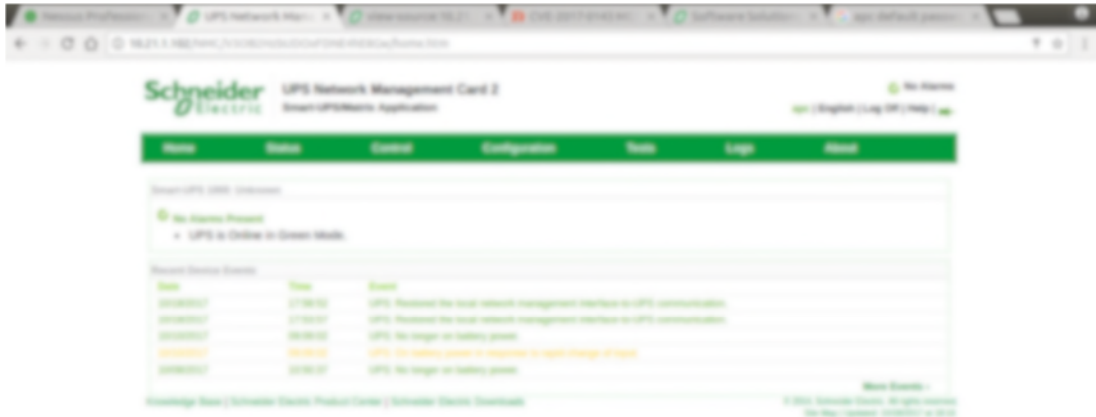
C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Physical Penetration Testing

UPS Network Management

The following screenshot is from a UPS System Console on the Internal Financial Client Network. Access was gained by using the default username and password.



CONFIDENTIAL

Enviromon.net SensorHawk

We were also able to gain administrative access to a temperature monitoring system using default username and password, screenshot shown below.



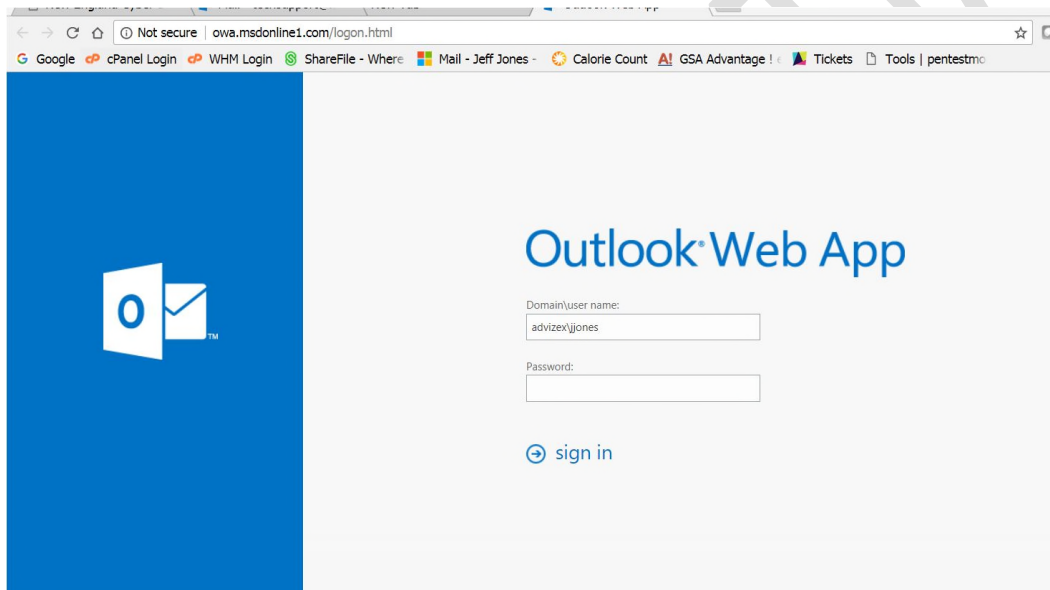
Email Phishing Testing

Email Phishing Testing was conducted for Financial Client. We purchased a domain name that was similar Financial Client domain. The domain we bought was msdonline1.com. This domain would serve as our email and our phishing exploit site domain name.

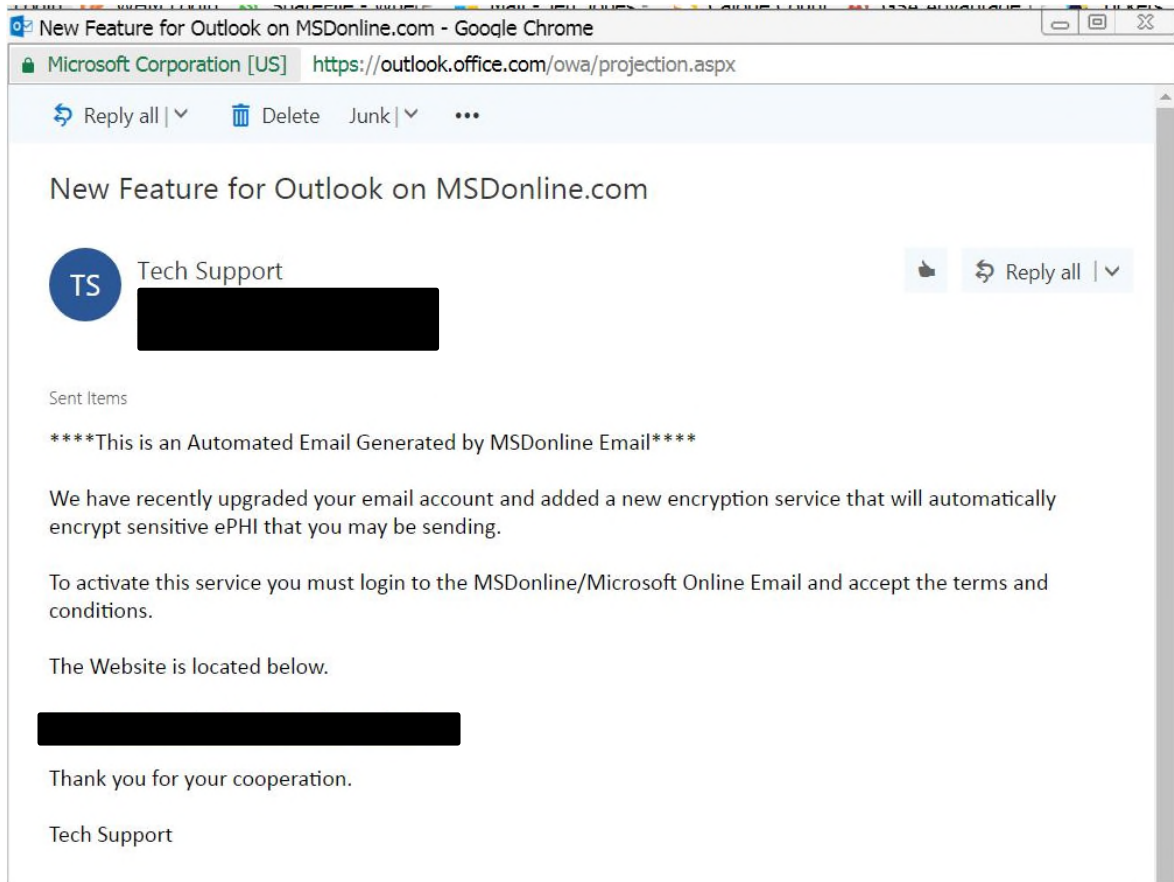
A list of potential targets was provided by Financial Client. Of those we chose 56 random names and began phishing test.

We created an Email Web Site that was a clone of an Outlook Web Server, IP Address 69.84.159.237, the ip address did not resolve in nslookup. The site was programmed to capture any input data and save as a text file. After entering the username and password the target would be passed instantly to the real web site.

The Site Pictured Below.



An Email was then sent to the 56 individuals throughout the organization asking that they login to verify new features in the email account. An Example is shown below.



Of the 56 emails, we received 1 response.

CONFIDENTIAL

Wi-Fi Security Testing

We tested the strength and ability for a hacker to capture and decode the Pre-Shared Authentication Password for the Wireless LANs in [REDACTED]

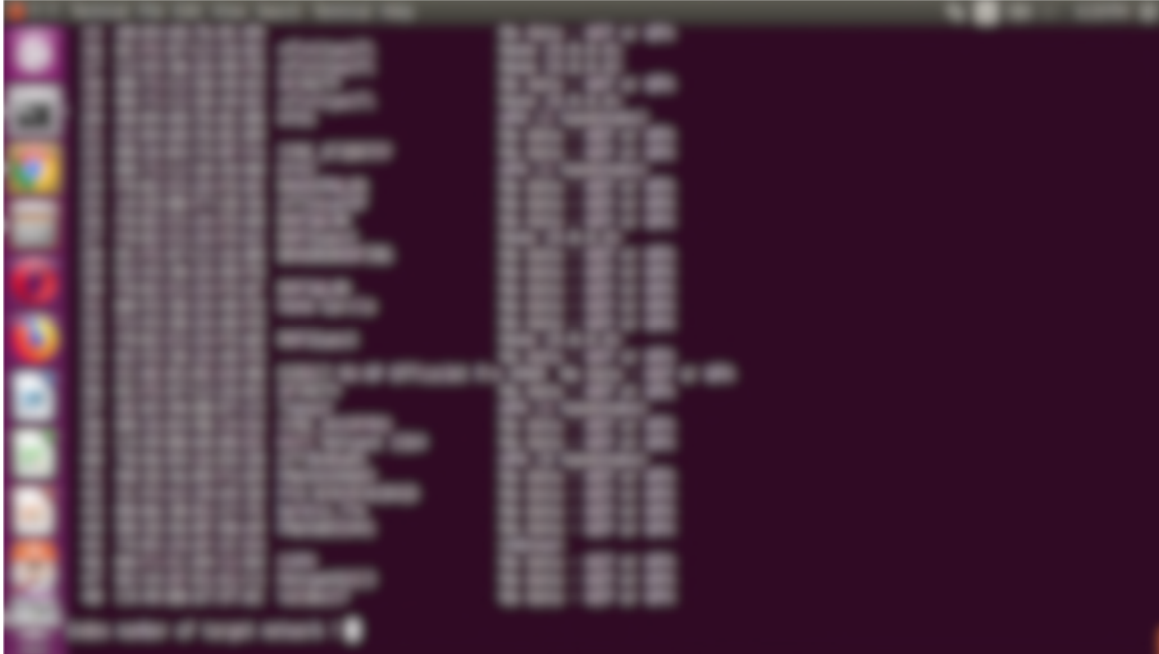
The process is straight forward, using a combination of Kismet and Aircrack Next Generation (Aircrack-NG) hacking tool Suite, we were able to capture the encrypted WPA2 Handshake.

Examples are shown below.

Target Identification with Kismet



Password Handshake Capture with AiroDump-NG



Once we capture handshake we attempted to break the password know as the Pre-shared key. The capture is of the handshake is then fed into the Password Cracker and is shown below.

```
root@HP-ProBook-6470b: ~  
Aircrack-ng 1.2 beta3  
[00:00:11] 22284 keys tested (2014.47 k/s)  
Current passphrase:  
Master Key      :  
Transient Key   :  
EAPOL HMAC     :
```

Although, the word list we used was over 16 GB of text, no Passwords were found.

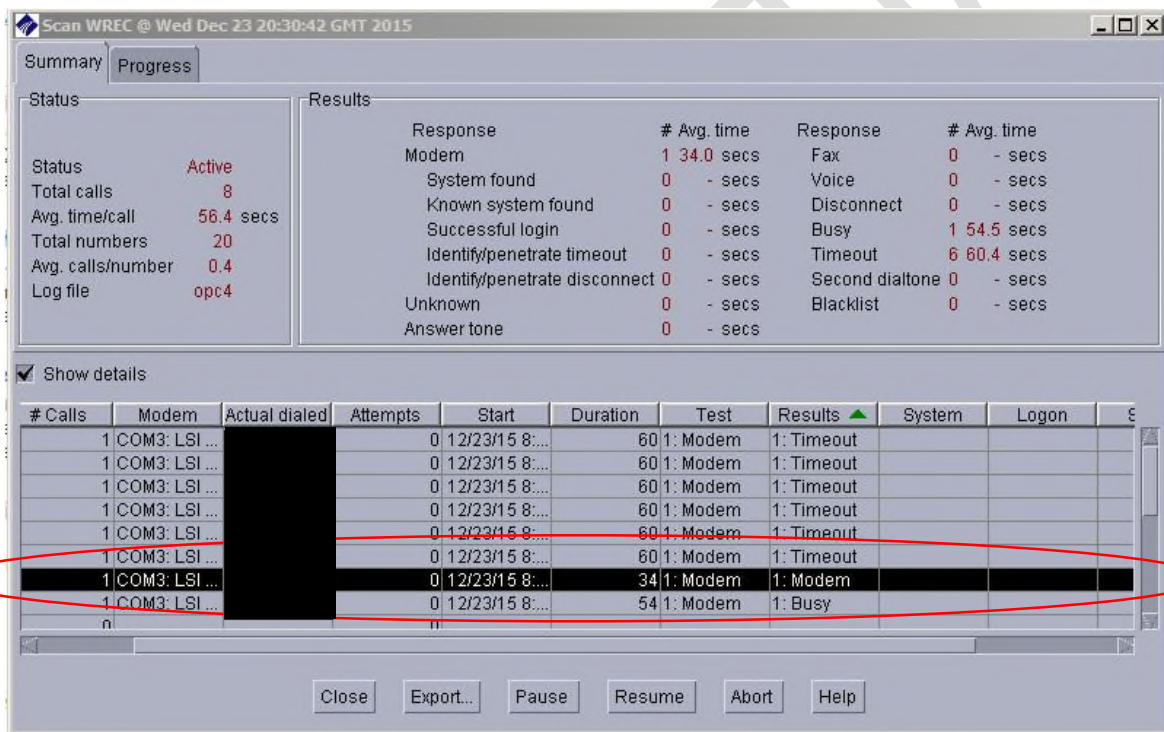
PBX Penetration Testing

War Dialing

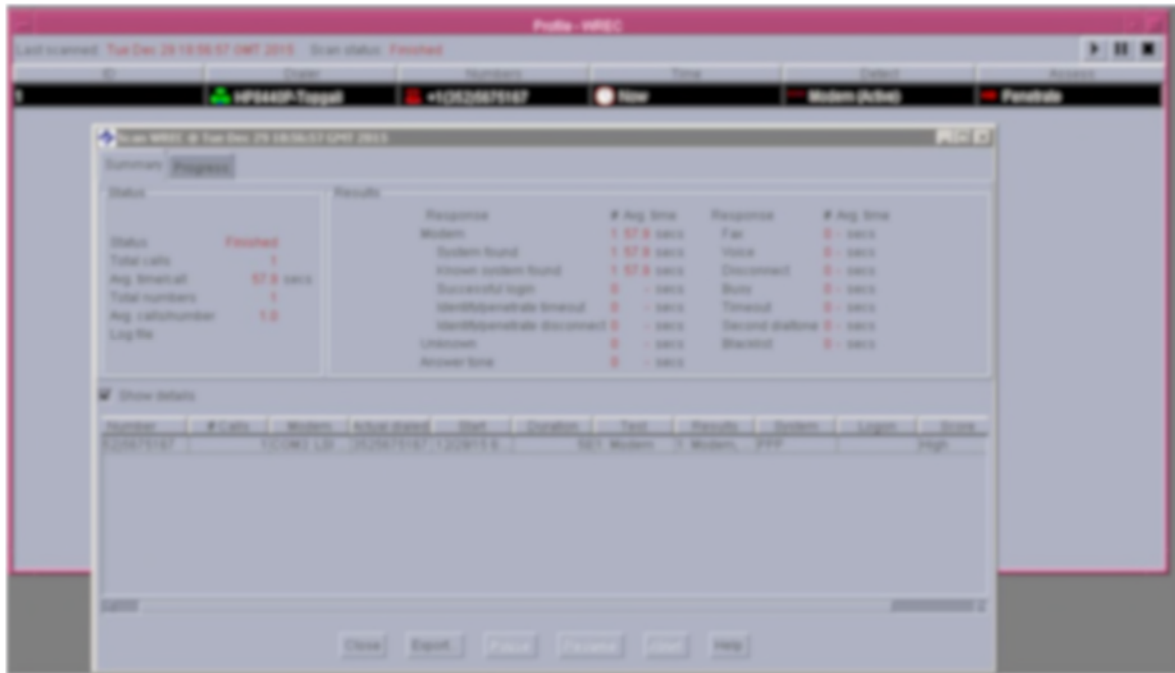
Another technique that a hacker might use is to scan phone numbers with similar phone numbers as WREC. We scanned over 200 numbers that we suspected may be used by the Clients PBX using a Modem Scanning and Penetration Tool called TeleSweep. The program is freely available on the Internet. The process lasted two days. Modems were scanned in groups of 30 phone numbers to prevent detection. We were able to identify one active modem.

Modem Discovery

The following screen shot provides the discovery process.



War Dialing Penetration Attempt



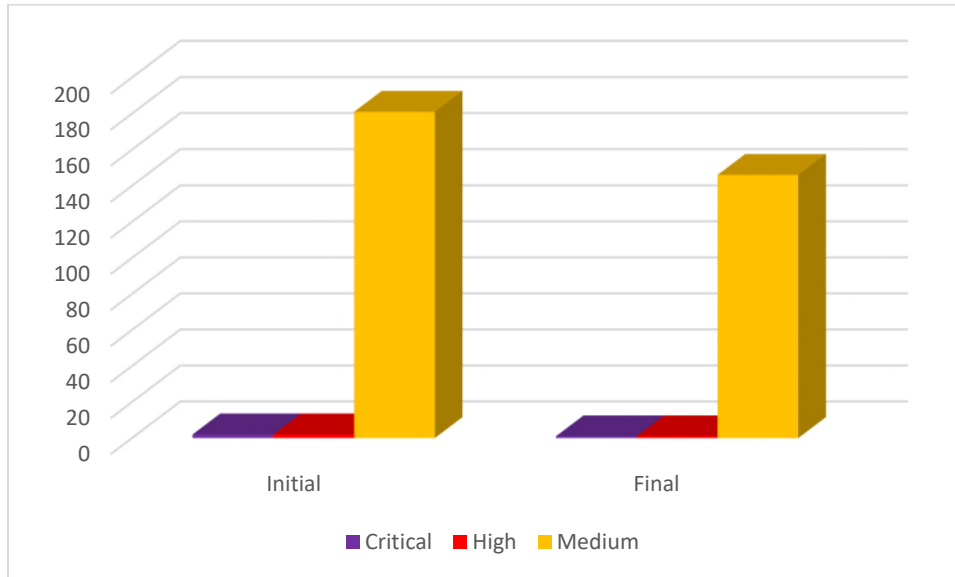
The penetration attempt failed.

CONFIDENTIAL

External Retest

We retested the external network to gauge whether changes had been made since the last retest. Following retest some vulnerabilities remain but over we saw of 100 Percent deduction for Critical and High Vulnerabilities found and a 24 Percent Drop in Medium vulnerability found. The final spread sheet is included in the file folder for the deliverable. The following depicts changes made.

Overall Severity



Risk	Initial	Final	Reduction
Critical	2	1	100%
High	2	1	100%
Medium	181	146	24%

Addendum A- Work Effort Matrix

Priority	Vulnerability	Mitigation	Risk Rating
1	Internal Systems susceptible to vulnerabilities	Update Software or remediate as required. Protect all critical resources from end users.	High
2	External System Potential Vulnerabilities	Update code and configuration for Cisco Routers. Do not use Telnet or HTTPS if possible	High
3	Users Susceptible to Phishing Attacks	Although, only one user provided their username and password, that is all it takes for system compromise. Develop a Training Regimen to educate users on phishing awareness and defense	High
4	Wi-Fi Authentication	Although, we were unable to brute force the captured password, a shared key can be compromised easily by end users. A stronger authentication method such as RADIUS authentication would provide a more robust and secure validation method.	High

Addendum B - External/Internal Vulnerability Testing Detail

Electronically sent and attached

CONFIDENTIAL

State of West Virginia / Lottery Commission
Network Penetration Testing and Cybersecurity Assessments
Advizex Response to CRFQ 0705 LOT2400000009



Bid Due Date: 3/27/2024
Bid Due Time: 1:30pm
Version: 1.2

Presented to:

Brandon L Barr
Buyer
Department of Administration
Purchasing Division
2019 Washington Street East
Charleston, WV 25305
304-558-2652 [office]
brandon.l.barr@wv.gov [e-Mail]

Submitted by:

Mika Munoz
Account Executive
Advizex Technologies, LLC
680 Andersen Drive
Foster Plaza 10, 2nd Floor
Pittsburgh, PA 15220
304-615-3301 [mobile]
412-446-8300 [office]
412-937-0537 [fax]
mmunoz@advizex.com

Advizex Technologies, LLC (Advizex) has prepared this document solely for the State of West Virginia Lottery Commission (WV Lottery).

Information contained within this document is intellectual property and copyright of Advizex.

Distribution or reproduction of this document is restricted to WV Lottery.

Distribution or reproduction of this document outside of WV Lottery requires consent from Advizex.

Advizex



March 27, 2024

Brandon L Barr
Buyer
Department of Administration
Purchasing Division
2019 Washington Street East
Charleston, WV 25305

RE: State of West Virginia / Lottery Commission
Network Penetration Testing and Cybersecurity Assessments Advizex
Response to CRFQ 0705 LOT2400000005

Mr. Barr:

On behalf of Advizex Technologies, LLC (Advizex) I am pleased to submit our response to the **State of West Virginia / Lottery Commission's (WV Lottery) Network Penetration Testing and Cybersecurity Assessments as part of CRFQ 0705 LOT2400000009.**

I, Mika Munoz, and your Account Executive and can always be reached at:

Mika Munoz	680 Andersen Drive, Foster Plaza 10
Account Executive	2nd Floor, Pittsburgh, PA 15220
304-615-3301 [mobile]	216-901-1447 [fax]
mmunoz@advizex.com	

Advizex is an industry-leading information technology provider, of over 49 years, which combines the technical expertise of over 175 technical consultants holding over 1,000 certifications and leverages solutions from the industry's top technology partners.

Following an acquisition by Fulcrum Technology Partners, Advizex is now a keystone organization and business unit with international presence that provides IT products, Professional Services, Managed Services, and Security Consulting in Canada, Europe, and the United States.

In addition, Advizex holds state-term contracts with over 17 US states and conducts business with over 125 agencies in those states; successful business relationships of over 20 years.

Advizex prides itself in its full-service capabilities. specializes in **consulting, architecting, deploying, Managed Services, Security Consulting, and growth planning** of advanced custom solutions across multiple practices, including:

ADAPTIVE INFRASTRUCTURE	INTELLIGENT OPERATIONS	NETWORK & SECURITY	CLOUD MANAGED SERVICES
HCI/CI	Cloud Infrastructure (VMC and Azure*)	Networking	Public Cloud
SDDC	Collaboration (Microsoft 365/Teams)	Zero Trust	Database Management
Data Protection	Identity & Access Management (IDM/SSO)	Next-Gen Firewall	HCI/CI & SDDC
Storage	Automation & Orchestration	Secure Remote Access	Virtualization
Digital Workspace	Multi-Cloud Management	Threat Detection & Response (XDR)	Network
Database	IT Service Management	Business Continuity Planning	Servers/OS
	IT Operations Management	Disaster Recovery	Backup, Storage & Disaster Recovery
		Security Advisory Services	Monitoring as a Service (MaaS)
			

I Thank you for this opportunity and look forward to future reviews of this proposal with your technical teams.

Sincerely,



Mika Munoz
Account Executive
Advizex Technologies, LLC

Table of Contents

1. Cover Pages	5
2. Terms and Conditions, Designated Contact, and Contract Contact.....	6
3. Qualifications Requirements.....	7
3.1 Years In Business	7
3.2 Client References.....	8
3.3 Vendor Accreditations.....	11
3.4 Cybersecurity Certifications.....	14
3.5 Industry Standards Compliance.....	15
3.6 Background Checks.....	16
3.7 Non-Disclosure Agreement (NDA).....	16
4. Mandatory Requirements.....	17
4.1 External Network Penetration Testing	17
4.2 Website Penetration Testing.....	22
4.3. Internal/Client-Side Network Penetration Testing.....	28
4.4. Wireless Penetration Testing.....	32
5. Engagement Approach.....	37
5.1 Engagement Summary	37
5.2 Cyber Security Testing Project Scope	38
5.2.1 External Penetration Testing.....	38
5.2.2 Web Application Penetration Testing	38
5.2.3 Internal Vulnerability Assessment.....	38
5.2.4 Wi-Fi Penetration Testing	38
5.2.5 Result Analysis and Deliverable Creation	39
5.3 External Penetration Testing	39
5.3.1 External Reconnaissance/Enumeration Phase	39
5.3.2 External Vulnerability Scanning Phase.....	39
5.3.3 External Penetration Exploitation Phase.....	40
5.4 Web Application Penetration Testing.....	41
5.4.1 Web Application Penetration Testing Methodology	41
5.4.2 Web Application Enumeration Phase.....	42
5.4.3 Web Application Vulnerability Scanning	43
5.4.4 Web App Exploitation	44
5.4.5 Web Application Privilege Escalation (Post Exploitation).....	44
5.5 Internal Vulnerability Scanning	45
5.5.1 Internal Enumeration Phase.....	45
5.5.2 Internal Vulnerability Scanning Phase.....	46
5.6 Wi-Fi Penetration Testing	47
5.7 Reporting	48
5.7.1 Executive Summary Report	49
5.7.2 Detailed Technical Report.....	49
5.7.3 Findings Presentation	49
6. Pricing Page (Exhibit A)	50
Appendix A. Certificate of Insurance.....	51
Appendix B. Acknowledgement of Addendums	52
Appendix C. Non-Disclosure Agreement (Exhibit B)	53
Appendix D. Redacted Sample Cybersecurity Report.....	54



1. COVER PAGES



Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

State of West Virginia
 Centralized Request for Quote
 Service - Prof

Proc Folder: 1369290	Reason for Modification:
Doc Description: Network Penetration Testing and Cybersecurity Assessments	
Proc Type: Central Master Agreement	

Date Issued	Solicitation Closes	Solicitation No	Version
2024-03-08	2024-03-28 13:30	CRFQ 0705 LOT2400000009	1

BID RECEIVING LOCATION

BID CLERK
 DEPARTMENT OF ADMINISTRATION
 PURCHASING DIVISION
 2019 WASHINGTON ST E
 CHARLESTON WV 25305
 US

VENDOR

Vendor Customer Code: 000000181088
Vendor Name : Advizex Technologies, LLC
Address : 680 Andersen Drive, Foster Plaza 10, 2nd Floor
Street :
City : Pittsburgh
State : PA **Country :** USA **Zip :** 15220
Principal Contact : Mika Munoz
Vendor Contact Phone: 304-615-3301 **Extension:**

FOR INFORMATION CONTACT THE BUYER
 Brandon L Barr
 304-558-2652
 brandon.l.barr@wv.gov

Scott Hess / Proposal Desk Manager

Vendor Signature X  **FEIN#** 37-1504931 **DATE** 3/27/2024

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Lottery to establish a contract for Network Penetration Testing and Cybersecurity Assessments per the terms and conditions, Exhibit A Pricing Page and Exhibit B NDA, and specifications as attached.

INVOICE TO		SHIP TO	
LOTTERY PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON US	WV	CHARLESTON US	WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	External Network Penetration Testing		SEE PRICING PAGE		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

INVOICE TO		SHIP TO	
LOTTERY PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON US	WV	CHARLESTON US	WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Website Penetration Testing		SEE PRICING PAGE		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page

INVOICE TO			SHIP TO		
LOTTERY PO BOX 2067			LOTTERY 900 PENNSYLVANIA AVE		
CHARLESTON	WV	US	CHARLESTON	WV	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Internal/Client-Side Network Penetration Testing		SEE PRICING PAGE		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:
See Attached Specifications and Exhibit - A Pricing Page

INVOICE TO			SHIP TO		
LOTTERY PO BOX 2067			LOTTERY 900 PENNSYLVANIA AVE		
CHARLESTON	WV	US	CHARLESTON	WV	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Wireless Penetration Testing		SEE PRICING PAGE		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description:
See Attached Specifications and Exhibit - A Pricing Page

SCHEDULE OF EVENTS

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions due by 10:00am ET	2024-03-21



2. TERMS AND CONDITIONS, DESIGNATED CONTACT, AND CONTRACT CONTACT

REQUEST FOR QUOTATION
West Virginia Lottery
Network Penetration Testing and Cybersecurity Assessments

10.2. The following remedies shall be available to Agency upon default.

10.2.1. Immediate cancellation of the Contract.

10.2.2. Immediate cancellation of one or more release orders issued under this Contract.

10.2.3. Any other remedies available in law or equity.

11. MISCELLANEOUS:

11.1. Contract Manager: During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager: Jennifer Sprague
Telephone Number: 440-225-9445
Fax Number: 216-901-1447
Email Address: jsprague@advizex.com

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Mika Munoz

(Address) 680 Andersen Drive, Foster Plaza 10, 2nd Floor, Pittsburgh, PA 15220

(Phone Number) / (Fax Number) 304-615-3301 / 216-901-1818

(email address) mmunoz@advizex.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Advizex Technologies, LLC

(Company) 

(Signature of Authorized Representative)

Scott Hess / Proposal Desk Manager

(Printed Name and Title of Authorized Representative) (Date) 3/27/23

440-622-1089 / 216-901-1447

(Phone Number) (Fax Number)

shess@advizex.com

(Email Address)

3. QUALIFICATIONS REQUIREMENTS

3.1 YEARS IN BUSINESS

3.1	<p>Vendor must be in business at a minimum fifteen (15) years performing and delivering information technology cybersecurity assessments.</p>
	<p>Advizex Response: As stated previously, Advizex is an industry-leading information technology provider, of over 49 years, that combines the technical expertise of over 175 technical consultants holding over 1,000 certifications and leverages solutions from the industry's top technology partners.</p> <p>Following an acquisition by Fulcrum Technology Partners, Advizex is now a keystone organization and business unit with international presence that provides IT products, Professional Services, Managed Services, and Security Consulting in Canada, Europe, and the United States.</p> <p>In addition, Advizex holds state-term contracts with over 17 US states and conducts business with over 125 agencies in those states; successful business relationships of over 20 years.</p> <p>Our Security Practice business units have provided over 20 years of Security Consulting with experienced staff members from the secular industries and the military.</p>

3.1.1	<p>Vendor should provide with their bid, a general company overview that must include information regarding the number of years of qualification, experience, training, relevant professional education for each individual that will be assigned to the project team, professional services offered, and number of dedicated security staff resources.</p>
	<p>Advizex Response: Our Security Practice commonly includes, but is not limited to, performing services such as:</p> <ul style="list-style-type: none"> • CISO Contract Chief Information Security Officer Consulting Services • Vulnerability Testing • Penetration Testing • Web Application Penetration Testing • Risk Assessments based on Standards and Laws

	<ul style="list-style-type: none"> • IT Control Policy Review and Authoring • Employee Training and Awareness • Social Engineering (Malicious Phone Calls, Malicious • E-mail Phishing, USB Rubber Duck Drops, Employee • Impersonation, and WIFI Pineapple Tests among other services • Employee Standard and Law Compliance Interviews • Frameworks Leveraged for Assessments (NIST Cybersecurity Special Publications, SANS CWE 25, OWASP, OSTMM, CERT) <p>We maintain a particularly strong presence in working with clients who need to comply with specific standards and laws that include:</p> <ul style="list-style-type: none"> • HIPAA/ARRA HITECH ACT • NY Shield Law • MASS CMR 201 17.00 • Other State Privacy Laws • ISO 27001 • ISO 27002 • NIST SP800-53 Rev 4 • NIST SP800-171 • FISMA • FIPS • GDPR • SOX
--	---

3.2 CLIENT REFERENCES

	<p>Vendor should provide with their bid, a minimum of three (3) references for projects of like size and scope of the assessments to be performed for the Lottery.</p> <p>3.2.1 References shall include contact information and brief details of the services performed for each reference.</p>
<p>3.2 and 3.2.1</p>	<p>Advizex Response:</p> <p>Advizex signs Non-Disclosure agreements with each client that limits the dissemination of contact information, client information, and security data. We have included 4 approved references and ask that you work closely with Mika Munoz, your Account Executive, to facilitate additional reference discussions.</p> <p>A sample of past engagements similar to this one includes the following:</p> <ul style="list-style-type: none"> • DGA Security Systems – New York City, NY

- NCH Healthcare Systems - Lancaster, NH
- TRC Engineering/Avangrid – Augusta, ME
- Ulster Savings Bank – Kingston, NY
- Sadara/Dow Chemical - Houston TX
- Massachusetts State Lottery- Dorchester, MA
- Delaware Electric Cooperative – Greenwood, DE
- New York Chiropractic College – Seneca Falls, NY
- Albany College of Pharmacy– Albany NY
- Massachusetts School Building Authority - Boston, MA
- IUOE Health Services – Chicago, IL
- Withlacoochee Electric – Dade City, FL
- Copley Hospital, Morrisville, VT
- Town of Lexington – Lexington, MA
- Narragansett Bay Water Commission – Providence, RI

Sample references include:

Mass State Lottery

Bob Moran
Chief Information Security Officer
150 Mount Vernon Street
Dorchester, MA 02125-3573
(p) 781.849/5555
Project Time Frame: May/June 2019
Project Description:

Advizex conducted a phased Cyber Security Evaluation and Test for the Massachusetts State Lottery Commission (MSLC). Advizex was provided with the minimum information by Client. The test was conducted as a Black Box Test. The testing followed the guidelines and procedures established by GLBA, FFIEC, NIST SP 800 IT Security Standards and the Open-Source Security Testing Methodology Manual (OSSTMM).

The Cyber Security Testing and Evaluation involved an active analysis of internal and external information systems and web applications for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware, software flaws, and operational weaknesses in process or technical countermeasures. This testing was carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities.

Security issues uncovered through the Cyber Security Testing and Evaluation were presented to the Client. These effective vulnerability and penetration tests coupled this automated and manual interpretation of information provided an accurate assessment of the potential impacts to the organization and outlined a range of technical and procedural countermeasures to reduce risks. Our Security Testing Methodology always uses a phased approach. This requires several different types of tests. Each phase provides valuable information which ultimately leads to exploitation or no exploitation. All Testing was performed during normal business hours of 9am to 5pm Eastern Standard Time. Testing lasted approximately six weeks from start to final deliverable. All Services were delivered on time and on budget. End Customer was extremely satisfied with Quality and Technical Support

Fresenius Kidney Care

Duane Dumont
Vice President, Information Technology and Security Officer
350 Merrimack St.
Lawrence, MA 01843
Tel: (978) 687-4700
Project Time Frame: October 2009 – Present

Project Description:

Fresenius Kidney Care formally known as NxStage Medical hired Advizex as a Cyber Security Consultant to assist with maintaining annual compliance to HIPAA and NIST SP800-53 Rev. 5. Testing follows the guidelines and procedures established by Laws, Standards, and the Open-Source Security Testing Methodology Manual (OSSTMM) and the SANS Security Institute.

The testing methodology uses HIPAA, and NIST SP800-53 Rev.5 requirements for Cyber Security Compliance. Fresenius contracts Advizex on a yearly basis to perform quarterly testing services of the Kidney Care Dialysis Center Networks and Server Infrastructure:

- Internal Vulnerability Assessments
- Internal Penetration Testing
- External Vulnerability Assessments
- External Penetration Testing

All Testing is performed in White Box mode so that everyone in IT is aware of the testing. Once the testing is completed Advizex meets with NxStage IT to review

	<p>and clarify all testing results. Advizex provides detailed reporting as well as a Work Effort Remediation Matrix to identify what vulnerabilities in terms of criticality and exploits needing immediate remediated to maintain a high level of Cyber Security.</p> <p>About NxStage – NxStage has a history rooted deeply in technology and research. Our inventions and groundbreaking technology are helping to improve the lives of kidney patients across the globe and we are just getting started.</p> <p><u>Massachusetts Port Authority / Mass State Lottery Commission</u> Pat Barry - CISO Massachusetts Port Authority / Mass State Lottery 60 Columbian Street Braintree, MA 02184 pbarry@masslottery.com</p> <p><u>Constellium Rolled Products</u> Greg Hutton IT Director Constellium Rolled Products 859 Century Rd, Ravenswood, WV 26164 304-273-6872 greg.hutton@constellium.com</p>
--	---

3.3 VENDOR ACCREDITATIONS

<p>3.3</p>	<p>Vendor should provide with their bid, documentation of current accreditations held by the project team assigned to Lottery cybersecurity assessments.</p>
	<p>Advizex Response: Advizex has provided Cyber Security Consulting for many years and have a focus on assisting companies with their Cyber Security Compliance needs by performing services such as:</p> <ul style="list-style-type: none"> • CISO Contract Chief Information Security Officer Consulting Services • Vulnerability Testing • Penetration Testing • Web Application Penetration Testing • Risk Assessments based on Standards and Laws • IT Control Policy Review and Authoring

	<ul style="list-style-type: none"> • Employee Training and Awareness • Social Engineering (Malicious Phone Calls, Malicious • E-mail Phishing, USB Rubber Duck Drops, Employee • Impersonation, and WIFI Pineapple Tests among other services • Employee Standard and Law Compliance Interviews • Frameworks Leveraged for Assessments (NIST Cybersecurity Specia • Publications, SANS CWE 25, OWASP, OSTMM, CERT) <p>In addition, we have a particularly strong presence in working with Clients who need to comply with Standards and Laws. Such as:</p> <ul style="list-style-type: none"> • HIPAA/ARRA HITECH ACT • NY Shield Law • MASS CMR 201 17.00 • Other State Privacy Laws • ISO 27001 • ISO 27002 • NIST SP800-53 Rev 4 • NIST SP800-171 • FISMA • FIPS • GDPR • SOX <p>Please refer to Section 3.4 of this submission for additional information.</p>
--	---

	<p>Documentation shall consist of an overview of the project team security assessments, resumes and documentation of certifications namely CISSP or SAN should be provided as stated below in section 3.4.</p>
<p>3.3.1</p>	<p>Advizex Response: Our primary resource assigned to this engagement is:</p> <p>Jeffrey W. Jones</p> <p>Cyber Security Architect and Ethical Hacker, 2003-Present Cyber Security Architect and Ethical Hacker that is responsible for all day-to-day operations, technical consulting, and security design for major customers throughout the United States. Responsible for Security Program Design, Security Risk Analysis and Assessment and Cyber Security Testing to include</p>

Penetration Testing, Vulnerability Testing, Social Engineering, Phishing, Wi-Fi Exploitations, Password Cracking, Man-in-the Middle Attacks and Web Application Hacking

Education

Webster University 1989

Bachelor's Degree Purdue University 1985

Accreditations/Certifications

- ISC2 Certified Information Systems Security Professional
- EC-Council Certified Ethical Hacker Cisco Certified Network Associate
Cisco Certified Network Design Professional
- Juniper Certified Internet Associate

Hacker Tool Skill Set

- AirCrack-NG Wi-Fi Cracking Suite Commix Command Injection Suite
HTTRack
- IKE-Scan
- Kali Linux Software Suite Metasploit Armitage
- Metasploit Framework Command Line Interface
- Nessus Professional Feed Vulnerability Scanning Software
- NMAP Port Scanning and Enumeration Software
- OWASP Zed Attack Proxy (ZAP)
- PSK-Crack
- SQLMap
- WPScan

Programming Languages

- Python
- Debian Linux
- Regex
- Perl
- C++
- Java

Expert Networking Knowledge of:

- Cisco - Wi-Fi, Routers, Switches, VoIP, UTM Firewall
- Juniper - Routers Switches
- Fortinet - UTM Firewalls, VPNHP Enterprise - Switching, HP Logger, ArcSight,
Wi-Fi
- Extreme Switching

	<ul style="list-style-type: none"> • VMware - vSphere, ESX, Workstation Brocade - • EMC – VNX Storage • RSA - SecureID, Data Loss Prevent Symantec Enterprise End Point <p>Professional History</p> <p>Captain United States Marine Corps 1981-1997 (Retired Reserves 1997) Retired Marine Corps Captain from the Marine Corps Reserve commissioned as a Marine Corps Officer in 1985 after graduation from College and began active-duty service immediately. Serving in a variety of security and communications focused roles with the 1st Marine Division, the 5th Marine Expeditionary Brigade, the 1st Force Service Support Group and the 1st Marine Expeditionary Force, 4th Force Service Support Group, GSM Company and the 25th Marine Infantry Regiment. Team Member for initial IP Based Network for US Marine Corps.</p> <p>Senior Systems Engineer, Fore Systems/Ericsson 1997-2002 Systems Engineer Core Asynchronous Mode Transport Data Switches at Ericsson (formerly FORE Systems) at the individual, regional and national levels, the projects total value of Systems Designed</p> <p>Senior Systems Engineer, Anixter Corporation 1991-1997 Senior Systems Engineer at Anixter, responsible for all data communications and security engineer to over 100 large corporations in the Boston Area. Provided Design, Architecture and Installation for Cisco, HP, Fore Systems</p>
--	--

3.4 CYBERSECURITY CERTIFICATIONS

3.4	<p>Vendor staff performing information technology cybersecurity assessments must hold a current certification from a source of accreditation and should provide the certification credentials with their bid response. Examples of certifications shall include:</p> <ul style="list-style-type: none"> 3.4.1 Certified Information Systems Security Professional (CISSP) 3.4.2 GIAC Penetration Tester (GPEN) 3.4.3 Offensive Security Certified Professional (OSCP) 3.4.4 Certified Ethical Hacker (CEH) 3.4.5 Certified Penetration Testing Engineer (CPTe)
-----	---

	<p>3.4.6 Certified Expert Penetration Tester (CEPT) 3.4.7 Certified Red Team Operations Professional (CRTOP) 3.4.8 Certified Security Analyst (ECSA) 3.4.9 Certified Professional Penetration Tester (CPPT) 3.4.10 Certified Wireless Security Professional (CWSP) 3.4.11 Certified Mobile and Web Application Penetration Tester (CMWAPT)</p>
	<p>Advizex Response: The staff associated with this engagement hold the following certifications:</p> <ul style="list-style-type: none"> • Certified Information Systems Security Professional (CISSP) • EC-Council Certified Pen Testing Professional (CPENT) exam scheduled • Certified Ethical Hacker (CEH) • Certified Information Security Manager (CISM) 2024 renewal in process • Additional Military certifications

3.5 INDUSTRY STANDARDS COMPLIANCE

3.5a	<p>Vendor must comply with industry standards and compliance, namely the Penetration Testing Execution Standard (PTES), and follow a documented methodology to ensure consistent and thorough testing. 3.5.1 Vendor should provide with their bid, documentation of the industry standard and testing methodology leveraged and evidence of compliance.</p>
	<p>Advizex Response: Advizex adheres strictly to the Penetration Testing Execution Standard (PTES) for all penetration testing procedures. PTES is a comprehensive and widely recognized framework that guides our process from the initial stages of engagement to post-engagement recommendations and follow-up. Our adherence to PTES ensures that our testing is consistent, thorough, and in compliance with industry standards. We are compliant with NIST Sp 800-155, at minimum,</p>

3.5b	<p>Vendor should provide with their bid, documentation of the industry standard and testing methodology leveraged and evidence of compliance.</p>
	<p>Advizex Response: As part of our commitment to transparency and compliance, we are pleased to provide documentation outlining our use of the PTES methodology in our penetration testing procedures. This includes:</p>

	<p>Pre-engagement Interactions: We define the rules of engagement and establish clear communication channels.</p> <p>Intelligence Gathering: We collect as much information as possible about the target before the test.</p> <p>Threat Modeling: We identify potential threats to the system.</p> <p>Vulnerability Analysis: We identify potential points of exploit.</p> <p>Exploitation: We attempt to compromise the system.</p> <p>Post Exploitation: We identify what can be accomplished with the level of access obtained.</p> <p>Reporting: We provide a detailed report of our findings, including identified vulnerabilities and recommended remediation strategies.</p> <p>We regularly review and update our procedures to ensure continued compliance with the PTES and any updates to the standard.</p>
--	--

3.6 BACKGROUND CHECKS

3.6	<p>Prior to award and upon request the Vendor must provide names, addresses and fingerprint information for a law enforcement background check for any Vendor staff working on Lottery project team.</p>
	<p>Advizex Response: Advizex will comply and provide the requested information when requested by WV Lottery.</p>

3.7 NON-DISCLOSURE AGREEMENT (NDA)

3.7	<p>Prior to award both parties, the Vendor and Lottery must sign a mutual Non-Disclosure Agreement (NDA), attached as Exhibit —B, to ensure the confidentiality of the information exposed and proprietary tools and techniques used during these assessments.</p>
	<p>Advizex Response: We agree to this requirement and have attached a signed copy of your Non-Disclosure Agreement. The following file has been included with our submission:</p> <ul style="list-style-type: none"> • CRFQ LOT24-09 - Exhibit B NDA v1_1.pdf

4. MANDATORY REQUIREMENTS

4.1 EXTERNAL NETWORK PENETRATION TESTING

4.1.1	External Network Penetration Testing may be performed remotely.
	Advizex Response: Advizex acknowledges.

4.1.2	Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.
	Advizex Response: Advizex acknowledges.

4.1.3	Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.
	Advizex Response: Advizex acknowledges.

4.1.3.1 4.1.3.1.1 4.1.3.1.2 4.1.3.1.3 4.1.3.1.4 4.1.3.1.5 4.1.3.1.6	Reconnaissance should include:
	<ul style="list-style-type: none"> • Perform WHOIS, ARIN, and DNS (public server) lookups • OSINT - Public Searches/Dorks
	<ul style="list-style-type: none"> • Build custom password lists
	<ul style="list-style-type: none"> • DNS lookups (entities server)
	<ul style="list-style-type: none"> • Gather information from entities network resources
	<ul style="list-style-type: none"> • Analyze metadata
	Advizex Response:
	Advizex acknowledges. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.

<p>4.1.3.2 4.1.3.2.1 4.1.3.2.2 4.1.3.2.3</p>	<p>Mapping should include:</p> <ul style="list-style-type: none"> • Network Discovery (ICMP sweeps, traceroutes, bypass firewall restrictions, etc.) • Port/Protocol Scanning (Scan for accepted IP protocols, open TCP/UDP ports) • OS/Version Scanning (Identify underlying OS and software and their versions)
	<p>Advizex Response: Advizex acknowledges. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.</p>

<p>4.1.3.3 4.1.3.3.1 4.1.3.3.2 4.1.3.3.3 4.1.3.4.1 4.1.3.4.2 4.1.3.4.3</p>	<p>Discovery should include:</p> <ul style="list-style-type: none"> • Vulnerability Scanning (Identify vulnerabilities. Open source tools as well as Commercial: Nessus – network vulnerability scanner, Burp Suite – web application scanner) • Enumerating Network Services (Connect and interact with services to disclose information, gain access, identify misconfigurations, etc.) • Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.) <p>4.1.3.4. Exploitation should include:</p> <ul style="list-style-type: none"> • Brute Force Logins (Using discovered username/email addresses, gain additional access through brute force) • Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information) • Post-Exploitation and Pivot (Pillage the system to disclose information and additional vulnerabilities. Repeat the penetration test steps to attempt to gain privileged access. Use the compromised systems as a pivot point to attack other systems that are in scope).
	<p>Advizex Response: Advizex acknowledges. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.</p>

4.1.4	Must identify exploitable vulnerabilities and demonstrate organizational impact.
	Advizex Response: Advizex acknowledges. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables. Most specifically, the “Goals” subsection for each phase of the engagement.

4.1.5	Denial of service (DoS) attacks are prohibited for External Network Penetration Testing services.
	Advizex Response: Advizex Acknowledges and Agrees. “Denial of service (DoS) attacks will not be performed during any portion of the External Network Penetration Test.”

4.1.6	A social engineering exercise must be included. This will consist of a single phishing email scenario targeting approximately 200 active Lottery staff. The content must be designed to maximize successful phishing, and the email content and target addresses must be verified and approved by the Lottery.
	Advizex Response: Advizex acknowledges. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.

4.1.7	Heavy load brute force or automated attacks will only be performed with prior Lottery approval.
	Advizex Response: Advizex Complies and Agrees. “Heavy load brute force or automated attacks will only be performed with prior Lottery approval and Denial of service (DoS) attacks are never used.

4.1.8	Must notify Lottery of any portion or portions of the assessment resulting in service disruption.
	Advizex Response: Yes, Advizex will notify the lottery of any portion or portions of the assessment resulting in service disruption.

4.1.9	The Lottery must be notified immediately upon identifying any security vulnerability threatening critical business processes or IT services.
	Advizex Response: Advizex Acknowledges. “The WV Lottery will be notified immediately upon identifying any security vulnerability threatening critical business processes or IT services.”

4.1.10	Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.
	Advizex Response: Advizex acknowledges and agrees.

4.1.10.1	The vendor shall provide a sample of the executive summary report with their bid response.
	Advizex Response: Advizex has included a redacted technical report with this submission for your review. The file name is: <ul style="list-style-type: none"> • Sample Redacted Client Cyber Security Testing v1.0 - Advizex v1_0.pdf

4.1.10.2	The report must be submitted to the Lottery electronically for review.
	Advizex Response: Advizex acknowledges.

4.1.11	Upon conclusion of the assessment the Vendor must provide a Technical Report. This report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.
	Advizex Response: Advizex acknowledges.

4.1.12 4.1.12.1 4.1.12.2	Reports must include specific details for each vulnerability found, including:
	<ul style="list-style-type: none"> • How the vulnerability was discovered • The potential impact of its exploitation. • Recommendations for remediation. • Vulnerability references
4.1.12.3 4.1.12.4	Advizex Response: Advizex acknowledges. Please refer to each “Reporting” Section in Section 5 of this submission.

4.1.12.5	The vendor shall provide a sample of the technical report with their bid response.
	Advizex Response: Advizex has included a redacted technical report with this submission for your review. The file name is: <ul style="list-style-type: none"> • Sample Redacted Client Cyber Security Testing v1.0 - Advizex v1_0.pdf

4.1.12.6	The report must be submitted to the Lottery electronically for review.
	Advizex Response: Advizex acknowledges.

4.1.13	Upon conclusion of the assessment, the Vendor must provide a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.
	Advizex Response: Advizex acknowledges and agrees.

4.1.13.1	The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.
	Advizex Response: Advizex acknowledges.

4.2 WEBSITE PENETRATION TESTING

4.2.1	Website Penetration Testing may be performed remotely.
	Advizex Response: Advizex acknowledges.

4.2.2	Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.
	Advizex Response: Advizex acknowledges.

4.2.3	The successful vendor must determine static and dynamic page counts.
	Advizex Response: Advizex acknowledges. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.

4.2.4	Any environment, such as production, development, quality assurance, etc., may be tested. Each environment will be assessed separately.
	Advizex Response: Advizex acknowledges and agrees.

4.2.5	Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.
	Advizex Response: Advizex acknowledges.

4.2.5.1 4.2.5.1.1 4.2.5.1.2 4.2.5.1.3 4.2.5.1.4	Reconnaissance should include: <ul style="list-style-type: none"> • Perform WHOIS, ARIN, and DNS (public server) lookups • OSINT - Public Searches/Dorks • Build custom password lists • DNS lookups (entities server) • Gather information from entities network resources • Analyze metadata
4.2.5.1.5 4.2.5.1.6	Advizex Response: Advizex acknowledges. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.

<p>4.2.5.2 4.2.5.2.1 4.2.5.2.2 4.2.5.2.3 4.2.5.2.4 4.2.5.2.5 4.2.5.2.6 4.2.5.2.7 4.2.5.2.8</p>	<p>Mapping should include:</p> <ul style="list-style-type: none"> • SSL/TLS Analysis (Identify accepted SSL/TLS ciphers) • Virtual Hosting & Load Balancer Analysis • Software Configuration Discovery (Identify HTTP version, web services, scripting languages, third-party web applications, etc.) • HTTP Options Discovery (Identify accepted HTTP methods) • Web Application Spidering (gather/follow all links) 4.2.5.2.6. Directory Browsing (Identify web directory listings, brute force common web directory names) • Web Application Flow (Identify the business logic, flow, organization, and functionalities of the app) • Session Analysis (Identify locations where session cookies are set and analyze predictability)
	<p>Advizex Response: Advizex acknowledges. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.</p>

<p>4.2.5.3 4.2.5.3.1 4.2.5.3.2 4.2.5.3.3 4.2.5.3.4</p>	<p>Discovery should include:</p> <ul style="list-style-type: none"> • Vulnerability Scanning (Identify vulnerabilities. Open source tools as well as Commercial: Nessus – network vulnerability scanner, Burp Suite – web application scanner) • Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.) • Identify Web Application Specific/Web Service Specific Vulnerabilities (Command/XML/XXE/SQL Injection, File Inclusion, Directory Traversal, File Upload, XSS, CSRF, etc.) • Identify Authentication/Authorization Issues/Bypasses (Weak access control, weak password policy, session management, etc.)
	<p>Advizex Response: Advizex acknowledges. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.</p>

<p>4.2.5.4 4.2.5.4.1 4.2.5.4.2 4.2.5.4.3</p>	<p>Exploitation should include:</p> <ul style="list-style-type: none"> • Brute Force Logins (Using discovered username/email addresses, gain additional access through brute force) • Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information) • Post-Exploitation and Pivot (Pillage the system to disclose information and additional vulnerabilities. Repeat the pentest steps to attempt to gain privileged access. Use the compromised systems as a pivot point to attack other systems that are in scope).
	<p>Advizex Response: Advizex acknowledges. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.</p>

<p>4.2.6</p>	<p>Must provide identification of prioritized remediation needs, requirements, and associated risks.</p> <p>Advizex Response: Advizex acknowledges and agrees.</p>
--------------	--

<p>4.2.7</p>	<p>Testing shall determine if website vulnerabilities exist by testing each website, including server operating systems, application platforms, and databases.</p> <p>Advizex Response: Advizex acknowledges and agrees. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.</p>
--------------	--

<p>4.2.8</p>	<p>Denial of Service (DoS) attacks are required for Website Penetration Testing and require notification to the Lottery and Lottery approval before the attack commences.</p> <p>Advizex Response: Advizex acknowledges. If for some reason, Denial of Service (DoS) attacks are required for Website Penetration Testing. Advizex will notify the Lottery and obtain Lottery approval before the attack commences.”</p>
--------------	--

4.2.9	Heavy load brute force or automated attacks will only be performed with prior Lottery approval.
	Advizex Response: Advizex acknowledges. "If Heavy load brute force or automated attacks will only be performed with prior Lottery approval".

4.2.10	Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.
	Advizex Response: Advizex acknowledges.

4.2.10.1	The vendor shall provide a sample of the technical report with their bid response.
	Advizex Response: Advizex has included a redacted technical report with this submission for your review. The file name is: <ul style="list-style-type: none"> • Sample Redacted Client Cyber Security Testing v1.0 - Advizex v1_0.pdf

4.2.10.2	The report must be submitted to the Lottery electronically for review.
	Advizex Response: Advizex acknowledges.

4.2.11	Upon conclusion of the assessment, the Vendor must provide a Technical Report. This report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.
	Advizex Response: Advizex acknowledges.

<p>4.2.12 4.2.12.1 4.2.12.2 4.2.12.3 4.2.12.4</p>	<p>Reports must include specific details for each vulnerability found, including:</p> <ul style="list-style-type: none"> • How the vulnerability was discovered • The potential impact of its exploitation. • Recommendations for remediation. • Vulnerability references <p>Advizex Response: Advizex acknowledges.</p>
---	---

<p>4.2.12.5</p>	<p>The vendor shall provide a sample of the technical report with their bid response.</p> <p>Advizex Response: Advizex has included a redacted technical report with this submission for your review. The file name is:</p> <ul style="list-style-type: none"> • Sample Redacted Client Cyber Security Testing v1.0 - Advizex v1_0.pdf
-----------------	--

<p>4.2.12.6</p>	<p>The report must be submitted to the Lottery electronically for review.</p> <p>Advizex Response: Advizex acknowledges.</p>
-----------------	---

<p>4.2.13 4.2.13.1</p>	<p>Upon conclusion of the assessment, the Vendor must provide a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.</p> <p>The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project..</p> <p>Advizex Response: Advizex acknowledges.</p>
----------------------------	--

4.3. INTERNAL/CLIENT-SIDE NETWORK PENETRATION TESTING

4.3.1	Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. Assessing locations remotely or from one central location is prohibited.
	Advizex Response: Advizex acknowledges.

4.3.2	Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.
	Advizex Response: Advizex acknowledges.

4.3.3	Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.
	Advizex Response: Advizex acknowledges.

4.3.3.1 4.3.3.1.1 4.3.3.1.2 4.3.3.1.3 4.3.3.1.4 4.3.3.2.1 4.3.3.2.2	Reconnaissance should include: <ul style="list-style-type: none"> • Identify software versions along with potentially useful software configurations or settings • Identify any anti-malware, firewall, and IDS products on the system • Gather information about the network (i.e., domain user/group information, domain computers, password policy) • Verify the ability to execute scripts or third-party programs • Mapping and Discovery should include: <ul style="list-style-type: none"> • Identify possible vulnerabilities affecting the provided host • Determine the possibility of receiving and executing various malicious payloads
	Advizex Response: Advizex acknowledges and agrees. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.

4.3.3.2.1	Mapping and Discovery should include: <ul style="list-style-type: none"> • Identify possible vulnerabilities affecting the provided host • Determine the possibility of receiving and executing various malicious payloads
4.3.3.2.2	Advizex Response: Advizex acknowledges and agrees. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.

4.3.3.3	Exploitation should include: <ul style="list-style-type: none"> • Attempt to bypass anti-malware solutions and security restrictions, escape restricted environments, and escalate privileges • Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)
4.3.3.3.1 4.3.3.3.2	Advizex Response: Advizex acknowledges and agrees. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.

4.3.4	Exploitation should include: <ul style="list-style-type: none"> • Attempt to bypass anti-malware solutions and security restrictions, escape restricted environments, and escalate privileges • Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)
	Advizex Response: Advizex acknowledges and agrees. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.

4.3.5	Testing shall assess the security of all networked assets, including but not limited to servers, endpoints, firewalls, network devices, and network monitoring and management.
	Advizex Response: Advizex acknowledges with the specification that the scope of this engagement will only include select endpoint workstations and laptops.

4.3.6	Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.
	Advizex Response: Advizex acknowledges.

4.3.6.1	Vendor shall provide a sample of the executive summary report with their bid response.
	Advizex Response: Advizex has included a redacted technical report with this submission for your review. The file name is: <ul style="list-style-type: none"> • Sample Redacted Client Cyber Security Testing v1.0 - Advizex v1_0.pdf

4.3.6.2	The report must be submitted to the Lottery electronically for review.
	Advizex Response: Advizex acknowledges.

4.3.7	Upon conclusion of the assessment, the Vendor must provide a Technical Report. This report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.
	Advizex Response: Advizex acknowledges.

<p>4.3.8 4.3.8.1 4.3.8.2 4.3.8.3</p>	<p>Reports must include specific details for each vulnerability found, including:</p> <ul style="list-style-type: none"> • How the vulnerability was discovered. • The potential impact of its exploitation. • Recommendations for remediation. • Vulnerability references.
<p>4.3.8.4</p>	<p>Advizex Response: Advizex acknowledges.</p>

<p>4.3.8.5</p>	<p>Vendor shall provide a sample of the executive summary report with their bid response.</p> <p>Advizex Response: Advizex has included a redacted technical report with this submission for your review. The file name is:</p> <ul style="list-style-type: none"> • Sample Redacted Client Cyber Security Testing v1.0 - Advizex v1_0.pdf
-----------------------	---

<p>4.3.8.6</p>	<p>The report must be submitted to the Lottery electronically for review.</p> <p>Advizex Response: Advizex acknowledges.</p>
-----------------------	--

<p>4.3.9</p>	<p>Upon conclusion of the assessment, the Vendor must provide a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.</p> <p>Advizex Response: Advizex acknowledges.</p>
---------------------	--

<p>4.3.9.1</p>	<p>The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.</p> <p>Advizex Response: Advizex acknowledges.</p>
-----------------------	---

4.4. WIRELESS PENETRATION TESTING

4.4.1	Wireless Penetration Testing must be performed onsite at all Lottery locations. Assessing locations remotely or from one central location is prohibited.
	Advizex Response: Advizex acknowledges.

4.4.2	Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.
	Advizex Response: Advizex acknowledges.

4.4.2	Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.
	Advizex Response: Advizex acknowledges.

4.4.3.1 4.4.3.1.1 4.4.3.1.2 4.4.3.1.3 4.4.3.1.4 4.4.3.1.5 4.4.3.1.6	Reconnaissance should include:
	<ul style="list-style-type: none"> • Perform WHOIS, ARIN, and DNS (public server) lookups • OSINT - Public Searches/Dorks • Build custom password lists • DNS lookups (entities server) • Gather information from entities web applications • Analyze metadata
	Advizex Response:
	Advizex acknowledges and agrees. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.

<p>4.4.3.2 4.4.3.2.1 4.4.3.2.2 4.4.3.2.3 4.4.3.2.4</p>	<p>Mapping should include:</p> <ul style="list-style-type: none"> • Sniffing (establish a baseline of traffic, sniff Wi-Fi, Bluetooth, Zigbee, and other RF) • War Walk (map location of access points and their coverage, identify leakage) • Identify Rogue Access Points* (Friendly, malicious, or unintended access points) • Full access to the buildings will be granted to the testing team
	<p>Advizex Response: Advizex acknowledges and agrees. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.</p>

<p>4.4.3.3 4.4.3.3.1 4.4.3.3.2 4.4.3.3.3</p>	<p>Discovery should include:</p> <ul style="list-style-type: none"> • Identify Points of Attack (Identify WEP networks, capture WPA/WPA2 PSK key exchanges, identify clients for evil-twin and MiTM attacks) • Enumerating Services (Connect and interact with services on APs, Bluetooth Devices, and other RF devices to disclose misconfigurations) • Vulnerability Scanning (Identify vulnerabilities)
	<p>Advizex Response: Advizex acknowledges and agrees. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.</p>

<p>4.4.3.4 4.4.3.4.1 4.4.3.4.2 4.4.3.4.3 4.4.3.4.4</p>	<p>Exploitation should include:</p> <ul style="list-style-type: none"> • AP Attacks (Exploit hotspots, perform MiTM attacks, crack WEP, crack WPA/WPA2 PSK, etc.) • Client Attacks (Perform Evil-Twin attacks, perform rogue AP attacks, MiTM, etc.) • Denial of Service where applicable and with prior Lottery approval • Bluetooth/Zigbee/SDR Attacks where applicable and with prior Lottery approval
	<p>Advizex Response: Advizex acknowledges and agrees. Please refer to Section 5 of this submission for detailed information related to our approach, methodology, tasks, and their associated deliverables.</p>

<p>4.4.4</p>	<p>Must identify prioritized remediation needs, requirements, and associated risks.</p>
	<p>Advizex Response: Advizex acknowledges.</p>

<p>4.4.5</p>	<p>Testing shall assess the security of all wireless assets.</p>
	<p>Advizex Response: Advizex acknowledges.</p>

<p>4.4.6</p>	<p>Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.</p>
	<p>Advizex Response: Advizex acknowledges.</p>

<p>4.4.6.1</p>	<p>The vendor shall provide a sample of the technical report with their bid response.</p>
----------------	--

	<p>Advizex Response: Advizex has included a redacted technical report with this submission for your review. The file name is:</p> <ul style="list-style-type: none"> • Sample Redacted Client Cyber Security Testing v1.0 - Advizex v1_0.pdf
--	--

4.4.6.2	The report must be submitted to the Lottery electronically for review.
	<p>Advizex Response: Advizex acknowledges.</p>

4.4.7	Upon completing the assessment, the Vendor must provide a Technical Report. This report details each vulnerability type discovered and assigns a critical, high, medium, or low risk rating.
	<p>Advizex Response: Advizex acknowledges.</p>

4.4.8	Reports must include specific details for each vulnerability found, including:	
	<ul style="list-style-type: none"> • How the vulnerability was discovered. 	
	4.4.8.1	<ul style="list-style-type: none"> • The potential impact of its exploitation.
	4.4.8.2	<ul style="list-style-type: none"> • Recommendations for remediation.
	4.4.8.3	<ul style="list-style-type: none"> • Vulnerability references.
4.4.8.4	<p>Advizex Response: Advizex acknowledges.</p>	

4.4.8.5	The vendor shall provide a sample of the technical report with their bid response.
	<p>Advizex Response: Advizex has included a redacted technical report with this submission for your review. The file name is:</p> <ul style="list-style-type: none"> • Sample Redacted Client Cyber Security Testing v1.0 - Advizex v1_0.pdf

4.4.8.6	The report must be submitted to the Lottery electronically for review.
	Advizex Response: Advizex acknowledges.

4.4.9	Upon the completion of the project, results will be presented to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.
	Advizex Response: Our team will provide a comprehensive and detailed presentation of all findings from the assessment. This will include a thorough analysis of strengths, weaknesses, and vulnerabilities found within your current systems and processes. We will also provide recommendations for remediation to address any identified issues and improve overall security posture. Our goal is to help your organization make informed decisions to better protect your data and assets.

4.4.9.1	The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon completion of the project.
	Advizex Response: The presentation can be delivered - either in person or via a conference call, depending on what works best for your team at Lottery. Our goal is to ensure that all key stakeholders have the opportunity to fully understand and discuss the results of the assessment, so that together we can make informed decisions about next steps to improve your organization's security posture.

5. ENGAGEMENT APPROACH

5.1 ENGAGEMENT SUMMARY

Advizex will provide conduct a Phased Cyber Security Test for Advizex Client, the West Virginia lottery.

Our penetration testing framework is in strict compliance with the Penetration Testing Execution Standard (PTES), covering all critical phases: Planning, Information Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, and Reporting. This ensures a thorough and effective assessment, providing a clear roadmap for enhancing the web application's security.

The testing will follow the guidelines and procedures established by NIST SP 800-115, titled "Technical Guide to Information Security Testing and Assessment," SANS CWE Top 25, CERT Secure Coding, the OSTMM Open-Source Security Testing Methodology Manual and (OWASP) Open Web Application Security Project.

The Cyber Security Web Application Penetration Test process involves an active analysis of internal and external information systems for any potential vulnerabilities and exploits that could result from poor or improper system configuration, both known and unknown hardware, software flaws, and operational weaknesses in process or technical countermeasures. This testing is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities.

Security issues uncovered through the Cyber Security Vulnerability Test and Web Application Penetration Test will be presented to the Advizex Client. ALL URGENT SECURITY ISSUES FOUND DURING TESTING WILL BE REPORTED IMMEDIATELY AFTER PROPER ANALYSIS.

Advizex will perform remote vulnerability, penetration tests, and web application penetration tests from our corporate headquarters in Londonderry, NH. Advizex Client will provide credentials as required. Testing will identify whether exploits can be used to penetrate web-based software applications. Advizex will perform web application penetration tests remotely. Internal Vulnerability and Wi-Fi Penetration Testing will be performed on-site as requested by the RFP.

All Testing will be performed during normal business hours of 9am to 5pm Eastern Time. Internal Testing will be performed at location in Charlestown, WV and we expect to be able to scan all other locations from that site. Testing will last approximately two to three weeks from

start to draft deliverable. The acceptance period for the draft deliverable will be 5 business days after draft delivery.

Due to the unpredictable nature of Vulnerability and Penetration Testing hardware and software may perform erratically during testing. Therefore, Advizex cannot guarantee availability and uptime of all systems tested.

5.2 CYBER SECURITY TESTING PROJECT SCOPE

Advizex understands the following and will perform the following:

5.2.1 External Penetration Testing

- Advizex will Perform an External Penetration Test on approximately 24 External IP Addresses for the Advizex Client from a remote location.
- Remote vulnerability, penetration tests, and web application penetration tests from one of our secure branch locations.

5.2.2 Web Application Penetration Testing

Advizex will Perform Web Application Penetration Test on selected Web Sites and Web Applications. Web Application Penetration Testing will occur on up to four software application environments. The Application Penetration Test on approximately 1 Host and related supporting systems and attempt to gain access to the system via Web Application Vulnerabilities. Web Application Penetration Testing will occur on up to four Web Based Applications following software application environments.

5.2.3 Internal Vulnerability Assessment

Advizex will Perform a Vulnerability Assessment on less than 1000 Hosts/IP Addresses for the Advizex Client. The Credentialed Vulnerability Assessment will be comprised of Servers, Computers, Notebooks, Switches, and Routers spread across multiple Subnets. Advizex will perform vulnerability tests locally on-site at in Charlestown, WV. We will also performing internal vulnerability scanning on-site at all sites.

5.2.4 Wi-Fi Penetration Testing

Testing will include wireless availability internally and on the physical exterior perimeter. Wi-Fi Testing will include reconnaissance, vulnerability assessment, exploitation and off-line password cracking. The main goal of wireless penetration testing is to see how well the security measures in place to protect wireless networks are working and to find any flaws that could lead to unauthorized access, data breaches, or other cyber threats. We will also performing Wi-Fi Penetration Testing on-site at all sites.

5.2.5 Result Analysis and Deliverable Creation

Advizex will provide a preliminary draft report to the Advizex Project Manager point of contact(s) for the purpose of review and clarification with Project Manager. The draft review will take place via an internet-based meeting with the Advizex Client. Following this process, the final reports will be issued. The end deliverables will consist of a word document, detailed technical reports, an abbreviated Executive and a Findings Technical Presentation. All Presentation will be done remotely via Microsoft Teams.

The reports will be in full compliance with all requirements set forth by the Advizex Client in the proposal and will include:

5.3 EXTERNAL PENETRATION TESTING

5.3.1 External Reconnaissance/Enumeration Phase

Our objective is to perform a successful External White Box Vulnerability Assessment and Penetration Test that provides for a stealthy approach. External Testing will be performed as a White Box Test where the Advizex Client will supply all information needed for External Testing. External IP Addressing will be provided by the Advizex Client. Reconnaissance will be used to verify information provided by the Advizex Client.

We utilize several tools that provide us with corroborating information that will determine what testing methodology we will use. This testing will include but not limited to:

- Internet searches
- Domain name management/search services
- DNSMap
- Non-intrusive network scanning
- Ping Sweeps
- Open Port Scanning

Goals

The goal of this phase is to determine the breadth of the number of IPs and the security architecture used by the client.

5.3.2 External Vulnerability Scanning Phase

The Vulnerability Assessment Scanning of External IP Addresses is enabled using a combination of port-based enumeration and vulnerability software Tools. The Scans will identify Vulnerabilities that can be exploited during the next phase. These Vulnerability Assessment

Tools will include:

Automated and Commercial Tools

- Nessus Professional Feed Vulnerability Scanner
- Saint Vulnerability Scanner
- Burp Suite Professional

Manual Open-Source Tools

- OpenVAS Vulnerability Scanner
- Nmap
- Zenmap
- Fping
- Hping3
- ParrotOS

Goals

Phase Two Goals will include the following:

- Open services
- Vulnerable applications, including operating systems
- Weak protection of data in transit
- Make and model of each piece of LAN/WAN equipment
- Web Application Identification
- Identify Live Host
- IDS IPS Identification
- Network Traffic Analysis
- OS Finger Printing
- Route Analysis
- Service Finger Printing
- SMTP Analysis
- Vulnerability Identification

5.3.3 External Penetration Exploitation Phase

Gaining access to resources is the whole point of a modern-day attack. The usual goal is to either extract information of value to the attacker or use the network as a launch site for attacks against other targets. In either situation, the attacker must gain some level of access to one or more network devices.

We utilize a combination of “open source” and commercial grade penetration solutions to test Internet Facing IP’s and Websites.

The following tools will be used:

Automated and Commercial

- Saint Exploit Server
- Manual and Open Source
- Metasploit Framework
- Backtrack Framework Version
- Kali Linux
- ParrotOS
- GitHub POCs

Goals

- Provide Positive Proof that any Exploit Exists
- Provide Proof that a new Denial of Service Vulnerability Exists

5.4 WEB APPLICATION PENETRATION TESTING

5.4.1 Web Application Penetration Testing Methodology

Advizex will internally test the Advizex Client Servers and Web Based Applications for Vulnerabilities, and Exploits which may be used as attack vectors to penetrate. A successful Penetration Test can be as simple as interrogating a server which yields information about its configuration in terms of software and versions, which can be used as attach vectors in further testing.

Advizex will perform Web application testing based on OWASP (Open Web Application Security Project) Top 10, and OSSTMM (Open-Source Security Testing Methodology Manual) security testing and analysis to provide value and the knowledge that it has been done thoroughly, efficiently, and accurately. Web Application Penetration Testing will identify without a doubt whether the Advizex Client Web Applications can be compromised.

Web Application Testing based on OSSTMM (Open-Source Security Testing Methodology Manual):

- Physical Security Testing
- Telecommunications Security Testing
- Data Networks Security Testing
- Wireless Security Testing
- Compliance Regulations
- Operational Security Metrics
- Trust Analysis
- Workflow.

- Human Security Testing
- Web Application Testing based on OWASP will test the following:
 - A1 Injection
 - A2 Weak authentication and session management
 - A3 XSS
 - A4 Insecure Direct Object References
 - A5 Security Misconfiguration
 - A6 Sensitive Data Exposure
 - A7 Missing Function Level Access Control
 - A8 Cross Site Request Forgery
 - A9 Using Components with Known Vulnerabilities
 - A10 Unvalidated Redirects and Forwards

5.4.2 Web Application Enumeration Phase

Advizex will enumerate the Web Applications to determine, the type of Web Application, Open Port, IP Addresses, Domain Names, Aliases and Users.

- Web Application Typing: classify the specific type of each web application, which helps in understanding the application's framework and potential vulnerabilities.
- Open Port Detection: identify any open ports that are essential for the application's communication but may also represent potential security risks.
- IP Address Mapping: document all IP addresses associated with the web application, aiding in network mapping and security zoning.
- Domain Name Cataloging: compile a comprehensive list of domain names linked to the web application, which is crucial for managing digital assets and understanding domain exposure.
- Alias Identification: uncover and list any aliases, pointing to the flexibility and reach of the web application within the digital space.
- User Enumeration: enumerate user accounts which can be a critical component in assessing access controls and audit trails.

Goals

Goals will include identifying the following:

- Open services
- Vulnerable applications, including operating systems
- Weak protection of data in transit
- Web Application Identification
- Identify Live Host
- IDS IPS Identification
- Network Traffic Patterns
- OS Finger Printing

- Route Analysis
- Service Finger Printing
- SMTP Analysis
- Vulnerability Identification

Automated and Commercial Tools

- Nessus Professional Feed Vulnerability Scanner
- Saint Vulnerability Scanner
- Burp Suite Professional

Manual Open-Source Tools

- OpenVAS Vulnerability Scanner
- Nmap
- Zenmap
- Fping
- Hping

5.4.3 Web Application Vulnerability Scanning

The Vulnerability Assessment Scanning of 4 IP Addresses is enabled using a combination of port-based enumeration and vulnerability software Tools. These Vulnerability Assessment

Tools will include:

Automated and Commercial Tools

- Tenable Nessus Professional
- OWASP ZAP Web Scanner
- Accunetix
- Burp Suite Professional

Manual and Open-Source Tools

- Kali Linux
- ParrotOS
- NMAP
- Burp Suite Professional
- DIG
- Nuclei 2.7.6
- Metasploit Framework
- MSAF Web Attack and Audit Framework
- N-Stalker
- Open-Source Tools
- Scrawlr

- Watcher
- Web Scarab
- Websecurify

5.4.4 Web App Exploitation

The Web Application Exploitation component of this Scope of Work involves a comprehensive analysis and testing of the target web application to identify and exploit security vulnerabilities.

This process is critical for assessing the security posture of the application and ensuring its resilience against malicious cyber threats.

Our approach includes a thorough examination of the application's architecture, codebase, and operational environment.

We will employ a combination of automated tools and manual testing techniques to uncover weaknesses such as SQL injection, cross-site scripting (XSS), broken authentication, and security misconfigurations.

This phase is vital for understanding potential attack vectors and the associated risks.

Web Application Testing will test for the following flaws:

- Information Relay
- Invalidated Input
- Insecure Configuration Management
- Broken Access Control
- Broken Authentication and Session Management
- Cross Site Scripting
- Buffer Overflow
- SQL Injection Flaws
- Misc. Code Injections
- Improper Error Handling
- Insecure Storage
- Access Control in J2EE Applications
- Application Backdoors
- Privilege Escalation

Goals

Demonstrate ability to Alter/Change, or input code into web applications.

5.4.5 Web Application Privilege Escalation (Post Exploitation)

Most Web Based Applications are designed for use with multiple users. Privileges mean what a user is permitted to do. Common privileges include viewing and editing files or modifying system files.

Privilege escalation means a user receives privileges they are and are not entitled to. These privileges can be used to delete files, view private information, or install unwanted programs such as Viruses, Malware, and Trojans. It usually occurs when a system has a bug that allows security measures to be bypassed or, alternatively has flawed design assumptions about how it will be used.

To achieve these goals, Advizex uses the following types of attacks and associated tools that fit the pen testing parameters such as.

On-line Password Cracking

- Hydra
- Medusa

Off-line Password Cracking

- Jack-the-Ripper
- Cain and Abel
- L0pht Crack
- Rainbow Tables
- Cracking Services

Goals

Gain User, Root and Administrative Access to Web Applications. Demonstrate ability to Alter/Change, or input code into web applications.

5.5 INTERNAL VULNERABILITY SCANNING

5.5.1 Internal Enumeration Phase

Our objective is to perform a successful White Box Vulnerability Assessment and Penetration Test that provides for a stealthy approach. Advizex will be performing services for Advizex. Testing will be performed as a White Box Test where the Advizex Client will supply all information needed for Testing. Internal IP Addressing will be provided by the Advizex Client. Advizex will utilize its own reconnaissance to verify information provided by the Advizex Client, as well.

Advizex will perform these services on-site at the following locations

- Charleston
- Mardi-Gras
- Bridgeport
- Weirton
- Greenbrier
- Hollywood

- Mountaineer
- Wheeling

We utilize several tools that provide us with corroborating information that will determine what testing methodology we will use. This testing will include but not limited to:

- Non-intrusive network scanning
- Ping Sweeps
- Selective Open Port Scanning
- NMAP Scanning

Goals

The goal of this phase is to determine the breadth of the number of IPs and the security architecture used by the client.

5.5.2 Internal Vulnerability Scanning Phase

The Vulnerability Assessment Scanning of up to 400 IP Addresses is enabled using a combination of port-based enumeration and vulnerability software Tools. These Vulnerability Assessment Tools will include:

Automated and Commercial Tools

- Nessus Professional Feed Vulnerability Scanner
- Saint Vulnerability Scanner

Manual Tools

- OpenVAS Vulnerability Scanner
- Nmap
- Zenmap
- Fping
- Hping

Goals

Phase Two Goals will include the following:

- Identify Open services
- Vulnerable applications, including operating systems
- Weak protection of data in transit
- Make and model of each piece of LAN/WAN equipment
- Web Application Identification
- Identify Live Host
- IDS IPS Identification
- Network Traffic Analysis
- OS Finger Printing
- Route Analysis

- Service Finger Printing
- SMTP Analysis
- Vulnerability Identification

5.6 Wi-Fi PENETRATION TESTING

We will conduct Wi-Fi Security Testing. Testing will include wireless availability internally and on the physical exterior perimeter. Wi-Fi Testing will include reconnaissance, vulnerability assessment, exploitation and off-line password cracking.

The main goal of wireless penetration testing is to see how well the security measures in place to protect wireless networks are working and to find any flaws that could lead to unauthorized access, data breaches, or other cyber threats.

Key aspects of wireless penetration testing include:

- **Network Discovery:** Identifying all wireless access points (APs), routers, and other network devices within the target environment.
- **Vulnerability Assessment:** Identifying and assessing potential vulnerabilities in the wireless network infrastructure, such as outdated firmware, weak encryption protocols, default credentials, and misconfigured settings.
- **Authentication and Encryption:** Evaluating the strength of authentication mechanisms and encryption protocols used in the wireless network to ensure they are resistant to attacks like brute force and eavesdropping.
- **Traffic Analysis:** Analyzing network traffic to detect anomalies, rogue devices, and potential unauthorized access attempts.
- **Exploitation:** Attempting to exploit discovered vulnerabilities to gain unauthorized access to the network, simulate potential attack scenarios, and assess the impact of successful attacks.
- **Mitigation Recommendations:** Providing recommendations and actionable steps to address identified vulnerabilities and improve the overall security posture of the wireless network.
- **Compliance and Regulation:** Ensuring that the wireless network complies with relevant industry standards and regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) for networks handling payment card data.

Wireless penetration testing helps organizations proactively identify and address security weaknesses before malicious hackers can exploit them.

Wi-Fi Testing will include:

- Discover the SSID using Aircrack-ng and Kismet
- Look for Rogue Devices and Ad-hoc Internal Wireless Networks

- Discover and Decrypt the Wi-Fi Password if possible
- Sniff and Capture any Unencrypted Data
- Test if users can access the network without authentication
- Test Guest Login Credential for access to Production Network
- Assess networks configurations such as encryption standards and passwords
- Check the status of MAC filtering
- Spoof the MAC Address if MAC Authentication is being used.
- Check network accessibility
- Check for any obsolete hardware or services running

Advizex will perform these services on-site at the following locations

- Charleston
- Mardi-Gras
- Bridgeport
- Weirton
- Greenbrier
- Hollywood
- Mountaineer
- Wheeling

Tools

Advizex will perform the evaluation using a variety of open source and commercial based testing tools to include:

- Aircrack NG
- Airodump
- Kismet
- Etherdump
- Wireshark

Goals

Determine the feasibility of a Wi-Fi Penetration Attack and Exploit the Wi-Fi

5.7 REPORTING

Advizex will provide a preliminary draft report to the Advizex Project Manager point of contact(s) for the purpose of review and clarification with Project Manager. The draft review will take place via an internet-based meeting with the Advizex Client. Following this process, the final reports will be issued. The end deliverables will consist of a word document, detailed technical reports, an abbreviated Executive and a Findings Technical Presentation.

The reports will be in full compliance with all requirements set forth by the Advizex Client in the proposal.

5.7.1 Executive Summary Report

The Executive Summary Report will include charts, graphs and tables. The design of the overview is to provide the Advizex Client management an easy to read and understand overview of the potential impact these exploits could have on the environment.

5.7.2 Detailed Technical Report

The Technical Report will detail each system's and application's discovered vulnerabilities. The technical report will include recommended resolutions for all high-risk vulnerabilities. The technical report should include the scope of any the Advizex Client data extracted through penetration testing.

5.7.3 Findings Presentation

The Technical Findings Presentation will mirror and detail the Detailed Technical Report. The PowerPoint will detail each system's and application's discovered vulnerabilities. The technical report will include recommended resolutions for all high-risk vulnerabilities. The technical report should include the scope of any the Advizex Client data extracted through penetration testing. Presentation will be done remotely via Microsoft Teams.



6. PRICING PAGE (EXHIBIT A)

EXHIBIT A - Pricing Page

Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	\$1,537.13	\$12,297.00
2	4.2	Website Penetration Testing	8	\$1,302.63	\$10,421.00
3	4.3	Internal/Client-Side Network Penetration Testing	8	\$2,787.13	\$22,297.00
4	4.4	Wireless Penetration Testing	8	\$1,849.38	\$14,795.00
TOTAL BID AMOUNT					\$59,810.00

Please note the following information is being captured for auditing purposes and is an estimate for evaluation only

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

Any product or service not on the Agency provided Pricing Page will not be allowable.

The state cannot accept alternate pricing pages, failure to use Exhibit A Pricing Page could lead to disqualification of vendors bid.

Vendor Name:	Advizex Technologies, LLC
Vendor Address:	680 Andersen Drive, Foster Plaza 10, 2nd Floor, Pittsburgh, PA 15220
Email Address:	mmunoz@advizex.com
Phone Number:	304-615-3301
Fax Number:	216-901-1447
Signature and Date:	<i>Mika Munoz</i>



APPENDIX A. CERTIFICATE OF INSURANCE

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

XTEND ENDORSEMENT FOR TECHNOLOGY

This endorsement modifies insurance provided under the following:

COMMERCIAL GENERAL LIABILITY COVERAGE PART

GENERAL DESCRIPTION OF COVERAGE – This endorsement broadens coverage. However, coverage for any injury, damage or medical expenses described in any of the provisions of this endorsement may be excluded or limited by another endorsement to this Coverage Part, and these coverage broadening provisions do not apply to the extent that coverage is excluded or limited by such an endorsement. The following listing is a general coverage description only. Read all the provisions of this endorsement and the rest of your policy carefully to determine rights, duties, and what is and is not covered.

- | | |
|---|---|
| <ul style="list-style-type: none"> A. Non-Owned Watercraft – 75 Feet Long Or Less B. Who Is An Insured – Unnamed Subsidiaries C. Who Is An Insured – Employees – Supervisory Positions D. Who Is An Insured – Newly Acquired Or Formed Limited Liability Companies E. Who Is An Insured – Liability For Conduct Of Unnamed Partnerships Or Joint Ventures F. Blanket Additional Insured – Persons Or Organizations For Your Ongoing Operations As Required By Written Contract Or Agreement G. Blanket Additional Insured – Broad Form Vendors H. Blanket Additional Insured – Controlling Interest | <ul style="list-style-type: none"> I. Blanket Additional Insured – Mortgagees, Assignees, Successors Or Receivers J. Blanket Additional Insured – Governmental Entities – Permits Or Authorizations Relating To Premises K. Blanket Additional Insured – Governmental Entities – Permits Or Authorizations Relating To Operations L. Medical Payments – Increased Limit M. Blanket Waiver Of Subrogation N. Contractual Liability – Railroads O. Damage To Premises Rented To You |
|---|---|

PROVISIONS

A. NON-OWNED WATERCRAFT – 75 FEET LONG OR LESS

1. The following replaces Paragraph (2) of Exclusion **g.**, **Aircraft, Auto Or Watercraft**, in Paragraph 2. of **SECTION I – COVERAGES – COVERAGE A – BODILY INJURY AND PROPERTY DAMAGE LIABILITY**:

(2) A watercraft you do not own that is:

- (a) 75 feet long or less; and
- (b) Not being used to carry any person or property for a charge;

2. The following replaces Paragraph 2.e. of **SECTION II – WHO IS AN INSURED**:

e. Any person or organization that, with your express or implied consent, either uses or

is responsible for the use of a watercraft that you do not own that is:

- (1) 75 feet long or less; and
- (2) Not being used to carry any person or property for a charge.

B. WHO IS AN INSURED – UNNAMED SUBSIDIARIES

The following is added to **SECTION II – WHO IS AN INSURED**:

Any of your subsidiaries, other than a partnership or joint venture, that is not shown as a Named Insured in the Declarations is a Named Insured if:

- a. You are the sole owner of, or maintain an ownership interest of more than 50% in, such subsidiary on the first day of the policy period; and
- b. Such subsidiary is not an insured under similar other insurance.

COMMERCIAL GENERAL LIABILITY

No such subsidiary is an insured for "bodily injury" or "property damage" that occurred, or "personal and advertising injury" caused by an offense committed:

- a. Before you maintained an ownership interest of more than 50% in such subsidiary; or
- b. After the date, if any, during the policy period that you no longer maintain an ownership interest of more than 50% in such subsidiary.

For purposes of Paragraph 1. of Section II – Who Is An Insured, each such subsidiary will be deemed to be designated in the Declarations as:

- a. A limited liability company;
- b. An organization other than a partnership, joint venture or limited liability company; or
- c. A trust;

as indicated in its name or the documents that govern its structure.

C. WHO IS AN INSURED – EMPLOYEES – SUPERVISORY POSITIONS

The following is added to Paragraph 2.a.(1) of SECTION II – WHO IS AN INSURED:

Paragraphs (1)(a), (b) and (c) above do not apply to "bodily injury" to a co-"employee" while in the course of the co-"employee's" employment by you arising out of work by any of your "employees" who hold a supervisory position.

D. WHO IS AN INSURED – NEWLY ACQUIRED OR FORMED LIMITED LIABILITY COMPANIES

The following replaces Paragraph 3. of SECTION II – WHO IS AN INSURED:

3. Any organization you newly acquire or form, other than a partnership or joint venture, and of which you are the sole owner or in which you maintain an ownership interest of more than 50%, will qualify as a Named Insured if there is no other similar insurance available to that organization. However:
 - a. Coverage under this provision is afforded only:
 - (1) Until the 180th day after you acquire or form the organization or the end of the policy period, whichever is earlier, if you do not report such organization in writing to us within 180 days after you acquire or form it; or
 - (2) Until the end of the policy period, when that date is later than 180 days after you acquire or form such organization, if you report such

organization in writing to us within 180 days after you acquire or form it;

- b. Coverage A does not apply to "bodily injury" or "property damage" that occurred before you acquired or formed the organization; and
- c. Coverage B does not apply to "personal and advertising injury" arising out of an offense committed before you acquired or formed the organization.

For the purposes of Paragraph 1. of Section II – Who Is An Insured, each such organization will be deemed to be designated in the Declarations as:

- a. A limited liability company;
- b. An organization, other than a partnership, joint venture or limited liability company; or
- c. A trust;

as indicated in its name or the documents that govern its structure.

E. WHO IS AN INSURED – LIABILITY FOR CONDUCT OF UNNAMED PARTNERSHIPS OR JOINT VENTURES

The following replaces the last paragraph of SECTION II – WHO IS AN INSURED:

No person or organization is an insured with respect to the conduct of any current or past partnership or joint venture that is not shown as a Named Insured in the Declarations. This paragraph does not apply to any such partnership or joint venture that otherwise qualifies as an insured under Section II – Who Is An Insured.

F. BLANKET ADDITIONAL INSURED – PERSONS OR ORGANIZATIONS FOR YOUR ONGOING OPERATIONS AS REQUIRED BY WRITTEN CONTRACT OR AGREEMENT

The following is added to SECTION II – WHO IS AN INSURED:

Any person or organization that is not otherwise an insured under this Coverage Part and that you have agreed in a written contract or agreement to include as an additional insured on this Coverage Part is an insured, but only with respect to liability for "bodily injury" or "property damage" that:

- a. Occurs subsequent to the signing of that contract or agreement; and
- b. Is caused, in whole or in part, by your acts or omissions in the performance of your ongoing operations to which that contract or

agreement applies or the acts or omissions of any person or organization performing such operations on your behalf.

The limits of insurance provided to such insured will be the minimum limits that you agreed to provide in the written contract or agreement, or the limits shown in the Declarations, whichever are less.

G. BLANKET ADDITIONAL INSURED – BROAD FORM VENDORS

The following is added to **SECTION II – WHO IS AN INSURED:**

Any person or organization that is a vendor and that you have agreed in a written contract or agreement to include as an additional insured on this Coverage Part is an insured, but only with respect to liability for "bodily injury" or "property damage" that:

- a. Occurs subsequent to the signing of that contract or agreement; and
- b. Arises out of "your products" that are distributed or sold in the regular course of such vendor's business.

The insurance provided to such vendor is subject to the following provisions:

- a. The limits of insurance provided to such vendor will be the minimum limits that you agreed to provide in the written contract or agreement, or the limits shown in the Declarations, whichever are less.
- b. The insurance provided to such vendor does not apply to:
 - (1) Any express warranty not authorized by you or any distribution or sale for a purpose not authorized by you;
 - (2) Any change in "your products" made by such vendor;
 - (3) Repackaging, unless unpacked solely for the purpose of inspection, demonstration, testing, or the substitution of parts under instructions from the manufacturer, and then repackaged in the original container;
 - (4) Any failure to make such inspections, adjustments, tests or servicing as vendors agree to perform or normally undertake to perform in the regular course of business, in connection with the distribution or sale of "your products";
 - (5) Demonstration, installation, servicing or repair operations, except such operations

performed at such vendor's premises in connection with the sale of "your products"; or

- (6) "Your products" that, after distribution or sale by you, have been labeled or relabeled or used as a container, part or ingredient of any other thing or substance by or on behalf of such vendor.

Coverage under this provision does not apply to:

- a. Any person or organization from whom you have acquired "your products", or any ingredient, part or container entering into, accompanying or containing such products; or
- b. Any vendor for which coverage as an additional insured specifically is scheduled by endorsement.

H. BLANKET ADDITIONAL INSURED – CONTROLLING INTEREST

- 1. The following is added to **SECTION II – WHO IS AN INSURED:**

Any person or organization that has financial control of you is an insured with respect to liability for "bodily injury", "property damage" or "personal and advertising injury" that arises out of:

- a. Such financial control; or
- b. Such person's or organization's ownership, maintenance or use of premises leased to or occupied by you.

The insurance provided to such person or organization does not apply to structural alterations, new construction or demolition operations performed by or on behalf of such person or organization.

- 2. The following is added to Paragraph 4. of **SECTION II – WHO IS AN INSURED:**

This paragraph does not apply to any premises owner, manager or lessor that has financial control of you.

I. BLANKET ADDITIONAL INSURED – MORTGAGEES, ASSIGNEES, SUCCESSORS OR RECEIVERS

The following is added to **SECTION II – WHO IS AN INSURED:**

Any person or organization that is a mortgagee, assignee, successor or receiver and that you have agreed in a written contract or agreement to include as an additional insured on this Coverage Part is an insured, but only with respect to its

COMMERCIAL GENERAL LIABILITY

liability as mortgagee, assignee, successor or receiver for "bodily injury", "property damage" or "personal and advertising injury" that:

- a. Is "bodily injury" or "property damage" that occurs, or is "personal and advertising injury" caused by an offense that is committed, subsequent to the signing of that contract or agreement; and
- b. Arises out of the ownership, maintenance or use of the premises for which that mortgagee, assignee, successor or receiver is required under that contract or agreement to be included as an additional insured on this Coverage Part.

The insurance provided to such mortgagee, assignee, successor or receiver is subject to the following provisions:

- a. The limits of insurance provided to such mortgagee, assignee, successor or receiver will be the minimum limits that you agreed to provide in the written contract or agreement, or the limits shown in the Declarations, whichever are less.
- b. The insurance provided to such person or organization does not apply to:
 - (1) Any "bodily injury" or "property damage" that occurs, or any "personal and advertising injury" caused by an offense that is committed, after such contract or agreement is no longer in effect; or
 - (2) Any "bodily injury", "property damage" or "personal and advertising injury" arising out of any structural alterations, new construction or demolition operations performed by or on behalf of such mortgagee, assignee, successor or receiver.

J. BLANKET ADDITIONAL INSURED – GOVERNMENTAL ENTITIES – PERMITS OR AUTHORIZATIONS RELATING TO PREMISES

The following is added to **SECTION II – WHO IS AN INSURED**:

Any governmental entity that has issued a permit or authorization with respect to premises owned or occupied by, or rented or loaned to, you and that you are required by any ordinance, law, building code or written contract or agreement to include as an additional insured on this Coverage Part is an insured, but only with respect to liability for "bodily injury", "property damage" or "personal and advertising injury" arising out of the existence, ownership, use, maintenance, repair,

construction, erection or removal of any of the following for which that governmental entity has issued such permit or authorization: advertising signs, awnings, canopies, cellar entrances, coal holes, driveways, manholes, marquees, hoist away openings, sidewalk vaults, elevators, street banners or decorations.

K. BLANKET ADDITIONAL INSURED – GOVERNMENTAL ENTITIES – PERMITS OR AUTHORIZATIONS RELATING TO OPERATIONS

The following is added to **SECTION II – WHO IS AN INSURED**:

Any governmental entity that has issued a permit or authorization with respect to operations performed by you or on your behalf and that you are required by any ordinance, law, building code or written contract or agreement to include as an additional insured on this Coverage Part is an insured, but only with respect to liability for "bodily injury", "property damage" or "personal and advertising injury" arising out of such operations.

The insurance provided to such governmental entity does not apply to:

- a. Any "bodily injury", "property damage" or "personal and advertising injury" arising out of operations performed for the governmental entity; or
- b. Any "bodily injury" or "property damage" included in the "products-completed operations hazard".

L. MEDICAL PAYMENTS – INCREASED LIMIT

The following replaces Paragraph 7. of **SECTION III – LIMITS OF INSURANCE**:

7. Subject to Paragraph 5. above, the Medical Expense Limit is the most we will pay under Coverage C for all medical expenses because of "bodily injury" sustained by any one person, and will be the higher of:
 - a. \$10,000; or
 - b. The amount shown in the Declarations of this Coverage Part for Medical Expense Limit.

M. BLANKET WAIVER OF SUBROGATION

The following is added to Paragraph 8., **Transfer Of Rights Of Recovery Against Others To Us**, of **SECTION IV – COMMERCIAL GENERAL LIABILITY CONDITIONS**:

If the insured has agreed in a contract or agreement to waive that insured's right of recovery against any person or organization, we

waive our right of recovery against such person or organization, but only for payments we make because of:

- a. "Bodily injury" or "property damage" that occurs; or
- b. "Personal and advertising injury" caused by an offense that is committed;

subsequent to the execution of the contract or agreement.

N. CONTRACTUAL LIABILITY – RAILROADS

1. The following replaces Paragraph **c.** of the definition of "insured contract" in the **DEFINITIONS** Section:

- c. Any easement or license agreement;

2. Paragraph **f.(1)** of the definition of "insured contract" in the **DEFINITIONS** Section is deleted.

O. DAMAGE TO PREMISES RENTED TO YOU

The following replaces the definition of "premises damage" in the **DEFINITIONS** Section:

"Premises damage" means "property damage" to:

- a. Any premises while rented to you or temporarily occupied by you with permission of the owner; or
- b. The contents of any premises while such premises is rented to you, if you rent such premises for a period of seven or fewer consecutive days.

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

SHORT TERM HIRED AUTO – ADDITIONAL INSURED AND LOSS PAYEE

This endorsement modifies insurance provided under the following:

- AUTO DEALERS COVERAGE FORM
- BUSINESS AUTO COVERAGE FORM
- MOTOR CARRIER COVERAGE FORM

SCHEDULE

Additional Insured (Lessor):

Any lessor of a "leased auto" under a leasing or rental agreement of less than 6 months.

Designation Or Description Of "Leased Autos":

Any "leased auto" under a leasing or rental agreement of less than 6 months.

A. Coverage

1. Any "leased auto" designated or described in the Schedule will be considered a covered "auto" you own and not a covered "auto" you hire or borrow for **Covered Autos Liability Coverage**.
2. For a "leased auto" designated or described in the Schedule, the **Who Is An Insured** provision under **Covered Autos Liability Coverage** is changed to include as an "insured" the lessor of such "leased auto". However, the lessor is an "insured" only for "bodily injury" or "property damage" resulting from the acts or omissions by:
 - a. You;
 - b. Any of your "employees" or agents; or
 - c. Any person, except the lessor or any "employee" or agent of the lessor,

operating a "leased auto" with the permission of any of the above.

3. Coverage for any "leased auto" described in the Schedule applies until the end of the policy period shown in the Declarations or when the lessor or his or her agent takes possession of the "leased auto", whichever occurs first.

B. Loss Payable Clause

1. We will pay, as interest may appear, you and the lessor, if your policy includes Hired Auto Physical Damage Coverage, for "loss" to a "leased auto".
2. The insurance covers the interest of the lessor unless the "loss" results from fraudulent acts or omissions on your part.
3. If we make any payment to the lessor, we will obtain his or her rights against any other party.

C. The lessor is not liable for payment of your premiums.

D. Additional Definition

As used in this endorsement:

"Leased auto" means an "auto" leased or rented to you, including any substitute, replacement or extra "auto" needed to meet seasonal or other needs, under a leasing or rental agreement that requires you to provide direct primary insurance for the lessor.



THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

**WAIVER OF OUR RIGHT TO RECOVER
FROM OTHERS ENDORSEMENT**

Policy Number: 45 WEC AA7S8F

Endorsement Number:

Effective Date: 11/01/23

Effective hour is the same as stated on the Information Page of the policy.

Named Insured and Address: Rolta AdvizeX Technologies LLC
6480 ROCKSIDE WOODS BLVD S
INDEPENDENCE OH 44131

We have the right to recover our payments from anyone liable for an injury covered by this policy. We will not enforce our right against the person or organization named in the Schedule.

This agreement shall not operate directly or indirectly to benefit anyone not named in the Schedule.

SCHEDULE

Any person or organization for whom you are required by contract or agreement to obtain this waiver from us. Endorsement is not applicable in KY, NH, NJ or for any MO construction risk

Countersigned by _____
Authorized Representative



APPENDIX B. ACKNOWLEDGEMENT OF ADDENDUMS

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: LOT240000009

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7 |
| <input type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8 |
| <input type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9 |
| <input type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

ADVIZEX TECHNOLOGIES, LLC
Company
SCOTT NESS
Authorized Signature
3/27/24
Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.
Revised 6/8/2012



APPENDIX C. NON-DISCLOSURE AGREEMENT (EXHIBIT B)

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

MUTUAL NON-DISCLOSURE AGREEMENT

This Mutual Non-Disclosure Agreement (“Agreement”) is entered into by and between the West Virginia Lottery, with its principal offices located at 900 Pennsylvania Avenue Charleston, WV 25302 (“Lottery”), and Advizex Technologies, LLC, with its principal offices located at 6480 Rockside Woods Blvd S, Suite 190, Independence, OH 44131 (“Party of the second part”), with an Effective Date of 3/27/2024. Lottery and Party of the second party also are referred to herein individually as a “party”, or collectively as the “parties”.

WHEREAS, the parties to this Agreement may wish to exchange certain information related to the provision of certain information or communication technology services by one party of interest to the other party; and

WHEREAS, the parties agree that improper disclosure of either party’s Confidential Information, as defined below, by the other party could cause material harm to the party whose Confidential Information was improperly disclosed;

NOW THEREFORE, in order to protect certain Confidential Information that may be disclosed between the parties, Lottery and Alpha agree to maintain the confidentiality of the Confidential Information as follows:

I. Definition of Confidential Information. The "Confidential Information" disclosed under this Agreement is defined as follows:

Any data or information that is proprietary to the disclosing party and not generally known to the public, whether in tangible or intangible form, whenever and however disclosed, including, but not limited to: (i) any marketing strategies, plans, financial information, or projections, operations, sales estimates, business plans and performance results relating to the past, present or future business activities of such party, its affiliates, subsidiaries and affiliated companies; (ii) plans for products or services, and customer or supplier lists; (iii) any scientific or technical information, invention, design, process, procedure, formula, improvement, technology or method; (iv) any concepts, reports, data, know-how, works-in-progress, designs, development tools, specifications, computer software, source code, object code, flow charts, databases, inventions, intellectual property, and trade secrets; (v) solicitation for proposals, responses to proposals, bids, or information disclosed in connection with such solicitation, response, or bid; (vi) any other information that should reasonably be recognized as confidential information of the disclosing party.

II. Disclosure Period and Term. This Agreement protects against the disclosure of Confidential Information which is disclosed between the parties during each party’s performance of its obligations associated with that certain CRFQ Agreement executed between the parties on 3-27-24 (the “Effective Date”) and 3 year(s) after the termination of such Agreement (“Disclosure Period”). Therefore, the duty of a recipient of Confidential Information to protect such Confidential Information disclosed under this Agreement begins on the Effective Date and expires 3 year(s) after the end of Disclosure

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

Period. Upon termination of this Agreement or upon the disclosing party's request, the recipient shall cease use of Confidential Information and return or destroy it.

- III. Use of Confidential Information.** A party hereunder receiving Confidential Information shall use such Confidential Information solely for the purposes of, as applicable to the recipient, understanding current business activities of a party, soliciting a proposal for certain information technology services, responding to such proposal solicitation, reviewing solicitation responses, tendering a bid, or discussions or negotiations related to such solicitation, proposal, or bid.
- IV. Protection of Confidential Information.** Each party shall not disclose the Confidential Information of the other party to any third party. The recipient shall protect the Confidential Information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination or publication of the Confidential Information as the recipient uses to protect its own confidential information of a like nature. A recipient shall restrict disclosure of Confidential Information to its employees, provided that such employees (i) have a need to know, and (ii) are bound by obligations of confidentiality equally as restrictive as the terms of this Agreement.
- V. Exclusions.** This Agreement imposes no obligation upon the recipient with respect to Confidential Information which: (a) was in the recipient's possession before receipt from the disclosing party; (b) is or becomes a matter of public knowledge through no fault of the recipient; (c) is rightfully received by the recipient from a third party without a duty of confidentiality; (d) is disclosed by the disclosing party to a third party without a duty of confidentiality on the third party; (e) is independently developed by the recipient; (f) is disclosed under operation of law; or (g) is disclosed by the recipient with the disclosing party's prior written approval.
- VI. Miscellaneous.** Neither party to this Agreement shall acquire any intellectual property rights nor any other rights under this Agreement except the limited right to use as set forth in this Agreement. This Agreement does not prevent either Party from competing with one another for work or clients unless the parties specifically agree otherwise, in writing, as to a specific client. Each disclosing party warrants and represents that the Confidential Information and other information provided which is necessary to the purposes described hereunder, are true and correct to the best of the disclosing party's knowledge and belief. Nothing in this Agreement shall be construed to preclude either party from developing, using, marketing, licensing, and/or selling any software or other material that is developed without reference to the Confidential Information.
- VII. Export Administration.** Each party to this Agreement agrees to comply fully with all relevant export laws and regulations of the United States and other countries to assure that no Confidential Information or any portion thereof is exported, directly or indirectly, in violation of such laws.
- VIII. No Obligation to Purchase or Offer Products or Services.** Neither party has an obligation under this Agreement to purchase or otherwise acquire any service or item from

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

the other party. Neither party has an obligation under this Agreement to commercially offer any products using or incorporating the Confidential Information. The disclosing party may, at its sole discretion, offer such products commercially and may modify them or discontinue such offerings at any time.

IX. General. The parties do not intend that any agency or partnership relationship be created between them by this Agreement. This Agreement sets forth the entire agreement with respect to the Confidential Information disclosed herein and supersedes all prior or contemporaneous agreements concerning such Confidential Information, whether written or oral. All additions or modifications to this Agreement must be made in writing and must be signed by both parties. This Agreement and all matters arising out of or relating to this Agreement shall be governed by the laws of the State of West Virginia. The parties agree that the information provided as allowed by this Agreement will not contain any proprietary technical or confidential contractual information, or any financial information related to the relationship between Alpha and its partners. As a result, damages will not be included as a remedy.

The undersigned authorized representatives of each party have agreed to be legally bound by the terms of this Agreement as of the Effective Date shown above.

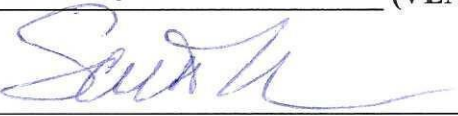
WEST VIRGINIA LOTTERY

By: _____

Name: _____

Title: _____

Advizex Technologies, LLC _____ **(VENDOR)**

By:  _____ 3/27/2024

Name: Scott Hess

Title: Proposal Desk Manager

APPENDIX D. REDACTED SAMPLE CYBERSECURITY REPORT

A redacted Cybersecurity report has been included with this submission for your review. This document is named:

- Sample Redacted Client Cyber Security Testing v1.0 - Advizex v1_0.pdf

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

XTEND ENDORSEMENT FOR TECHNOLOGY

This endorsement modifies insurance provided under the following:

COMMERCIAL GENERAL LIABILITY COVERAGE PART

GENERAL DESCRIPTION OF COVERAGE – This endorsement broadens coverage. However, coverage for any injury, damage or medical expenses described in any of the provisions of this endorsement may be excluded or limited by another endorsement to this Coverage Part, and these coverage broadening provisions do not apply to the extent that coverage is excluded or limited by such an endorsement. The following listing is a general coverage description only. Read all the provisions of this endorsement and the rest of your policy carefully to determine rights, duties, and what is and is not covered.

- | | |
|---|---|
| <ul style="list-style-type: none"> A. Non-Owned Watercraft – 75 Feet Long Or Less B. Who Is An Insured – Unnamed Subsidiaries C. Who Is An Insured – Employees – Supervisory Positions D. Who Is An Insured – Newly Acquired Or Formed Limited Liability Companies E. Who Is An Insured – Liability For Conduct Of Unnamed Partnerships Or Joint Ventures F. Blanket Additional Insured – Persons Or Organizations For Your Ongoing Operations As Required By Written Contract Or Agreement G. Blanket Additional Insured – Broad Form Vendors H. Blanket Additional Insured – Controlling Interest | <ul style="list-style-type: none"> I. Blanket Additional Insured – Mortgagees, Assignees, Successors Or Receivers J. Blanket Additional Insured – Governmental Entities – Permits Or Authorizations Relating To Premises K. Blanket Additional Insured – Governmental Entities – Permits Or Authorizations Relating To Operations L. Medical Payments – Increased Limit M. Blanket Waiver Of Subrogation N. Contractual Liability – Railroads O. Damage To Premises Rented To You |
|---|---|

PROVISIONS

A. NON-OWNED WATERCRAFT – 75 FEET LONG OR LESS

1. The following replaces Paragraph (2) of Exclusion **g.**, **Aircraft, Auto Or Watercraft**, in Paragraph 2. of **SECTION I – COVERAGES – COVERAGE A – BODILY INJURY AND PROPERTY DAMAGE LIABILITY**:

(2) A watercraft you do not own that is:

- (a) 75 feet long or less; and
- (b) Not being used to carry any person or property for a charge;

2. The following replaces Paragraph 2.e. of **SECTION II – WHO IS AN INSURED**:

e. Any person or organization that, with your express or implied consent, either uses or

is responsible for the use of a watercraft that you do not own that is:

- (1) 75 feet long or less; and
- (2) Not being used to carry any person or property for a charge.

B. WHO IS AN INSURED – UNNAMED SUBSIDIARIES

The following is added to **SECTION II – WHO IS AN INSURED**:

Any of your subsidiaries, other than a partnership or joint venture, that is not shown as a Named Insured in the Declarations is a Named Insured if:

- a. You are the sole owner of, or maintain an ownership interest of more than 50% in, such subsidiary on the first day of the policy period; and
- b. Such subsidiary is not an insured under similar other insurance.

COMMERCIAL GENERAL LIABILITY

No such subsidiary is an insured for "bodily injury" or "property damage" that occurred, or "personal and advertising injury" caused by an offense committed:

- a. Before you maintained an ownership interest of more than 50% in such subsidiary; or
- b. After the date, if any, during the policy period that you no longer maintain an ownership interest of more than 50% in such subsidiary.

For purposes of Paragraph 1. of Section II – Who Is An Insured, each such subsidiary will be deemed to be designated in the Declarations as:

- a. A limited liability company;
- b. An organization other than a partnership, joint venture or limited liability company; or
- c. A trust;

as indicated in its name or the documents that govern its structure.

C. WHO IS AN INSURED – EMPLOYEES – SUPERVISORY POSITIONS

The following is added to Paragraph 2.a.(1) of SECTION II – WHO IS AN INSURED:

Paragraphs (1)(a), (b) and (c) above do not apply to "bodily injury" to a co-"employee" while in the course of the co-"employee's" employment by you arising out of work by any of your "employees" who hold a supervisory position.

D. WHO IS AN INSURED – NEWLY ACQUIRED OR FORMED LIMITED LIABILITY COMPANIES

The following replaces Paragraph 3. of SECTION II – WHO IS AN INSURED:

3. Any organization you newly acquire or form, other than a partnership or joint venture, and of which you are the sole owner or in which you maintain an ownership interest of more than 50%, will qualify as a Named Insured if there is no other similar insurance available to that organization. However:

- a. Coverage under this provision is afforded only:
 - (1) Until the 180th day after you acquire or form the organization or the end of the policy period, whichever is earlier, if you do not report such organization in writing to us within 180 days after you acquire or form it; or
 - (2) Until the end of the policy period, when that date is later than 180 days after you acquire or form such organization, if you report such

organization in writing to us within 180 days after you acquire or form it;

- b. Coverage A does not apply to "bodily injury" or "property damage" that occurred before you acquired or formed the organization; and
- c. Coverage B does not apply to "personal and advertising injury" arising out of an offense committed before you acquired or formed the organization.

For the purposes of Paragraph 1. of Section II – Who Is An Insured, each such organization will be deemed to be designated in the Declarations as:

- a. A limited liability company;
- b. An organization, other than a partnership, joint venture or limited liability company; or
- c. A trust;

as indicated in its name or the documents that govern its structure.

E. WHO IS AN INSURED – LIABILITY FOR CONDUCT OF UNNAMED PARTNERSHIPS OR JOINT VENTURES

The following replaces the last paragraph of SECTION II – WHO IS AN INSURED:

No person or organization is an insured with respect to the conduct of any current or past partnership or joint venture that is not shown as a Named Insured in the Declarations. This paragraph does not apply to any such partnership or joint venture that otherwise qualifies as an insured under Section II – Who Is An Insured.

F. BLANKET ADDITIONAL INSURED – PERSONS OR ORGANIZATIONS FOR YOUR ONGOING OPERATIONS AS REQUIRED BY WRITTEN CONTRACT OR AGREEMENT

The following is added to SECTION II – WHO IS AN INSURED:

Any person or organization that is not otherwise an insured under this Coverage Part and that you have agreed in a written contract or agreement to include as an additional insured on this Coverage Part is an insured, but only with respect to liability for "bodily injury" or "property damage" that:

- a. Occurs subsequent to the signing of that contract or agreement; and
- b. Is caused, in whole or in part, by your acts or omissions in the performance of your ongoing operations to which that contract or

agreement applies or the acts or omissions of any person or organization performing such operations on your behalf.

The limits of insurance provided to such insured will be the minimum limits that you agreed to provide in the written contract or agreement, or the limits shown in the Declarations, whichever are less.

G. BLANKET ADDITIONAL INSURED – BROAD FORM VENDORS

The following is added to **SECTION II – WHO IS AN INSURED:**

Any person or organization that is a vendor and that you have agreed in a written contract or agreement to include as an additional insured on this Coverage Part is an insured, but only with respect to liability for "bodily injury" or "property damage" that:

- a. Occurs subsequent to the signing of that contract or agreement; and
- b. Arises out of "your products" that are distributed or sold in the regular course of such vendor's business.

The insurance provided to such vendor is subject to the following provisions:

- a. The limits of insurance provided to such vendor will be the minimum limits that you agreed to provide in the written contract or agreement, or the limits shown in the Declarations, whichever are less.
- b. The insurance provided to such vendor does not apply to:
 - (1) Any express warranty not authorized by you or any distribution or sale for a purpose not authorized by you;
 - (2) Any change in "your products" made by such vendor;
 - (3) Repackaging, unless unpacked solely for the purpose of inspection, demonstration, testing, or the substitution of parts under instructions from the manufacturer, and then repackaged in the original container;
 - (4) Any failure to make such inspections, adjustments, tests or servicing as vendors agree to perform or normally undertake to perform in the regular course of business, in connection with the distribution or sale of "your products";
 - (5) Demonstration, installation, servicing or repair operations, except such operations

performed at such vendor's premises in connection with the sale of "your products"; or

- (6) "Your products" that, after distribution or sale by you, have been labeled or relabeled or used as a container, part or ingredient of any other thing or substance by or on behalf of such vendor.

Coverage under this provision does not apply to:

- a. Any person or organization from whom you have acquired "your products", or any ingredient, part or container entering into, accompanying or containing such products; or
- b. Any vendor for which coverage as an additional insured specifically is scheduled by endorsement.

H. BLANKET ADDITIONAL INSURED – CONTROLLING INTEREST

- 1. The following is added to **SECTION II – WHO IS AN INSURED:**

Any person or organization that has financial control of you is an insured with respect to liability for "bodily injury", "property damage" or "personal and advertising injury" that arises out of:

- a. Such financial control; or
- b. Such person's or organization's ownership, maintenance or use of premises leased to or occupied by you.

The insurance provided to such person or organization does not apply to structural alterations, new construction or demolition operations performed by or on behalf of such person or organization.

- 2. The following is added to Paragraph 4. of **SECTION II – WHO IS AN INSURED:**

This paragraph does not apply to any premises owner, manager or lessor that has financial control of you.

I. BLANKET ADDITIONAL INSURED – MORTGAGEES, ASSIGNEES, SUCCESSORS OR RECEIVERS

The following is added to **SECTION II – WHO IS AN INSURED:**

Any person or organization that is a mortgagee, assignee, successor or receiver and that you have agreed in a written contract or agreement to include as an additional insured on this Coverage Part is an insured, but only with respect to its

COMMERCIAL GENERAL LIABILITY

liability as mortgagee, assignee, successor or receiver for "bodily injury", "property damage" or "personal and advertising injury" that:

- a. Is "bodily injury" or "property damage" that occurs, or is "personal and advertising injury" caused by an offense that is committed, subsequent to the signing of that contract or agreement; and
- b. Arises out of the ownership, maintenance or use of the premises for which that mortgagee, assignee, successor or receiver is required under that contract or agreement to be included as an additional insured on this Coverage Part.

The insurance provided to such mortgagee, assignee, successor or receiver is subject to the following provisions:

- a. The limits of insurance provided to such mortgagee, assignee, successor or receiver will be the minimum limits that you agreed to provide in the written contract or agreement, or the limits shown in the Declarations, whichever are less.
- b. The insurance provided to such person or organization does not apply to:
 - (1) Any "bodily injury" or "property damage" that occurs, or any "personal and advertising injury" caused by an offense that is committed, after such contract or agreement is no longer in effect; or
 - (2) Any "bodily injury", "property damage" or "personal and advertising injury" arising out of any structural alterations, new construction or demolition operations performed by or on behalf of such mortgagee, assignee, successor or receiver.

J. BLANKET ADDITIONAL INSURED – GOVERNMENTAL ENTITIES – PERMITS OR AUTHORIZATIONS RELATING TO PREMISES

The following is added to **SECTION II – WHO IS AN INSURED**:

Any governmental entity that has issued a permit or authorization with respect to premises owned or occupied by, or rented or loaned to, you and that you are required by any ordinance, law, building code or written contract or agreement to include as an additional insured on this Coverage Part is an insured, but only with respect to liability for "bodily injury", "property damage" or "personal and advertising injury" arising out of the existence, ownership, use, maintenance, repair,

construction, erection or removal of any of the following for which that governmental entity has issued such permit or authorization: advertising signs, awnings, canopies, cellar entrances, coal holes, driveways, manholes, marquees, hoist away openings, sidewalk vaults, elevators, street banners or decorations.

K. BLANKET ADDITIONAL INSURED – GOVERNMENTAL ENTITIES – PERMITS OR AUTHORIZATIONS RELATING TO OPERATIONS

The following is added to **SECTION II – WHO IS AN INSURED**:

Any governmental entity that has issued a permit or authorization with respect to operations performed by you or on your behalf and that you are required by any ordinance, law, building code or written contract or agreement to include as an additional insured on this Coverage Part is an insured, but only with respect to liability for "bodily injury", "property damage" or "personal and advertising injury" arising out of such operations.

The insurance provided to such governmental entity does not apply to:

- a. Any "bodily injury", "property damage" or "personal and advertising injury" arising out of operations performed for the governmental entity; or
- b. Any "bodily injury" or "property damage" included in the "products-completed operations hazard".

L. MEDICAL PAYMENTS – INCREASED LIMIT

The following replaces Paragraph 7. of **SECTION III – LIMITS OF INSURANCE**:

7. Subject to Paragraph 5. above, the Medical Expense Limit is the most we will pay under Coverage C for all medical expenses because of "bodily injury" sustained by any one person, and will be the higher of:
 - a. \$10,000; or
 - b. The amount shown in the Declarations of this Coverage Part for Medical Expense Limit.

M. BLANKET WAIVER OF SUBROGATION

The following is added to Paragraph 8., **Transfer Of Rights Of Recovery Against Others To Us**, of **SECTION IV – COMMERCIAL GENERAL LIABILITY CONDITIONS**:

If the insured has agreed in a contract or agreement to waive that insured's right of recovery against any person or organization, we

waive our right of recovery against such person or organization, but only for payments we make because of:

- a. "Bodily injury" or "property damage" that occurs; or
- b. "Personal and advertising injury" caused by an offense that is committed;

subsequent to the execution of the contract or agreement.

N. CONTRACTUAL LIABILITY – RAILROADS

1. The following replaces Paragraph **c.** of the definition of "insured contract" in the **DEFINITIONS** Section:

- c. Any easement or license agreement;

2. Paragraph **f.(1)** of the definition of "insured contract" in the **DEFINITIONS** Section is deleted.

O. DAMAGE TO PREMISES RENTED TO YOU

The following replaces the definition of "premises damage" in the **DEFINITIONS** Section:

"Premises damage" means "property damage" to:

- a. Any premises while rented to you or temporarily occupied by you with permission of the owner; or
- b. The contents of any premises while such premises is rented to you, if you rent such premises for a period of seven or fewer consecutive days.

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

SHORT TERM HIRED AUTO – ADDITIONAL INSURED AND LOSS PAYEE

This endorsement modifies insurance provided under the following:

- AUTO DEALERS COVERAGE FORM
- BUSINESS AUTO COVERAGE FORM
- MOTOR CARRIER COVERAGE FORM

SCHEDULE

Additional Insured (Lessor):

Any lessor of a "leased auto" under a leasing or rental agreement of less than 6 months.

Designation Or Description Of "Leased Autos":

Any "leased auto" under a leasing or rental agreement of less than 6 months.

A. Coverage

1. Any "leased auto" designated or described in the Schedule will be considered a covered "auto" you own and not a covered "auto" you hire or borrow for **Covered Autos Liability Coverage**.
2. For a "leased auto" designated or described in the Schedule, the **Who Is An Insured** provision under **Covered Autos Liability Coverage** is changed to include as an "insured" the lessor of such "leased auto". However, the lessor is an "insured" only for "bodily injury" or "property damage" resulting from the acts or omissions by:
 - a. You;
 - b. Any of your "employees" or agents; or
 - c. Any person, except the lessor or any "employee" or agent of the lessor,

operating a "leased auto" with the permission of any of the above.

3. Coverage for any "leased auto" described in the Schedule applies until the end of the policy period shown in the Declarations or when the lessor or his or her agent takes possession of the "leased auto", whichever occurs first.

B. Loss Payable Clause

1. We will pay, as interest may appear, you and the lessor, if your policy includes Hired Auto Physical Damage Coverage, for "loss" to a "leased auto".
2. The insurance covers the interest of the lessor unless the "loss" results from fraudulent acts or omissions on your part.
3. If we make any payment to the lessor, we will obtain his or her rights against any other party.

C. The lessor is not liable for payment of your premiums.

D. Additional Definition

As used in this endorsement:

"Leased auto" means an "auto" leased or rented to you, including any substitute, replacement or extra "auto" needed to meet seasonal or other needs, under a leasing or rental agreement that requires you to provide direct primary insurance for the lessor.



THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

**WAIVER OF OUR RIGHT TO RECOVER
FROM OTHERS ENDORSEMENT**

Policy Number: 45 WEC AA7S8F

Endorsement Number:

Effective Date: 11/01/23

Effective hour is the same as stated on the Information Page of the policy.

Named Insured and Address: Rolta AdvizeX Technologies LLC
6480 ROCKSIDE WOODS BLVD S
INDEPENDENCE OH 44131

We have the right to recover our payments from anyone liable for an injury covered by this policy. We will not enforce our right against the person or organization named in the Schedule.

This agreement shall not operate directly or indirectly to benefit anyone not named in the Schedule.

SCHEDULE

Any person or organization for whom you are required by contract or agreement to obtain this waiver from us. Endorsement is not applicable in KY, NH, NJ or for any MO construction risk

Countersigned by _____
Authorized Representative