STATE OF TEXAS §
§
COUNTY OF FORT BEND §

ADDENDUM TO REDTEAM COLLABORATIVE LLC DBA REDTEAM SECURITY'S AGREEMENT FOR SECURITY ENGAGEMENT SERVICES

THIS ADDENDUM ("Addendum") is entered into by and between Fort Bend County, ("County"), a body corporate and politic under the laws of the State of Texas, and RedTeam Collaborative LLC dba RedTeam Security, ("RedTeam Security"), a company authorized to conduct business in the State of Texas (hereinafter collectively referred to as the "parties").

WHEREAS, subject to the changes herein, the parties have executed and accepted RedTeam Security's Engagement # 8303, (the "Agreement"), attached hereto as Exhibit "A" and incorporated fully by reference, for the purchase of specified professional consulting Security Engagement Services (the "Services"); and

WHEREAS, County desires to hire RedTeam Security to provide certain professional consulting Services as will be more specifically described in this Agreement; and

WHEREAS, RedTeam's Services concern Network Penetration testing, Social Engineering and Advanced Penetration testing on the County's Network Infrastructure, including conducting vulnerability analyses for County; and

WHEREAS, County has determined that this Agreement is for personal or professional services and therefore exempt from competitive bidding under Chapter 262 of the Texas Local Government Code; and

WHEREAS, RedTeam Security represents that it is qualified and desires to perform such Services; and

NOW, THEREFORE, in consideration of the mutual covenants and conditions set forth below, the parties agree as follows:

AGREEMENT

1. **Scope of Services.** Subject to this Addendum, RedTeam Security will render Services to County as described in Exhibit A. The Services shall be scheduled at a time that is mutually agreeable between the parties but without reasonable delay. All performance of the Scope of Services by RedTeam Security including any changes in the Scope of Services and revision of work satisfactorily performed will be performed only when approved in advance and authorized by County.

2. **Payment; Non-appropriation; Taxes.** Payment shall be made by County within thirty (30) days of receipt of invoice. If County disputes charges related to the invoice submitted by RedTeam Security, County shall notify RedTeam Security no later than twenty-one (21) days after the date County receives the invoice. It is specifically understood and agreed that in the event no funds or insufficient funds are appropriated by Fort Bend County under this

Agreement, Fort Bend County shall notify all necessary parties that this Agreement shall thereafter terminate and be null and void on the last day of the fiscal period for which appropriations were made without penalty, liability or expense to Fort Bend County. County is a body corporate and politic under the laws of the State of Texas and claims exemption from sales and use taxes. A copy of a tax-exempt certificate will be furnished upon request. Interest resulting from late payments by County shall be governed by Chapter 2251, TEXAS GOVERNMENT CODE. County reserves the right to withhold payment pending verification of satisfactory work performed.

3. **Limit of Appropriation.** RedTeam Security clearly understands and agrees, such understanding and agreement being of the absolute essence of this Agreement, that County shall have available the total maximum sum of Seventy-Nine Thousand, Eight Hundred Fifteen and 00/100 dollars ($79,815.00), specifically allocated to fully discharge any and all liabilities County may incur. RedTeam Security does further understand and agree, said understanding and agreement also being of the absolute essence of this Agreement, that the total maximum compensation that RedTeam Security may become entitled to and the total maximum sum that County may become liable to pay to RedTeam Security shall not under any conditions, circumstances, or interpretations thereof exceed Seventy-Nine Thousand, Eight Hundred Fifteen and 00/100 dollars ($79,815.00). In no event will the amount paid by the County for all services under this Agreement exceed this Limit of Appropriation without an amendment executed by the parties.

4. **Public Information Act and Open Meetings Act.** RedTeam Security expressly acknowledges that County is subject to the Texas Public Information Act, TEX. GOV'T CODE ANN. §§ 552.001 *et seq.*, as amended, and notwithstanding any provision in the Agreement to the contrary, County will make any information related to the Agreement, or otherwise, available to third parties in accordance with the Texas Public Information Act. Any proprietary or confidential information marked as such provided to County by RedTeam Security shall not be disclosed to any third party, except as directed by the Texas Attorney General in response to a request for such under the Texas Public Information Act, which provides for notice to the owner of such marked information and the opportunity for the owner of such information to notify the Attorney General of the reasons why such information should not be disclosed. The terms and conditions of the Agreement are not proprietary or confidential information.

   RedTeam Security expressly acknowledges that County is subject to the Texas Open Meetings Act, TEX. GOV'T CODE ANN. §§ 551.001 *et seq.*, as amended, and notwithstanding any provision in the Agreement to the contrary, County will comply with the provisions of the Texas Open Meetings Act in relation to the Agreement.

5. **Indemnity.** The parties agree that under the Constitution and laws of the State of Texas, County cannot enter into an agreement whereby County agrees to indemnify or hold harmless another party; therefore, all references of any kind to County defending, indemnifying, holding or saving harmless RedTeam Security or any other party for any reason are hereby deleted. RedTeam Security shall indemnify and defend County against all losses, liabilities, claims, causes of action, and other expenses, including reasonable attorney's fees, arising from activities of RedTeam Security, its agents, servants or employees, performed

under this agreement that result from the negligent act, error, or omission of RedTeam Security or any of RedTeam Security's agents, servants or employees.

6. **Applicable Law; Arbitration; Attorney Fees.** The laws of the State of Texas govern all disputes arising out of or relating to this Agreement. The parties hereto acknowledge that venue is proper in Fort Bend County, Texas, for all legal actions or proceedings arising out of or relating to this Agreement and waive the right to sue or be sued elsewhere. Nothing in the Agreement shall be construed to waive the County's sovereign immunity. County does not agree to submit disputes arising out of the Agreement to binding arbitration. Therefore, any references to binding arbitration or the waiver of a right to litigate a dispute are hereby deleted. County does not agree to pay any and/or all attorney fees incurred by RedTeam Security in any way associated with the Agreement.

7. **Certain State Law Requirements for Contracts.** The contents of this Section are required by Texas Law and are included by County regardless of content. For purposes of Sections 2252.152, 2271.002, and 2274.002, Texas Government Code, as amended, RedTeam Security hereby verifies that RedTeam Security and any parent company, wholly owned subsidiary, majority-owned subsidiary, and affiliate:
   A. Unless affirmatively declared by the United States government to be excluded from its federal sanctions regime relating to Sudan or Iran or any federal sanctions regime relating to a foreign terrorist organization, is not identified on a list prepared and maintained by the Texas Comptroller of Public Accounts under Section 806.051, 807.051, or 2252.153 of the Texas Government Code.
   B. If employing ten (10) or more full-time employees and this Agreement has a value of $100,000.00 or more, RedTeam Security does not boycott Israel and is authorized to agree in such contracts not to boycott Israel during the term of such contracts. "Boycott Israel" has the meaning provided in § 808.001 of the Texas Government Code.
   C. If employing ten (10) or more full-time employees and this Agreement has a value of $100,000.00 or more, RedTeam Security does not boycott energy companies and is authorized to agree in such contracts not to boycott energy companies during the term of such contracts. "Boycott energy company" has the meaning provided in § 809.001 of the Texas Government Code.
   D. If employing ten (10) or more full-time employees and this Agreement has a value of $100,000.00 or more, RedTeam Security does not have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association and is authorized to agree in such contracts not to discriminate against a firearm entity or firearm trade association during the term of such contracts. "Discriminate against a firearm entity or firearm trade association" has the meaning provided in § 2274.001(3) of the Texas Government Code. "Firearm entity" and "firearm trade association" have the meanings provided in § 2274.001(6) and (7) of the Texas Government Code.

8. **Modifications and Waivers**. The parties may not amend or waive this Agreement, except by a written agreement executed by both parties. No failure or delay in exercising any right or remedy or requiring the satisfaction of any condition under this Agreement, and no course of dealing between the parties, operates as a waiver or estoppel of any right, remedy, or condition. The rights and remedies of the parties set forth in this Agreement are not exclusive

of, but are cumulative to, any rights or remedies now or subsequently existing at law, in equity, or by statute. No other provisions to this Agreement apply except for the terms which appear in this Addendum and the attached Exhibits.

9. **Human Trafficking**. BY ACCEPTANCE OF CONTRACT, REDTEAM SECURITY ACKNOWLEDGES THAT FORT BEND COUNTY IS OPPOSED TO HUMAN TRAFFICKING AND THAT NO COUNTY FUNDS WILL BE USED IN SUPPORT OF SERVICES OR ACTIVITIES THAT VIOLATE HUMAN TRAFFICKING LAWS.
10. **Use of Customer Name**. RedTeam Security may use County's name without County's prior written consent only in any of RedTeam Security's customer lists, any other use must be approved in advance by County.

11. **Product Assurance.** RedTeam Security represents and warrants that its hardware, software and any related systems and/or services related to its software and/or hardware (collectively, the "Product") furnished by RedTeam Security to County will not infringe upon or violate any patent, copyright, trademark, trade secret, or any other proprietary right of any third party. RedTeam Security will, at its expense, defend any suit brought against County and will indemnify County against an award of damages and costs (including reasonable attorney fees, court costs and appeals), made against County by settlement or final judgment of a court that is based on a claim that the use of RedTeam Security's Product infringes an intellectual property right of a third party. Such defense and indemnity shall survive termination or expiration of the Agreement and RedTeam Security's liability for the above is not limited by any limitation of liability clauses that may appear in any document executed by the parties.

12. **Performance Warranty.** RedTeam Security warrants to County that RedTeam Security has the skill and knowledge ordinarily possessed by well-informed members of its trade or profession practicing in the greater Houston metropolitan area and RedTeam Security will apply that skill and knowledge with care and diligence to ensure that the services provided hereunder will be performed and delivered in accordance with the highest professional standards.

    RedTeam Security warrants to County that the Services will be free from material errors and will materially conform to all requirements and specifications contained in the attached Exhibits.

13. **Conflict.** In the event there is a conflict between this Addendum and the Agreement, this Addendum controls to the extent of the conflict.

14. **Understanding, Fair Construction.** By execution of this Addendum, the parties acknowledge that they have read and understood each provision, term and obligation contained in this Addendum. This Addendum, although drawn by one party, shall be construed fairly and reasonably and not more strictly against the drafting party than the nondrafting party.

15. **Inspection of Books and Records**. RedTeam Security will permit County, or any duly authorized agent of County, to inspect and examine the books and records of RedTeam Security for the purpose of verifying the amount of work performed under the Scope of

Services. County's right to inspect survives the termination of this Agreement for a period of four (4) years.

16. **Captions**. The section captions used in this Agreement are for convenience of reference only and do not affect the interpretation or construction of this Agreement.

17. **Electronic and Digital Signatures.** The parties to this Agreement agree that any electronic and/or digital signatures of the parties included in this Agreement are intended to authenticate this writing and to have the same force and effect as the use of manual signatures.

18. **County Data**. Nothing in this Agreement will be construed to waive the requirements of § 205.009 of the Texas Local Government Code.

19. **Assignment and Delegation**.

    19.1. Neither party may assign any of its rights under this Agreement, except with the prior written consent of the other party. That party shall not unreasonably withhold its consent. All assignments of rights are prohibited under this subsection, whether they are voluntarily or involuntarily, by merger, consolidation, dissolution, operation of law, or any other manner.

    19.2. Neither party may delegate any performance under this Agreement.

    19.3. Any purported assignment of rights or delegation of performance in violation of this Section is void.

    19.4. Nothing herein shall be construed as creating any personal liability on the part of any officer or agent of the County.

20. **Successors and Assigns**. County and RedTeam Security bind themselves and their successors, executors, administrators and assigns to the other party of this Agreement and to the successors, executors, administrators and assigns of the other party, in respect to all covenants of this Agreement.

21. **Ownership and Reuse of Documents**. All documents, data, reports, research, graphic presentation materials, etc., developed by RedTeam Security as a part of its work under this Agreement, shall become the property of County upon completion of this Agreement, or in the event of termination or cancellation thereof, at the time of payment under § 2 for work performed. RedTeam Security shall promptly furnish all such data and material to County on request.

22. **Personnel**. RedTeam Security represents that it presently has, or is able to obtain, adequate qualified personnel in its employment for the timely performance of the Services required under this Agreement and that RedTeam Security shall furnish and maintain, at its own expense, adequate and sufficient personnel, in the opinion of County, to perform the Services when and as required and without delays.

All employees of RedTeam Security shall have such knowledge and experience as will enable them to perform the duties assigned to them. Any employee of RedTeam Security or agent of RedTeam Security who, in the opinion of County, is incompetent or by his conduct becomes detrimental to providing Services pursuant to this Agreement shall, upon request of County, immediately be removed from association with the Services required under this Agreement.

When performing Services for the County, RedTeam Security shall comply with, and ensure that all RedTeam Security Personnel comply with, all rules, regulations and policies of County that are communicated to RedTeam Security in writing, including security procedures concerning systems and data and remote access thereto, building security procedures, including the restriction of access by County to certain areas of its premises or systems for security reasons, and general health and safety practices and procedures.

23. **Compliance with Laws**. RedTeam Security shall comply with all federal, state, and local laws, statutes, ordinances, rules and regulations, and the orders and decrees of any courts or administrative bodies or tribunals in any matter affecting the performance of this Agreement, including, without limitation, Worker's Compensation laws, minimum and maximum salary and wage statutes and regulations, licensing laws and regulations. When required by County, RedTeam Security shall furnish County with certification of compliance with said laws, statutes, ordinances, rules, regulations, orders, and decrees above specified.

24. **Confidential Information.** RedTeam Security acknowledges that it and its employees or agents may, in the course of performing their responsibilities under this Agreement, be exposed to or acquire information that is confidential to County. Any and all information of any form obtained by RedTeam Security or its employees or agents from County in the performance of this Agreement shall be deemed to be confidential information of County ("Confidential Information"). Any reports or other documents or items (including software) that result from the use of the Confidential Information by RedTeam Security shall be treated with respect to confidentiality in the same manner as the Confidential Information. Confidential Information shall be deemed not to include information that (a) is or becomes (other than by disclosure by RedTeam Security) publicly known or is contained in a publicly available document; (b) is rightfully in RedTeam Security's possession without the obligation of nondisclosure prior to the time of its disclosure under this Agreement; or (c) is independently developed by employees or agents of RedTeam Security who can be shown to have had no access to the Confidential Information.

RedTeam Security agrees to hold Confidential Information in strict confidence, using at least the same degree of care that RedTeam Security uses in maintaining the confidentiality of its own confidential information, and not to copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than the provision of Services to County hereunder, and to advise each of its employees and agents of their obligations to keep Confidential Information confidential. RedTeam Security shall use its best efforts to assist County in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limitation

of the foregoing, RedTeam Security shall advise County immediately in the event RedTeam Security learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Agreement and RedTeam Security will at its expense cooperate with County in seeking injunctive or other equitable relief in the name of County or RedTeam Security against any such person. RedTeam Security agrees that, except as directed by County, RedTeam Security will not at any time during or after the term of this Agreement disclose, directly or indirectly, any Confidential Information to any person, and that upon termination of this Agreement or at County's request, RedTeam Security will promptly turn over to County all documents, papers, and other matter in RedTeam Security's possession which embody Confidential Information.

RedTeam Security acknowledges that a breach of this Section, including disclosure of any Confidential Information, or disclosure of other information that, at law or in equity, ought to remain confidential, will give rise to irreparable injury to County that is inadequately compensable in damages. Accordingly, County may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. RedTeam Security acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interest of County and are reasonable in scope and content.

RedTeam Security in providing all services hereunder agrees to abide by the provisions of any applicable Federal or State Data Privacy Act.

25. **Termination**.

25.1. Termination for Convenience. County may terminate this Agreement at any time upon thirty (30) days written notice.

25.2. Termination for Default. County may terminate the whole or any part of this Agreement for cause in the following circumstances:

(a). If RedTeam Security fails to timely perform services pursuant to this Agreement or any extension thereof granted by the County in writing;

(b). If RedTeam Security materially breaches any of the covenants or terms and conditions set forth in this Agreement or fails to perform any of the other provisions of this Agreement or so fails to make progress as to endanger performance of this Agreement in accordance with its terms, and in any of these circumstances does not cure such breach or failure to County's reasonable satisfaction within a period of ten (10) calendar days after receipt of notice from County specifying such breach or failure.

25.3. If, after termination, it is determined for any reason whatsoever that RedTeam Security was not in default, or that the default was excusable, the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of the County in accordance with § 25.1 above.

25.4. Upon termination of this Agreement, County shall compensate RedTeam Security in accordance with § 2, above, for those services which were provided under this Agreement prior to its termination and which have not been previously invoiced to County. RedTeam Security's final invoice for said services will be presented to and paid by County in the same manner set forth in § 2 above.

25.5. If County terminates this Agreement as provided in this Section, no fees of any type, other than fees due and payable at the Termination Date, shall thereafter be paid to RedTeam Security.

25.6. If County terminates this Agreement prior to the termination date, County shall not be subject to any early termination fee or other penalty.

25.7. Upon termination of this Agreement for any reason, if RedTeam Security has any property in its possession belonging to County, RedTeam Security will account for the same, and dispose of it or return it to the County in the manner the County directs.

26. **Independent Contractor**. In the performance of work or services hereunder, RedTeam Security shall be deemed an independent contractor, and any of its agents, employees, officers, or volunteers performing work required hereunder shall be deemed solely as employees of RedTeam Security or, where permitted, of its subcontractors. RedTeam Security and its agents, employees, officers, or volunteers shall not, by performing work pursuant to this Agreement, be deemed to be employees, agents, or servants of County and shall not be entitled to any of the privileges or benefits of County employment.

27. **Publicity**. Contact with citizens of Fort Bend County, media outlets, or governmental agencies shall be the sole responsibility of County. Under no circumstances whatsoever, shall RedTeam Security release any material or information developed or received in the performance of the Services hereunder without the express written permission of County, except where required to do so by law.

28. **Further Assurances**. Each party further agrees that it shall take any and all necessary steps and sign and execute any and all necessary documents or agreements required to implement the terms of the agreement of the parties contained in this contract, and each party agrees to refrain from taking any action, either expressly or impliedly, which would have the effect to prohibiting or hindering the performance of the other party to this Agreement.

29. **Third Party Beneficiaries**. This Agreement does not confer any enforceable rights or remedies upon any person other than the parties.

30. **Severability**. If any provision of this Agreement is determined to be invalid, illegal, or unenforceable, the remaining provisions remain in full force, if the essential terms and conditions of this Agreement for each party remain valid, binding, and enforceable.

31. **Dispute Resolution**.

31.1. The parties shall attempt in good faith to resolve promptly any dispute arising out of or relating to this Agreement by negotiation between the parties. In the event the dispute cannot be settled through negotiation, the parties agree to submit the dispute to non-binding mediation.

31.2. The party requesting mediation shall notify the other party in writing of the dispute desired to be mediated. If the parties are unable to resolve their differences within ten (10) days of the receipt of such notice, such dispute shall be submitted for mediation.

31.3. Each party shall be responsible for its own costs associated with the mediation.

31.4. The requirement to seek mediation shall be a condition required before filing an action at law or in equity, unless to do so would prevent either party from seeking relief in a court of law or equity under any applicable statute of limitations.

31.5. RedTeam Security acknowledges that County is subject to the requirements of the Texas Open Meetings Act, TEX. GOV'T CODE ANN. §§ 551.001 *et seq.*, as amended, and notwithstanding any provision in the Agreement to the contrary, the County will comply with the provisions of the Open Meetings Act.

32. **Grant Funding**. RedTeam Security understands that and acknowledges that this Agreement may be totally or partially funded with federal funds. RedTeam Security represents and warrants that it is and will remain in compliance with all applicable federal provisions, including those attached as Exhibit "B" attached hereto and incorporated herein for all purposes.

33. **Remote Access.** If RedTeam Security requires remote access to County Systems for support, installation, integrations, configurations, and/or maintenance, except as otherwise agreed by the parties and approved by the County's Information Technology Director in writing, the below requirements must be met before RedTeam Security is granted remote access to County Systems:
    A. RedTeam Security will adhere to the restricted and monitored channels that are provided by the County, or other technologies approved in advanced in writing by the County's Information Technology Security Manager or the Assistant Information Technology Manager.
    B. RedTeam Security will neither implement nor deploy a remote access solution which bypasses and/or is designed to bypass County provided or approved controls. RedTeam Security will not access County Systems via unauthorized methods.
    C. RedTeam Security's remote access to County Systems will only be requested and activated on as-needed basis and disabled when not in use.
    D. Remote access is restricted only to County Systems necessary for RedTeam Security to provide Services to County pursuant to this Agreement.

E. RedTeam Security will allow only its Workforce approved in advance by County to access County Systems. RedTeam Security will promptly notify County whenever an individual member of RedTeam Security's Workforce who has access to County Systems leaves its employ or no longer requires access to County Systems. RedTeam Security will keep a log of access when its Workforce remotely accesses County Systems. RedTeam Security will supply County with evidence of access logs concerning remote access to County Systems upon written request from County. Such access logs will be provided to County, within three business days from the date of County's request. These requests may be used to confirm compliance with these terms and/or to investigate a security incident.

F. If any member(s) of RedTeam Security's Workforce is provided with remote access to County Systems, then RedTeam Security's workforce will not remotely log-in to County Systems from a public internet access device (e.g., airport computer terminal, or Internet café). This is due to the possibility of sensitive information being monitored by video or computer surveillance in public areas.

G. Failure of RedTeam Security to comply with this Section may result in RedTeam Security and/or RedTeam Security's Workforce losing remote access to County Systems. County reserves the right at any time to disable remote access to protect County Systems.

H. For purposes of this Section, "Workforce" means employees, agents, subcontractors (where permitted), and/or other persons whose conduct, in the performance of work for RedTeam Security, is under the direct control of RedTeam Security, whether or not they are paid by RedTeam Security and who have direct or incidental access to County Systems.

I. For purposes of this Section, "Systems" means any: (i.) computer programs, including, but not limited to, software, firmware, application programs, operating systems, files and utilities; (ii.) supporting documentation for such computer programs, including, without limitation, input and output formats, program listings, narrative descriptions and operating instructions; (iii.) data and/or media; (iv.) equipment, hardware, servers, and/or devices; and/or (v.) network(s).

34. **Notices**.

34.1. Each party giving any notice or making any request, demand, or other communication (each, a "Notice") pursuant to this Agreement shall do so in writing and shall use one of the following methods of delivery, each of which, for purposes of this Agreement, is a writing: personal delivery, registered or certified mail (in each case, return receipt requested and postage prepaid), or nationally recognized overnight courier (with all fees prepaid).

34.2. Each party giving a Notice shall address the Notice to the receiving party at the address listed below or to another address designated by a party in a Notice pursuant to this Section:

County: Fort Bend County Information Technology Department
Attn: Information Technology Director

301 Jackson Street
Richmond, Texas 77469

With a copy to: Fort Bend County
Attn: County Judge
301 Jackson Street
Richmond, Texas 77469

Contractor: RedTeam Security
Attn: _____
Union Depot Building
214 4th Street, East Suite 140
Saint Paul, Minnesota 55101

34.3. A Notice is effective only if the party giving or making the Notice has complied with subsections 34.1 and 34.2 and if the addressee has received the Notice. A Notice is deemed received as follows:

34.3.1. If the Notice is delivered in person, or sent by registered or certified mail or a nationally recognized overnight courier, upon receipt as indicated by the date on the signed receipt.

34.3.2. If the addressee rejects or otherwise refuses to accept the Notice, or if the Notice cannot be delivered because of a change in address for which no Notice was given, then upon the rejection, refusal, or inability to deliver.

(Execution Page Follows)

(Remainder of Page Intentionally Left Blank)

IN WITNESS WHEREOF, this Addendum is signed, accepted, and agreed to by all parties by and through the parties or their agents or authorized representatives. All parties hereby acknowledge that they have read and understood this Addendum and the attachments and exhibits hereto. All parties further acknowledge that they have executed this legal document voluntarily and of their own free will. This Agreement is effective upon execution by both parties.

FORT BEND COUNTY

County Judge KP George

KP George, County Judge

12/14/2021

Date

ATTEST:

Laura Richard

Laura Richard, County Clerk

REVIEWED:

Robyn Doughtie

Information Technology Office

REDTEAM COLLABORATIVE LLC DBA REDTEAM SECURITY

Angie Dean Type text here

Authorized Agent – Signature

Angie Dean

Authorized Agent- Printed Name

Vice President of Sales

Title

12/3/2021

Date

AUDITOR'S CERTIFICATE

I hereby certify that funds in the amount of **$** 79,815.00 are available to pay the obligation of Fort Bend County within the foregoing Agreement.

Robert Ed Sturdivant, County Auditor

Exhibit A: RedTeam Security's Engagement # 8303; and
Exhibit B: Federal Clauses

Exhibit A

Exhibit A

RedTeam Security

Union Depot Building
214 4th St. E, Suite 140
Saint Paul, MN 55101
612-234-7848

info@redteamsecure
www.redteamsecure.com

Company Contact

Angie Dean

RedTeam Security™
THREAT PREVENTION EXPERTS

REDTEAM SECURITY ENGAGEMENT

RedTeam Security Engagement # 8303

Professional Information Security Services

Prepared for:

Fort Bend County

301 Jackson St
Richmond, Texas 77469

Date submitted:

September 16, 2021

Prepared by:

Angie Dean
angie@redteamsecure.com
612-245-1364

RedTeam Security™
THREAT PREVENTION EXPERTS

Union Depot Building
214 4th Street E., Suite 140
Saint Paul, Minnesota, 55101, USA
Phone: (612) 234-7848
Email: info@redteamsecure.com
Web: www.redteamsecure.com

September 16, 2021

Fort Bend County

301 Jackson St

Richmond, Texas 77469

Jahan,

Thank you for the opportunity to serve you!

This proposal documents our understanding of the project objectives and scope. It also describes our approach and our responsibilities. This proposal outlines the agreement between RedTeam Security and Fort Bend County with respect to the specific services we aim to provide to you and the pricing for those services.

Your organizational reputation is one of its most valuable assets. RedTeam Security's comprehensive portfolio of information security services aim to uncover hidden risks, vulnerabilities and compliance issues within your environment. As your security partner, finding and fixing is certainly a goal of any security assessment. But what's more, our consulting team can help your organization successfully identify and remediate vulnerabilities, thus increasing your security posture and ability to resist attacks and ensure compliance.

Once again, we humbly thank you for the opportunity.

Please let me know if you have any questions as you review our proposal.

Regards,

Jon Anderson

Jon Anderson
President
RedTeam Security

Comprehensive Service Offerings

Since 2008, RedTeam Security has been leading the pen testing industry with focused offensive security services including (but not limited to) the list below.

One of RedTeam's core strengths, as our name implies, is red team operations. Our red team operations are next-level engagements designed to be multi-blended and adversarial-based attack simulations against people, software, hardware, and facilities. During these engagements, we employ social engineering, application penetration testing, and network penetration testing simultaneously to achieve our objectives.

Penetration Testing	Social Engineering
Network Penetration Testing	Email Phishing
Web Application Penetration Testing	Telephone Phishing
Wireless Penetration Testing	Employee Awareness Training
Mobile Penetration Testing	Physical (On-site) Social Engineering
API Penetration Testing	
Azure Penetration Testing	**Advanced Penetration Testing**
AWS Penetration Testing	Red Teaming
Physical Penetration Testing	Advanced Adversary Simulation

Working with RedTeam Security

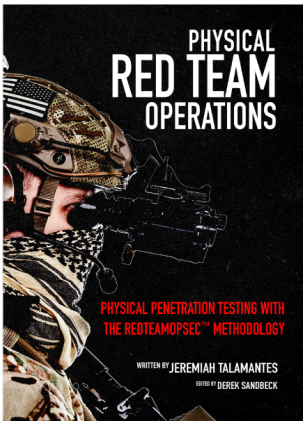
RedTeam works closely with each client to identify the greatest risk which will help set the goals for any engagement. RedTeam's reporting software and vulnerabilities libraries are exhaustive and are continually updated through daily research from their Pen Testing teams. The results of an engagement with RedTeam Security provide the real-world and actionable results needed to help our clients better understand their risk and how best to utilize limited budgets to improve their overall security posture.

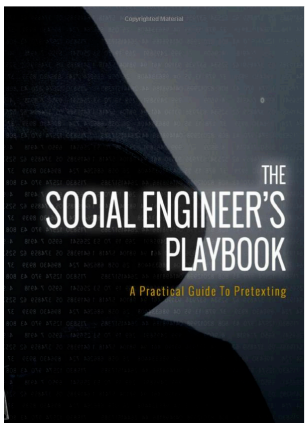
At RedTeam Security we offer more than our services and expertise. We want all our clients to feel that they have a security partner that they can reach out to at any time to discuss evolving security threats and related concerns. We appreciate the relationships we have developed over the years with our clients.

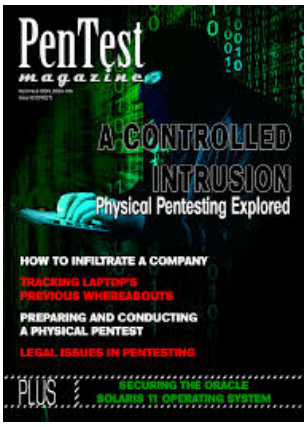
Our Team

Jeremiah Talamantes, Founder | RedTeam Security

Jeremiah Talamantes, the founder of RedTeam Security, has more than 20 years in the IT security industry. He holds a Master's degree in Information Security and Assurance and executive education from Notre Dame. He has held numerous security leadership roles as Chief Information Security Officer (CISO) and expert consultant to Fortune 50, 500, and SMBs. Jeremiah is adjunct faculty at Norwich University, College of Graduate Studies, and author of The Social Engineer's Playbook. His certifications include CISSP, CCENT, CCISO, CEH, and CHFI.







Jon Anderson, President | RedTeam Security

Jon Anderson is an entrepreneurial leader who develops award-winning sales and service teams. Before joining RedTeam Security, Jon held the roles of President and CEO of popular boutique technology companies, growing these companies into multi-million dollar organizations in less than three years. Jon's success stems from his ability to build innovative strategies that not only meet market demands but provide best-in-class customer responsiveness and overall client experiences.

REDTEAM SECURITY'S DISTINCT DIFFERENTIATORS

RedTeam's value is easily recognized in the following distinct differentiators:

Manual Intensive Testing

RedTeam security engineers utilize industry-standard automated tools while completing attacks on networks and systems during their red teaming engagements. While we recognize the time-saving features some of these tools offer, we proudly limit our use of these during engagements. At least 80% of our time is spent on manual exploits and scripts we have developed in-house or others spontaneously as needed during each engagement. Even the tool and code we plug into the network to initiate scanning is custom built with a repeatable process. RedTeam Security intends to launch this innovative device to the entire pen-testing community in August 2021.

As stated, while automated testing enables efficiency, it is only effective in providing efficiency during the initial phases of a penetration test. At RedTeam Security, we know that an effective and comprehensive penetration test can only be achieved through rigorous manual testing techniques.

Industry-Leading Tools

In order to perform a comprehensive real-world assessment, RedTeam Security utilizes commercial tools, internally developed tools, and the same tools that hackers use on each and every assessment. Our intent is to assess systems by simulating a real-world attack, and we leverage the many tools at our disposal to effectively carry out that task. See our comprehensive tools list here.

We employ tools from the following categories (not a complete list):

- Commercial tools (i.e., Nessus, Burp Suite Pro, AppScan, Nexpose, WebInspect)
- Open source/Hacker tools (i.e., Metasploit, BEeF, Kali Linux, OWASP Zap, nmap)
- RedTeam developed tools (i.e., nmapcli, Metasploit modules, PlugBot, various scripts)

Free Remediation Re-testing

Simply put, our objective is to help fix vulnerabilities, not just find them. As a result, remediation re-testing is always provided at no additional cost.

As your security partner, finding and fixing the vulnerabilities is the goal for any of security engagements with RedTeam. Our reports show everything RedTeam found, how we found it, and best practices to remediate the findings. Because our goal is to ensure your network is properly fixed once we have identified the issues, RedTeam provides remediation testing at no additional cost. When you and/or your team are ready for us to retest, just call us. Whether that's in two weeks or two months, we remain prepared to retested your remediated vulnerabilities and will get you scheduled when you feel prepared for your retest. We only ask that your retesting be within nine months of your report delivery.

Until you are ready for your retest, please use RedTeam as a resource. If you have questions that have come up during your remediation, whether they are related to your testing or not, call or email us, and we will get you the answers you need.

Extensive Industry Experience

RedTeam Security brings thought leadership, industry best practices, subject matter experts (SMEs) with deep technology experience to help the Fort Bend Countyimplement an effective Information Security and Risk Management program. Additionally, we bring methodologies, frameworks, and accelerators for the Fort Bend County to reduce risk and bring agility for the execution of residual risk mitigation. We further believe that RedTeam Security is the strong advisory partner to drive the successful definition and implementation of Fort Bend County Penetration Testing with the right processes and standard operating procedures aligning to organization policies. The foundation of our proposal is based on RedTeam Security's commitment to dedicate our experience, people, skills, as well as our leadership in a range of information security services for the Fort Bend County during the execution of services noted in this Solicitation.

RedTeam is a cybersecurity consulting firm seeking to provide customers with more than a report of their vulnerabilities. RedTeam is an ethical hacking firm in the purest sense. Our focus is on delivering deep-dive, highly advanced offensive security services that aim to provide maximum protection for businesses and the nation's most sensitive information.

Security Is Our Only Business

Many consulting firms offer information security services as a supplement to their business. RedTeam Security only focuses on providing deep-dive, highly advanced offensive security services that aim to provide maximum protection for businesses and the nation's most sensitive information. We are not a reseller or VAR of any kind. We are an ethical hacking services firm in the purest sense.

True Partnership

Our commitment to our clients shows. Should we utilize tactics that discover vulnerabilities either on the County's network or web applications, we provide all remediation re-testing at no additional charge, even if it takes more than a few re-tests and several months to fully remediate. Our goal is not only to find vulnerabilities but more importantly, to help the County fix them. All this from a firm that pours all of its time and resources into advancing its niche services for the protection and benefit of its prized clientele. This commitment will become evident during the remediation phases of this engagement as we work together to improve the County's overall security posture.

INDUSTRY SOURCE

Featured On

Our consultants are committed to being leaders through national TV appearances, documentaries, news article commentators, the publication of security research, authoring security books, being adjunct professors, and speaking at security conferences domestically and abroad. Our team is nationally recognized and has made numerous TV appearances to help organizations in the never-ending battle to divert bad actors from wrongfully accessing networks and related environments.

We remain consistently found in the top five Google results pages due to our long-standing ability to deliver quality results to our clients. Throughout the year, we regularly present our methodology to the pen testing community, and 1/3 of each pen tester's day is dedicated to ongoing research projects and collaborating with our extensive security network across the country.

Our regular communication with these security experts and members of industry professional associations are essential for acquiring the bleeding edge tools and techniques used to battle emerging security threats.

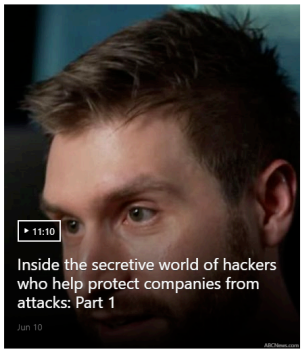
RedTeam Security has been a frequent cybersecurity contributor for news organizations such as ABC Nightline, Kare11, Darknet Diaries, CNN, Fox News, Tech Insider, Business Insider, and Yahoo News. These organizations consult with us for our expertise as a high-touch ethical hacking firm highly trained in a narrow field of cybersecurity. Our pen testing team is made up of former professors, software engineers, and network analysts. Our diverse backgrounds provide us with a unique edge in planning and executing our highly customized red team operations.

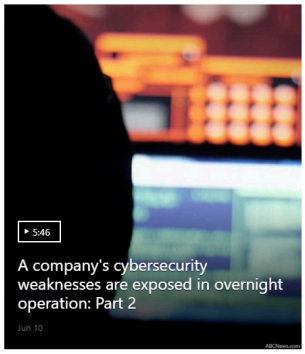
See RedTeam Security in Action

Business Insider

Business Insider rode along during a full-scope red team engagement on a power company that was compromised in less than 24 hours.

Watch Now





ABC Nightline

See our team in action as we attempt to break into two separate buildings with the hopes of uncovering security weaknesses.

Watch Now

Darknet Diaries

Join us from recon to execution as we take you on a big adventure of close encounters, and literal leaps of faith.

Listen to the Podcast

Channel 5 Eyewitness News Nightcast

Hear from our team as well as other industry experts talk about the rise of ransomware attacks across the country and what organizations can do to protect themselves.

Watch Now

TRUSTED BY THESE GREAT COMPANIES

At RedTeam Security, we are fortunate to work with a number of great organizations spanning various industries. Here are just a sample of the great companies that you may have heard of:

INDUSTRY CERTIFICATIONS

RedTeam Security consultants constantly work toward and achieve industry certifications relevant to the work they perform. To continually provide the quality security solutions our clients have come to expect, our team holds a number of industry certifications demonstrating high standards of proficiency.

RedTeam Security holds the following industry skills and certifications. Full resumes available upon request.

CompTIA PenTest+	CompTIA Security+	Certified Ethical Hacker (CEH)
Certified Information Systems Security Professional (CISSP)	Certified SonicWALL Security Professional (CSSP)	Cisco Certified Networking Associate (CCNA)
Cisco Certified Networking Associate Security (CCNA Security)	Cisco Certified Networking Associate (CCNA Routing & Switching)	Cisco Certified Networking Associate Cyber Ops (CCNA Cyber Ops)
Offensive Security Certified Professional (OSCP)	Offensive Security Wireless Pen Tester (OSWP)	Offensive Security Web Expert (OSWE)
Offensive Security Wireless Attacks (WiFu)	Evolve Security Certified Professional (ESCP)	Cisco Certified Cybersecurity Specialist
Penetration Testing with Kali Linux (PWK)	BlackOps Hacking, Master Level, SensePost	Dark Side Ops: Custom Penetration Testing
Adversary Tactics: Red Team Operations	Click Here For Ring0, Immunity Inc.	McAfee ePolicy Orchestrator (EPO)
GIAC Web Application Penetration Tester (GWAPT)	GIAC Certified Web Application Defender (GWEB)	GIAC Certified Incident Handler (GCIH)
GIAC Python Coder (GPYC)	GIAC Security Essentials (GSEC)	Microsoft Server 2016 70-740
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)	SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
Penetration Testing with Kali Linux (PWK)	LogRhythm Certified Professional (LCP)	Nessus Assured Compliance Assessment Solution (ACAS)
eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX) V2	Digital Forensics & Incident Response, Volatility Framework	Microsoft Server 2016 70-741

METHODOLOGY

Network Penetration Testing (Internal/External)

RedTeam Security's network penetration testing methodology is based on the Penetration Testing Execution Standard (PTES) framework and combines the results from industry-leading testing tools with manual testing to enumerate and validate security vulnerabilities, find attack vectors, configuration errors, and business logic flaws.

While automated tools check for known vulnerabilities, they are incapable of assessing real business risk or determining the extent of the possible exploitation. Automated tools are effective in providing efficiency only during the initial phases of a penetration test. At RedTeam Security, it is our belief that an effective and comprehensive network pen test can only be realized through rigorous manual testing techniques.

RedTeam Security's network penetration testing services utilize a risk-based approach to manually identify critical infrastructure vulnerabilities that exist on all services and systems within scope. Our network security testing helps you improve your security posture by lowering the risk of unauthorized access and sensitive data breaches, improving productivity, protecting your brand from cyber attacks, and maximizing the ROI from your network devices.

Using this approach, the primary goals are to:

1. Identify application security/network flaws present in the environment.
2. Understand the level of risk for your organization.
3. Help address and fix identified application flaws.

Before beginning the network pen test security assessment, the pre-engagement phase begins. During the pre-engagement phase, RedTeam Security will collect details required to execute and kick off the project. The data elements collected during this step include: testing windows, testing dates, IP addresses, along with other relevant information. This phase is crucial as it establishes the overall rules of engagement for the network security assessment.

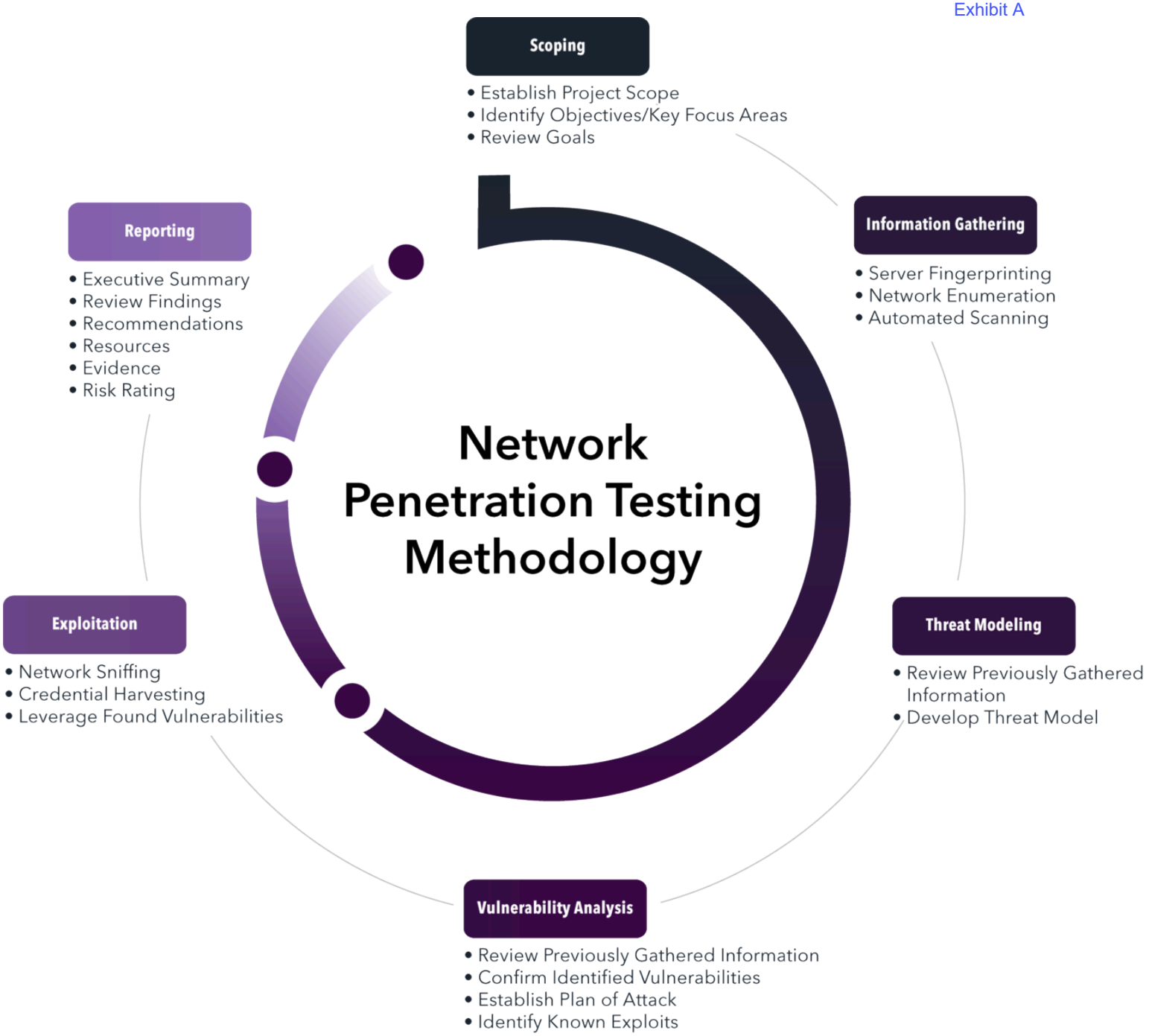
Using the information gathered for the kick-off meeting, RedTeam Security confirms the necessary details to ensure the assessment is executed efficiently, effectively and in accordance with the overall objectives.

The Value of Good Scoping

At RedTeam, we know that poor scoping leads to a lower quality deliverable. Good scoping begins with a clear understanding of what devices or applications are in scope for the engagement. Our client relationship managers work closely with our clients to identify the devices and applications in scope to assist with establishing the focus for pen-testing. Having the right focus for the pen testing team ensures the pen testing teams target areas of greatest concern which ultimately delivers the best value for the project. This begins with enumeration to understand the assets, knowing contracts with third parties (if applicable), and determining what areas contain critical information. Including all departments that should be involved (configuration management, asset manage, etc.) often leads to RedTeam discovering findings that other companies won't.

Before kicking off the actual assessment, the pre-engagement phase begins. During the pre-engagement phase, RedTeam will identify and gather the necessary details required to execute and kick off the project. The data elements collected during this step include: testing windows, testing dates, IP addresses along, application URLs, roles in scope, and other relevant information. This phase is crucial as it established the overall rules of engagement for the assessment.

Output from this step provides RedTeam with the necessary information that will be used to carry out the assessment efficiently, effectively, and in accordance with the overall objectives.



Network Penetration Testing Steps

Information Gathering

The information-gathering phase of our network pen testing methodology starts the process. Information-gathering consists of Google search engine reconnaissance, server fingerprinting, network enumeration, and more. Information gathering efforts result in a compiled list of metadata and raw output with the goal of obtaining as much information about the network's makeup as possible. Reconnaissance includes initial device footprinting, service enumeration, and operating system and application fingerprinting. The purpose of this step is to collectively map the in-scope environment and prepare for identified vulnerabilities.

During the Information Gathering phase, RedTeam Security will:

- Use discovery tools to passively uncover information about the network
- Perform network fingerprinting and enumeration in order to identify components, devices, operating systems, etc.

- Actively scan for available services and vulnerabilities and develop a test plan for latter phases in the security assessment

Threat Modeling

With the information collected from the previous step, security testing transitions to identifying vulnerabilities in the network. This typically begins with automated scans initially but quickly morphs into manual testing techniques using more pointed and direct tools. During the threat-modeling step, assets are identified and categorized into threat categories. These may involve sensitive information, trade secrets, financial documents, etc.

During this phase, RedTeam Security penetration testers will:

- Use open-source, commercial, and internally developed tools to identify and confirm well-known vulnerabilities
- Spider the in-scope network device(s) to effectively build a map of each of the operating systems, open ports and services, and areas of interest
- Use discovered sections, features, and capabilities to establish threat categories to be used for more manual/rigorous testing (i.e., default admin credentials, session hijacking, known vulnerabilities in out-of-date components)
- Build the network's threat model using the information gathered in this and the previous phase to be used as a plan of attack for later phases of the assessment
- Upload vulnerability information to the customer portal for those vulnerabilities that exist but will not be exploited due to time constraints or risk to devices

Vulnerability Analysis

The vulnerability analysis phase involves the documenting and analysis of vulnerabilities discovered as a result of the previous network penetration testing steps. This includes the analysis of out from the various security tools and manual testing techniques. At this point, a list of attractive vulnerabilities, suspicious services, and items worth researching further has been created and weighted for further analysis. In essence, the plan of attack is developed here.

Exploitation

Unlike a vulnerability assessment, a network penetration test takes such a test quite a bit further specifically by way of exploitation. Exploitation involves actually carrying out the vulnerability's exploit (i.e., buffer overflow) in an effort to be certain if the vulnerability is truly exploitable.

During the Exploitation phase of a penetration test, RedTeam Security's pen testers will attempt to gain access to the devices, networks, or applications through the bypassing of firewalls and other security controls and by the exploitation of vulnerabilities in order to determine their actual real-world risk. Throughout this step, we perform several manual tests simulating real-world attacks that are incapable of being performed through automated means. This phase of a RedTeam Security penetration test consists of heavy manual testing tactics and is often the most time-intensive phase.

Exploitation may include but is not limited to credential harvesting/guessing, network sniffing, leveraging known vulnerabilities in outdated software.

As part of the Exploitation phase, RedTeam Security will:

- Attempt to manually exploit the security issues identified in the previous phase to determine the level of risk and level of exploitation possible
- Capture and log evidence to provide proof of exploitation (images, screenshots, configs, etc.)
- Upload validated exploits and their corresponding evidence/information to the project portal for client review

- Upload validated exploits and their corresponding evidence/information to the project portal for client review

Reporting

The reporting step is intended to compile, document, and risk rate findings and generate a clear and actionable report, complete with evidence, for the project stakeholders. At RedTeam Security, we consider this phase to be the most important and we take great care to ensure we've communicated the value of our service and findings thoroughly. Upon completion of the assessment, RedTeam shall provide a single electronic report, delivered via RedTeam Security's portal. The report will provide an analysis of the current state of the assessed security controls. The deliverable for penetration testing is conveyed in a written report. RedTeam will address comments, make necessary revisions and request to schedule a report presentation. The analysis will identify areas that need to be resolved to achieve an adequate level of security. The detailed contents of the deliverable are described below.

The report deliverable will include the following high-level sections in a format suitable for management:

- Purpose of the engagement including project's scope and approach
- Positive security controls that were identified
- Tactical resolutions to immediately reduce risk in the environment
- Strategic recommendations for mitigating and preventing similar issues from recurring

The reporting step is intended to compile, document, and risk rate findings and generate a clear and actionable report, complete with evidence, for the project stakeholders. At RedTeam Security, we consider this phase to be the most important and we take great care to ensure we've communicated the value of our service and findings thoroughly. Upon completion of the assessment, RedTeam shall provide a single electronic report, delivered via RedTeam Security's portal. The report will provide an analysis of the current state of the assessed security controls. The deliverable for penetration testing is conveyed in a written report. RedTeam will address comments, make necessary revisions and request to schedule a report presentation. The analysis will identify areas that need to be resolved to achieve an adequate level of security. The detailed contents of the deliverable are described below.

The report deliverable will include the following high-level sections in a format suitable for management:

- Purpose of the engagement including project's scope and approach
- Positive security controls that were identified
- Tactical resolutions to immediately reduce risk in the environment
- Strategic recommendations for mitigating and preventing similar issues from recurring

The report deliverable will also include the following in-depth analysis and recommendations for technical staff to understand the underlying risks and recommendations:

- A technical description and classification of each vulnerability
- Anatomy of exploitation including steps taken and proof in the form of screenshots
- Business or technical risk inherent in the vulnerability
- Vulnerability classification that describes the risk level as a function of vulnerability impact and ease of exploitation
- Technical description of how to mitigate the vulnerability

SCOPE OF SERVICES

Overview

Penetration Testing | Web Application Penetration Testing

RedTeam Security's web application security testing combines the results from industry-leading scanning tools with manual testing to enumerate and validate vulnerabilities, configuration errors, and business logic flaws. In-depth manual application testing enables us to find what scanners often miss.

Web applications are particularly vulnerable to external attack given that they are inherently designed to be accessible to the Internet. While automated scanners check for known vulnerabilities, they are incapable of actually reporting on real business risk. Our web application security testing helps you lower your risk of data breach, improve productivity, protect your brand, and maximize the ROI from your web applications.

Objective

The primary objective for an web application penetration test is to identify critical exploitable vulnerabilities in applications before hackers discover and exploit them. This type of assessment is an attack simulation carried out by our highly trained security consultants in an effort to:

- Identify application security flaws present in the environment
- Understand the level of risk for your organization
- Help address and fix identified application flaws

Speaking overall, the overall goal of an application penetration test is to uncover software vulnerabilities, demonstrate the impact of the weaknesses, and provide recommendations for mitigation.

Web application penetration testing will reveal real-world opportunities for hackers to be able to compromise applications in such a way that allows for unauthorized access to sensitive data or even take-over systems for malicious/non-business purposes.

Approach

RedTeam Security's web application penetration testing service utilizes a risk-based approach to manually identify critical application-centric vulnerabilities that exist on all in-scope applications.

Using this approach, RedTeam's comprehensive approach covers the classes of vulnerabilities in the Open Web Application Security Project (OWASP) Top 10 2017 and beyond:

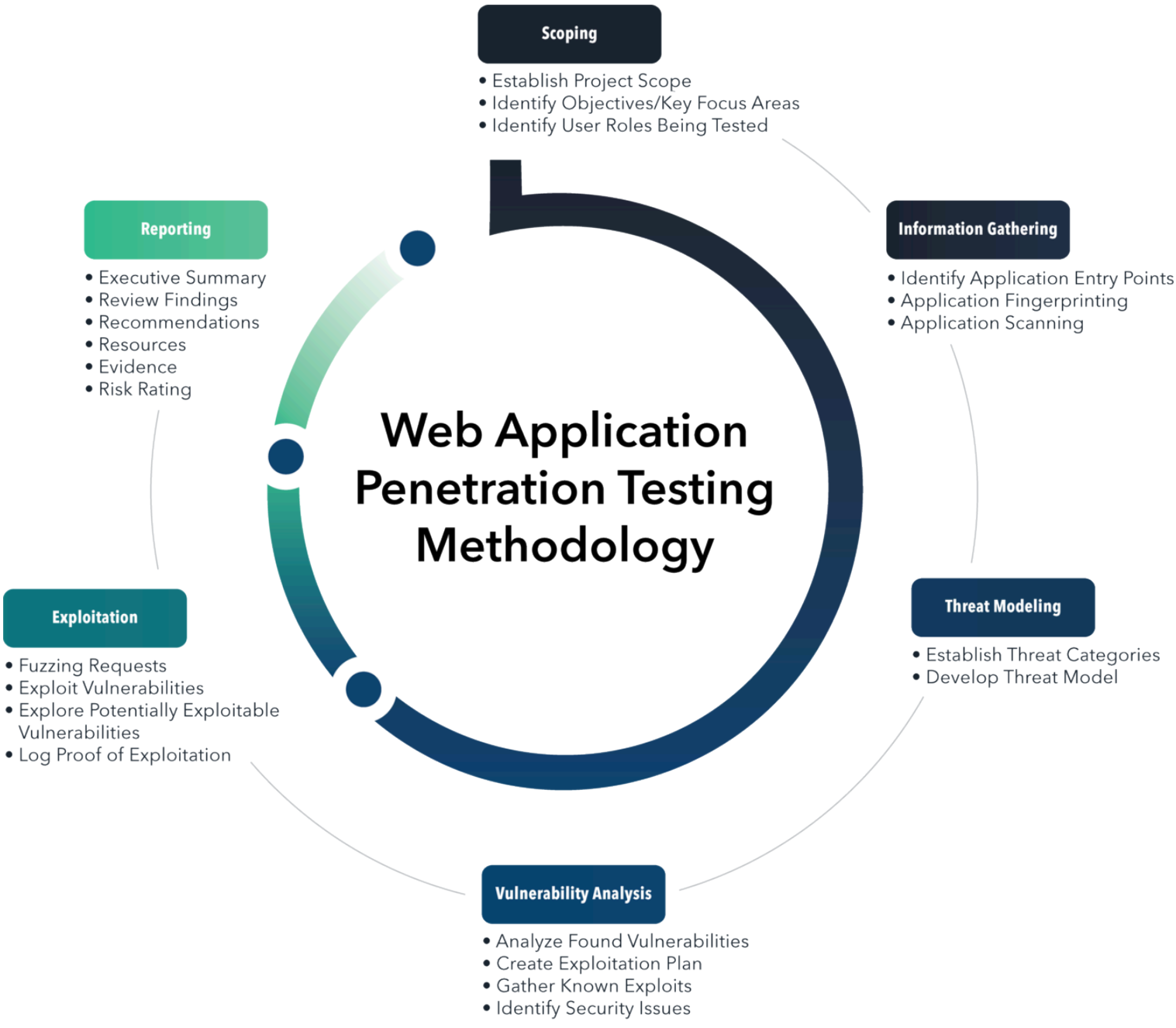
1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

METHODOLOGY

Web Application Penetration Testing

RedTeam Security's web application penetration test service utilizes a risk-based approach to manually identify critical application-centric security flaws in all in-scope applications. RedTeam Security's web application penetration test combines the results from industry-leading scanning tools with manual testing to enumerate and validate vulnerabilities, configuration errors, and business logic flaws. In-depth manual application testing enables us to find what scanners often miss.

RedTeam Security's web app penetration testing methodology is a consistent process based on industry-standard practices used for each pen test we perform. Experience has shown our clients and us that our proven web application penetration testing methodology works.



The Value of Good Scoping

At RedTeam, we know that poor scoping leads to a lower quality deliverable. Good scoping begins with a clear understanding of what devices or applications are in scope for the engagement. Our client relationship managers work closely with our clients to identify the devices and applications in scope to assist with establishing the focus for pen-testing. Having the right focus for the pen testing team ensures the pen testing teams target areas of greatest concern which ultimately delivers the best value for the project. This begins with enumeration to understand the assets, knowing contracts with third parties (if applicable), and determining what areas contain critical information. Including all departments that should be involved (configuration management, asset manage, etc.) often leads to RedTeam discovering findings that other companies won't.

Web Application Penetration Testing Steps

Information Gathering

The information-gathering phase consists of Google search engine reconnaissance, server fingerprinting, application enumeration, and more. Information gathering efforts result in a compiled list of metadata and raw output to obtain as much information about the application's makeup as possible. Reconnaissance includes web application footprinting, metafile leakage review, service enumeration, and operating system and application fingerprinting. The purpose of this step is to map the in-scope application and prepare for threat identification collectively.

During the Information Gathering phase, RedTeam Security will:

- Use discovery tools to passively uncover information about the application
- Identify entry points into the application, such as administration portals or backdoors
- Perform application fingerprinting to identify the underlying development language and components
- Send fuzzing requests to be used in the analysis of error codes that may disclose valuable information that could be used to launch a more targeted cyber attack
- Actively scan for open services and develop a test plan for the latter phases in the security assessment

Through testing, RedTeam Security's penetration testers actively try to force your web applications to leak information, disclose error messages that can be exploited, or reveal versions and technologies used.

Threat Modeling

With the information collected from the previous step, the testing process transitions to identifying security issues in the application. This typically begins with automated scans initially but quickly morphs into manual testing techniques using more pointed and direct tools. During the threat modeling step, assets are identified and categorized into threat categories. These may involve sensitive information, trade secrets, financial documents, etc.

During this phase, RedTeam Security will:

- Use open source, commercial, and internally developed tools to identify and confirm well-known vulnerabilities.
- Spider the in-scope application(s) to effectively build a map of each of the features, components, and areas of interest
- Use discovered sections, features, and capabilities to establish threat categories to be used for more manual/rigorous testing (i.e., file uploads, admin backdoors, web services, editors)
- Send fuzzing requests to be used to analyze error codes that may disclose valuable information that could be used to launch a more targeted attack.
- Build the application's threat model using the information gathered in this and the previous phase to be used as a plan of attack for later phases of the penetration test

- Upload vulnerability information to the customer portal for those vulnerabilities that exist but will not be exploited due to time constraints or risk to devices.

Vulnerability Analysis

The vulnerability analysis step involves documenting and analyzing vulnerabilities discovered due to Information Gathering and Threat Modeling. This includes the analysis of output from the various security tools and manual testing techniques.

During the Vulnerability Analysis phase, RedTeam Security will:

- Compile the list of areas of interest and develop a plan for exploitation
- Search and gather known exploits from various sources
- Analyze the impact and likelihood for each potentially exploitable vulnerability
- Search and gather known exploits from various sources
- Analyze the impact and likelihood for each potentially exploitable vulnerability
- Select the best methods and tools for properly exploiting each of the suspected exploitable vulnerabilities

Exploitation

Unlike a vulnerability assessment, a penetration test takes the additional step of exploitation. Exploitation involves establishing access to the application or connected components by bypassing security controls and exploiting vulnerabilities to determine their real-world risk. Throughout this step, we perform several manual tests simulating real-world exploits incapable of being performed through automated means. During a RedTeam Security web application penetration test, the exploitation phase consists of heavy manual testing tactics and is often the most time-intensive phase.

As part of the Exploitation phase, RedTeam Security will:

- Attempt to manually exploit the vulnerabilities identified in the previous phases to determine the level of risk and level of exploitation possible
- Capture and log evidence to provide proof of exploitation (images, screenshots, configs, etc.)
- Notify the client of any Critical findings upon discovery
- Capture and log evidence to provide proof of exploitation (images, screenshots, configs, etc.)
- Notify the client of any Critical findings upon discovery
- Upload validated exploits and their corresponding evidence/information to the project portal for client review

Reporting

The reporting step is intended to compile, document, and risk rate findings and generate a clear and actionable report, complete with evidence, for the project stakeholders. The report will be delivered through the customer portal. If a customer requests, a presentation of findings will occur via an online meeting.

During this phase, RedTeam Security will perform the following:

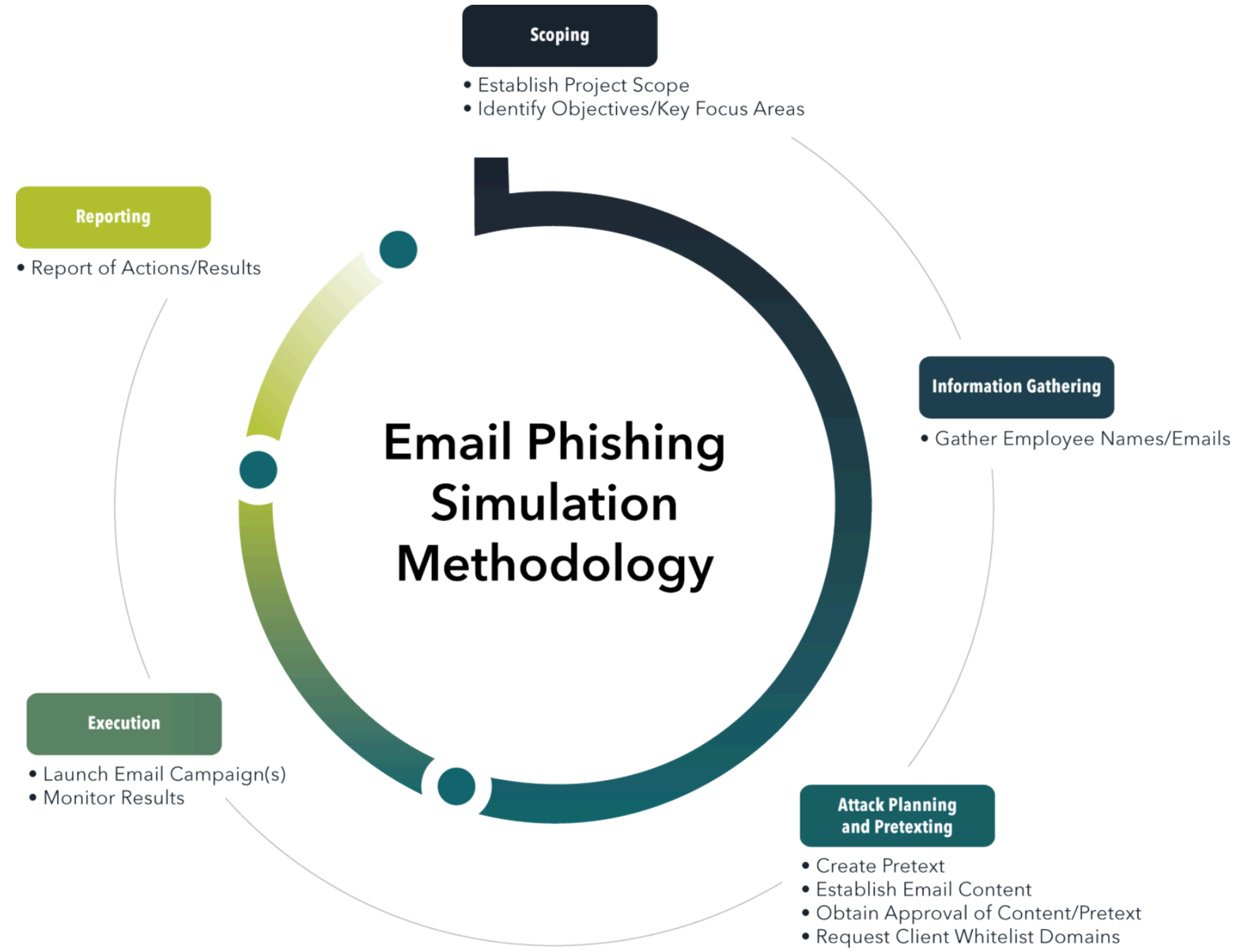
- Ensure all findings have been uploaded to the project portal for client review
- Create the web application penetration test report, along with evidence. This will go through an internal review process that then is uploaded to the client portal for review
- Additional meetings may take place to ensure the client understands the findings and recommendations for mitigation or remediation

Email Phishing Methodology

RedTeam Security's email Phishing Methodology combines industry-standard methodologies with our experience to develop a customized approach to testing employee's adherence to company procedures and their ability to protect company assets. As part of an email Phishing engagement, RedTeam Security will assess:

- Whether employees can identify a suspicious or malicious email
- How well procedures for disclosing information are followed and/or whether they are sufficient to protect company and client information
- Whether suspicious emails are reported appropriately
- In some instances, an email Phishing engagement will test the ability of technical controls to protect against phishing

RedTeam Security employs a standard methodology that includes multiple phases. These phases build on each other and ensure an effective and comprehensive test.



Email Phishing Steps

Information Gathering

As with other types of penetration testing, the first phase in an email phishing engagement is to focus on gathering as much information as possible about the target. This is done through passive reconnaissance and Open-Source Intelligence (OSINT). This is one of the most critical steps in the process because it helps to examine your organization from the perspective of a "bad guy" and enables RedTeam Security to see everything an attacker would by utilizing public tools, such as Google Earth, social media, and job boards. Using this approach, it is usually possible to learn a great deal about the business, its surroundings, and environment.

In an email Phishing test, Information Gathering will consist of gathering employee email addresses and names and learning information about the company that can be used to develop relevant pretexts for phishing emails.

The depth of this phase will vary based on the specific engagement. In many cases, the client will provide much of the information needed to create the pretext and launch the attack (i.e., vendors and software used, the list of names and email addresses to target).

Attack Planning & Pretexting

Intelligence gathered through the previous steps is combined into a plan of attack. The plan of attack for an email phishing engagement includes creating a Pretext (the story being used and who will be shown as the sender of the phishing email), the email content, the email addresses and names of targets, the goals of the engagement (i.e., will RedTeam Security attempt to gather credentials, will the email infrastructure be tested to determine if they filter malicious files), timing, etc. RedTeam Security will also work with the client contact to obtain approval of the content and the format of the phishing emails.

Execution

This is where the team executes the attack, launches the email campaign, and monitors the results. Generally, phishing emails will be sent out in a phased manner, over a period of hours or days depending on the number of employees in scope, and then the email campaign will stay open/active for a week or two to allow for recipients who do not read their email timely.

Reporting

RedTeam Security will provide a report that includes the pretext/content included in the email, a summary of the results (who read the email, who took an action, etc.) and then each target's results. You can use the results to develop or enhance your security awareness training.

Reports can be sent at any time during the running of the campaign or at the completion of the phishing test. Key metrics that will be reported:

- Users who opened the email.
- Users who clicked on a link within the email.
- Users who entered credentials on the phishing site landing page (if applicable).
- Users who viewed and completed any associated training material (if applicable).
- Users who had responded to BEC (business email compromise) emails and their respective responses (if applicable).

YOUR INVESTMENT

Below is the budget we've estimated based on the scope of services outlined earlier in this proposal. Thank you for the opportunity to win your business. Please do not hesitate to contact us for any reason.

SINGLE YEAR ENGAGEMENT	PRICE
Web Application Penetration Test RedTeam Security will assess the level of security awareness evident in the design of your web application. We will find and attempt to exploit security flaws that could allow privilege escalation, disclosure of sensitive information, injection of malicious code into trusted components, invalid transactions, and other conditions recognized as posing security vulnerabilities. This approach allows us to identify all existing attack vectors and demonstrate the impact of a real-world attack. RedTeam will provide a comprehensive report detailing exploitable findings, risk ratings and business impact, evidence of findings including screenshots and actionable recommendations for remediation. RedTeam will provide re-testing on all mitigated vulnerabilities which were identified during primary testing phases. **Scope:** • 49 Applications **(see list after signature page)** ◦ 21 applications with logins ◦ 28 with static pages and forms ◦ 12 did not load (no cost) ◦ 3 redirects to other sites - (no cost) • Assumes 2 user roles per application	$83,900
Internal and External Network Penetration Test During the penetration test, RedTeam will identify the susceptibility of the environment to threats from a malicious user, third party, or malicious hacker attempting to breach systems in an attempt to gain unauthorized access to networks, systems, hosts, applications, and any sensitive or restricted data. This is done by leveraging a combination of expert manual testing and commercial, open source, and proprietary software to fulfill the test objectives. **Network Penetration Test** **Scope:** • Up tp 5 External IPs-$3500 • Up to 65 Internal IPs-$6500	$10,000
SUBTOTAL	$93,900
FRIENDS AND FAMILY DISCOUNT (-15%)	-$14,085
TOTAL	$79,815

STATEMENT OF WORK

Date: September 16, 2021

Between "us", RedTeam Security, and "you", Fort Bend County

You, Fort Bend County, located at 301 Jackson St , Richmond, Texas 77469 are hiring RedTeam Security located at 214 4th St. E, Suite 140, St. Paul, MN 55101 to perform RedTeam Security Engagement for the estimated total price of $79,815.00 as outlined in the budget/investment section of this proposal.

1.0 Services Rendered

Project Touchpoint Meetings will provide the opportunity for Fort Bend County to review our work and provide feedback. If, at any stage, you're not satisfied with the direction our work is taking, you will pay us in full for everything we've produced up to that that point and then cancel this contract.

Errors

We can't guarantee that our work will be error-free so we can't be liable to you or any third-party for damages, including lost profits, lost savings or other incidental, consequential or special damages, even if you've advised us of them.

2.0 Mutual Cooperation

We agree to use our best efforts to fulfill and exceed your expectation on the deliverables listed above. You agree to aid us in doing so by making available to us needed information pertaining to this project and to cooperate with us in expediting the work.

3.0 Charges for Services Performed

Services or requests above and beyond those listed in the budget and/or the functionality specs may be considered out-of-scope and an amendment to the budget will be recommended. Projects that go dormant for longer than 45 days will incur fee to resume work at the discretion of RedTeam Security.

4.0 Terms of Payment

4.1 Billing Schedule

The total budget for this project: $79,815.00

For all projects under $12,000, RedTeam Security will invoice client for the full amount of this proposal upon execution of this agreement, **DUE UPON RECEIPT**, before work begins.

For any project over $12,000, RedTeam Security will invoice Fort Bend County for **fifty percent (50%)** of the initial fees (DUE UPON RECEIPT) at point of this signed contract agreement which will act as the deposit. The remaining 50% will be billed upon project completion upon NET 15 terms.

Fort Bend County will supply RedTeam Security with all necessary purchase order numbers and other internal information required for invoice processing upon signing this SOW (if applicable).

4.2 Client Agreement to Pay

You agree to pay our initial (1st) invoice upon receipt which will act as a deposit for the project. In the event payment is not made within 15 days, RedTeam Security will charge a late payment fee of 1% per month on any overdue and unpaid balance not in dispute, to cover the manpower, interest, and other costs RedTeam Security pays for carrying overdue invoices from Fort Bend County. In addition, RedTeam Security reserves the right to stop work until payment is received.

4.3 Collection Costs

In the event that we incur legal fees, costs and disbursements in an effort to collect our invoices, in addition to interest on the unpaid balance, you agree to reimburse us for these expenses.

5.0 Cancellation of Plans

You have the right to modify, reject, cancel or stop any and all plans or work in process. However, you agree to reimburse us for all costs and expenses we incurred prior to your change in instructions, and which relate to non-cancelable commitments, and to defend, indemnify and hold us harmless for any liability relating to such action. We agree to use our best efforts to minimize such costs and expenses.

6.0 Confidentiality

For the purposes of this engagement, the term "Confidential Information" means all information communicated orally, disclosed visually, in writing or via electronic media in the course of performing services for Fort Bend County. Confidential information includes, but is not limited to, (i) all forms of documents including vulnerability reports and findings, executive summary reports, evidence work papers, proposals, scoping information, IP addresses, source code, application flows, data models, materials, network design specifications, customer-related data, product documentation, processes, procedures and "know-how," (ii) customer information, marketing plans, price lists, strategies, intellectual property, trade secrets and other information regarding Fort Bend County and its business. All vulnerability information discovered and communicated, such as technical and non-technical security vulnerabilities, shall be considered Confidential Information in the course of this relationship regardless of whether disclosed visually, in writing, or on electronic media. Oral statements also constitute as Confidential Information. All Confidential Information shall remain the sole property of Fort Bend County.

RedTeam Security Corporation represents, warrants and agrees that (i) it will hold in trust and confidence all Confidential Information and will not publish, transfer or disclose to others, directly or indirectly, as Confidential Information or anything relating to such information without the prior written consent of Fort Bend County (ii) it will not copy or reproduce any Confidential Information; (iii) it will not use any Confidential information for any purpose without the prior written consent of Fort Bend County, except as may be necessary in the course of the business relationship with Fort Bend County (iv) it will upon termination or completion of the engagement, or at any other time upon the request of Fort Bend County, immediately return all or any part of the Confidential Information and all copies thereof as requested by Fort Bend County.

7.0 Term and Termination

7.1 Period of Agreement and Notice of Termination

This Agreement shall become effective as of September 16, 2021 and shall continue until terminated by either party upon not less than 60 days' notice in writing given by either party to the other.

7.2 Termination for Cause

Either party to this Agreement may terminate the Agreement if the other party defaults in the performance of any of its material duties and obligations and the default is not cured within thirty (30) days of the receipt of notice of said default, or if the default is not reasonably curable within said period of time, unless the defaulting party commences cure within said period of time and diligently proceeds to cure the default.

In addition, either party may immediately terminate this Agreement by giving written notice to the other party if the other party is insolvent or has a petition brought by or against it under the insolvency laws of any jurisdiction, if the other party makes an assignment for the benefit of creditors, if a trustee, or similar agent is appointed with respect to any property or business of the other party, or in the case of the Client, if the Client materially breaches its obligations to make payment pursuant to this Agreement.

7.3 Payment for Non-Cancelable Materials

Any non-cancelable materials, services, etc., we have properly committed ourselves to purchase for your account shall be paid for by you, in accordance with the provisions of this Agreement. We agree to use our best efforts to minimize such liabilities immediately upon written notification from you. We will provide written proof, upon request of the Fort Bend County, that any such materials and services, are non cancelable.

7.4 Materials Unpaid For

If upon termination there exist any materials furnished by us or any services performed by us for which you have not paid us in full, until such time as you have paid us in full you agree not to use any such materials, in whole or in part, or the product of such services.

7.5 Transfer of Materials

Upon termination of this agreement, provided that there is no outstanding indebtedness then owing by Fort Bend County to RedTeam Security, RedTeam Security shall transfer, assign and make available to Fort Bend County all property and materials in its possession or control belonging to Fort Bend County. Fort Bend County agrees to pay for all costs associated with the transfer of materials.

8.0 General Provisions

8.1 Governing Law

This Agreement shall be governed and construed in accordance with the laws of the State of Minnesota.

8.2 Representations and Warranties

The parties each individually represent and warrant that each has full power and authority to enter into this Agreement and to perform all of their obligations hereunder without violating the legal or equitable rights of any third party.

Client represents and warrants that it has the appropriate authorizations from the legal owner of the computer networks, systems, IP addresses or ranges of IP addresses, information assets, and / or hardware which permit Client to retain RedTeam to perform its penetration testing and vulnerability testing services, or which are targeted, scanned, monitored, or tested by RedTeam as directed by the Client. Client further acknowledges that the provision to RedTeam of IP addresses which are not owned by Client could cause potential damage or harm to the actual third party owner of said IP address(es) and therefore Client agrees that it will indemnify and hold harmless RedTeam and its employees, officers, owners, and other affiliated parties from any and all such costs, fees or damages.

8.3 Entire Agreement

Except as otherwise set forth or referred to in this Agreement, this Agreement constitutes the sole and entire Agreement and understanding between the parties hereto as to the subject matter hereof, and supersedes all prior discussions, agreements and understandings of every kind and nature between them as to such subject matter.

8.4 Severability

If any provision of this Agreement is held to be illegal, invalid, or unenforceable under any present or future law, then that provision will be fully severable. In such instance, this Agreement will be construed and enforced as if the illegal, invalid, or unenforceable provision had never comprised a part of this Agreement, and the remaining provisions of this Agreement will remain in full force and effect.

NEXT STEPS

1. Please read the SOW on the previous page to make sure you understand all the details involved with us working together. It's really important to us that everything is transparent and understood from the beginning so that we lay a solid foundation for a great working relationship.
2. If you have any questions at all, please let us know. We're happy to clarify any points and there may be some items that we can sort out together. We're committed to finding the best way to work together.
3. Once you feel confident about everything and are ready to move forward, please click the 'sign here' button below.
4. Sign in the box that pops up to make the acceptance official.
5. Once we receive notification of your acceptance, we'll contact you shortly to sort out next steps and get the project rolling!
6. We'll email you a separate copy of the signed contract for your records.
7. If you'd like to speak to us by phone, don't hesitate to call Angie Dean at 612-245-1364.

SIGNATURE
Angie Dean

Angie Dean
Director of Sales

SIGNATURE
Jahan Jolliver

Jahan Jolliver
Fort Bend County

SITES INCLUDED IN SCOPE OF ENGAGEMENT

- https://fbcwebser.fortbendcountytx.gov/ - static/form(s)
- https://cad.fortbendcountytx.gov/ - static/form(s)
- https://eeyp.fortbendcountytx.gov/ - doesn't load
- http://fbcassistancedistricts.org/ - static/form(s)
- http://fbcdiversityinitiative.com/ - doesn't load
- http://form.fortbendcountytx.gov/ - static/form(s)
- https://historicalcommission.fortbendcountytx.gov/ - static/form(s)
- https://meetings.fortbendcountytx.gov/ - static/form(s)
- https://odysseyreport.fortbendcountytx.gov/ - static/form(s)
- https://publictransportation.fortbendcountytx.gov/ - static/form(s)
- https://sampleballots.fortbendcountytx.gov/ - static/form(s)
- https://transparency.fortbendcountytx.gov/ - static/form(s)
- https://www.coronavirusfortbend.gov/ - static/form(s)
- https://coronavirus.fortbendcountytx.gov/ - static/form(s)
- https://fbcsso.fortbendcountytx.gov/ - log in required
- https://fbcssotest.fortbendcountytx.gov/ - log in required
- https://fbctx.gov - static/form(s)
- https://shared.fortbendcountytx.gov/ - log in required
- https://shared1.fortbendcountytx.gov/ - log in required
- https://shared2.fortbendcountytx.gov/ - log in required
- https://shared3.fortbendcountytx.gov/ - log in required
- https://takemehome.fortbendcountytx.gov/TakeMeHome/Account/Login.aspx - log in required
- http://tylerpaw.fortbendcountytx.gov/PublicAccess/default.aspx- static
- http://tylerpaw.fortbendcountytx.gov/SecureAccess/default.aspx - log in required
- https://tylerportal.fortbendcountytx.gov/FORTBENDPRODPORTAL/ - log in required
- http://odystagepa.fortbendcountytx.gov/PublicAccess/default.aspx - doesn't load
- http://odystagepa.fortbendcountytx.gov/SecureAccess/default.aspx - doesn't load
- https://odystgportalcl.fortbendcountytx.gov/FORTBENDSTGPORTAL- log in required
- https://callcenter.fortbendcountytx.gov/ - doesn't load
- https://communityvaccineevent.fortbendcountytx.gov/ - static/form(s)
- https://enotifier.fortbendcountytx.gov/ - static/form(s)
- https://equipmenttracker.fortbendcountytx.gov/ - static/form(s)
- https://landmarkcommunity.fortbendcountytx.gov/ - static/form(s)
- https://landmarkcommunitycheckin.fortbendcountytx.gov/UnauthorizedAccess/Index - doesn't load
- https://news.fortbendcountytx.gov - doesn't load

- https://nqwaittimes.fortbendcountytx.gov/ - redirect
- https://vaccinedosetracker.fortbendcountytx.gov/- login required
- https://vaccinewaitlist.fortbendcountytx.gov/ - redirect
- https://vaccinewaitlistmanage.fortbendcountytx.gov/ - doesn't load
- https://vaccinewaitlistreporting.fortbendcountytx.gov/ -doesn't load
- https://vaccinewaitlisttest.fortbendcountytx.gov/ -doesn't load
- https://chat.fortbendcountytx.gov/ - - static/form(s)
- https://crywolf.fortbendcountytx.gov/ - login required
- https://www.enablefortbend.com/Signin?ReturnUrl=%2f - login required
- https://histcomn.fortbendcountytx.gov/(S(cgdqqgoc0eq4xi5cxqcezlb3))/login.aspx- login required
- https://housewatchso.fortbendcountytx.gov/(S(0k5wim0a25fsw4gwkiw5bzcl))/default.aspx - login required
- https://jailinq.fortbendcountytx.gov/(S(wr45r4ltsxn230l2hihtn55p))/default.aspx - login required
- https://permitfeecalculator.fortbendcountytx.gov/ - static/form(s)
- https://schoolsurveillance.fortbendcountytx.gov/- login required
- https://taxrate.fortbendcountytx.gov/(S(pdluthn20bvrbep4nyubimsw))/login.aspx - login required
- https://taxrateinfo.fortbendcountytx.gov/(S(3f1r3i3oluim3n1jodqpbyut))/default.aspx - static/form(s)
- https://actecd.fortbendcountytx.gov/- static/form(s)
- https://utilcritinfo.fortbendcountytx.gov/(S(g410smvd1c5w2wyvrtttxixu))/login.aspx -- login required
- https://vectorcontrol.fortbendcountytx.gov/- static/form(s)
- https://voterinq.fortbendcountytx.gov/(S(kgmcgf5svwu2o15qrpb4ji0t))/default.aspx- static/form(s)
- https://chat.fortbendcountytx.gov/- static/form(s)
- https://electedofficials.fortbendcountytx.gov/- static/form(s)
- https://forms.fortbendcountytx.gov/ - static/form(s)
- https://fortbend-era.powerappsportals.us/- login required
- https://handylinks.fortbendcountytx.gov/ - static/form(s)
- https://kiosk.fortbendcountytx.gov/ - doesn't load
- https://media.fortbendcountytx.gov/ - static/form(s)
- https://qrcode.fortbendcountytx.gov/ - redirect
- https://splash.fortbendcountytx.gov/ -doesn't load

TEST CATEGORIES

Network Penetration Testing Test Categories

The primary objective for an external penetration test is to identify critical exploitable vulnerabilities of Internet-facing systems before hackers discover and exploit them. Using Nessus or Nmap, RedTeam security consultants will look at the open services and ports on your network perimeter. Some of our testers may reach out to these services manually doing a raw socket connect or tenet to get eyes on it. They will send a request or telnet to see what it does and try to get good visibility. Some of the tests covered may include:

- Assessing the security posture of your cryptographic implementation
- How do you have the TLS configured?
- Is SSLV still enabled?

In an effort to provide a consistent and comprehensive penetration test, we utilize the following tests as a bare minimum. While not all tests below will be applicable or desired (ie: denial-of-service), we make heavy use of this proven methodology to ensure our clients experience consistent and comprehensive testing for each and every penetration test, quarter after quarter, year after year.

Test Category	Test ID	Test Description
Password Security	NET-PS-001	Network credentials discovery
Password Security	NET-PS-002	Localhost credentials discovery
Password Security	NET-PS-003	Testing for password strength
Password Security	NET-PS-004	Testing for public/proprietary algorithms
Password Security	NET-PS-005	Rainbow table password cracking
Password Security	NET-PS-006	Dictionary password cracking
Password Security	NET-PS-007	Brute-force password cracking
Switch Security	NET-SS-001	Reconnaissance/banner grabbing
Switch Security	NET-SS-002	Port security
Switch Security	NET-SS-003	VLAN hopping attacks
Switch Security	NET-SS-004	Private VLAN hopping attacks
Switch Security	NET-SS-005	Spanning tree attacks
Switch Security	NET-SS-006	CDP attacks and discovery
Switch Security	NET-SS-007	Vulnerable services
Switch Security	NET-SS-008	ARP attacks

Switch Security	NET-SS-009	DHCP starvation
Router Security	NET-RS-001	Reconnaissance/banner grabbing
Router Security	NET-RS-002	Routing protocol security
Router Security	NET-RS-004	Vulnerable services
Router Security	NET-RS-003	VTY/TTY connection testing
Router Security	NET-RS-004	Vulnerable services
Router Security	NET-RS-005	SNMP walking
Router Security	NET-RS-006	TFTP access
Router Security	NET-RS-007	Password/auth security
Router Security	NET-RS-008	Access to console
Router Security	NET-RS-009	CDP attacks and discovery
VPN	NET-VP-005	Authentication attacks
VPN	NET-VP-006	Product-specific vulnerabilities
VPN	NET-VP-007	Split tunneling attacks
Antivirus	NET-AV-001	EICAR testing
Antivirus	NET-AV-002	MIME testing
Antivirus	NET-AV-003	Antivirus fingerprinting
Antivirus	NET-AV-004	AV evasion testing
Server & Host Security	NET-HS-001	Recon and footprinting
Server & Host Security	NET-HS-002	ARIN, WHOIS discovery
Server & Host Security	NET-HS-003	DNS enumeration / AXFR
Server & Host Security	NET-HS-004	Domain name registrar security
Server & Host Security	NET-HS-004	Domain name registrar security
Server & Host Security	NET-HS-005	Scanning for open ports and services
Server & Host Security	NET-HS-006	Testing for OS identification
Server & Host Security	NET-HS-007	Network domain discovery
Server & Host Security	NET-HS-008	Enumeration testing
Server & Host Security	NET-HS-008	Enumeration testing

Server & Host Security	NET-HS-009	Testing for administrative backdoors
Server & Host Security	NET-HS-010	Testing for malicious backdoors
Server & Host Security	NET-HS-011	SMTP relay testing
Server & Host Security	NET-HS-012	SNMP walking
Server & Host Security	NET-HS-013	Testing for remote control services (RDP, SSH)
Server & Host Security	NET-HS-014	Testing for network file shares
Server & Host Security	NET-HS-015	Testing for missing patches
Server & Host Security	NET-HS-016	Identification of vulnerable services
Server & Host Security	NET-HS-017	Exploitation of identified vulnerabilities
Server & Host Security	NET-HS-018	Testing for denial-of-service

TEST CATEGORIES

Web Application Penetration Testing Test Categories

Web applications will be examined using a black box position and conducting vulnerability analysis. RedTeam will use manual exploitation to breach the perimeter but not attempt to take an asset down. Once we establish an initial breach, we determine the value of the machine compromised and we may maintain control of the machine for later use. The value of the machine is determined by the sensitivity of the data stored on it and the machine's usefulness in further compromising the network. Full Web Application testing is another popular, but separate service offering.

While not all tests below will be applicable or desired (ie: denial-of-service), we utilize the following as a bare minimum to provide consistent and comprehensive penetration testing:

Test Category	Test ID	Test Description
Information Gathering	APP-IG-001	Spiders, robots and crawlers
Information Gathering	APP-IG-002	Search engine discovery / reconnaissance
Information Gathering	APP-IG-002	Search engine discovery / reconnaissance
Information Gathering	APP-IG-003	Identify application entry points
Information Gathering	APP-IG-004	Testing for web application fingerprint
Information Gathering	APP-IG-005	Application discovery
Information Gathering	APP-IG-006	Analysis of errors and error codes
Configuration Management	APP-CM-001	SLL/TLS testing
Configuration Management	APP-CM-002	Database listener testing
Configuration Management	APP-CM-003	Infrastructure config management testing
Configuration Management	APP-CM-004	Application configuration management testing
Configuration Management	APP-CM-005	Testing for file extension handling
Configuration Management	APP-CM-006	Old, backup and unreferenced files
Configuration Management	APP-CM-007	Infrastructure and application admin interfaces
Configuration Management	APP-CM-008	Testing for HTTP methods and XST
Authentication Testing	APP-AT-001	Credentials transport over an encrypted channel
Authentication Testing	APP-AT-002	Testing of user enumeration
Authentication Testing	APP-AT-003	Testing for guessable user accounts
Authentication Testing	APP-AT-004	Brute force testing

Authentication Testing	APP-AT-005	Testing for bypassing authentication schema
Authentication Testing	APP-AT-006	Testing for vulnerable remember password / reset
Authentication Testing	APP-AT-007	Testing for logout and browser cache management
Authentication Testing	APP-AT-008	CAPTCHA testing
Authentication Testing	APP-AT-010	Testing for race conditions
Session Management	APP-SM-001	Testing for session management schema
Session Management	APP-SM-002	Testing for cookie attributes
Session Management	APP-SM-003	Testing for session fixation
Session Management	APP-SM-004	Testing for exposed session variables
Session Management	APP-SM-005	Testing for cross-site request forgery
Authorization Testing	APP-AZ-001	Testing for path traversal
Authorization Testing	APP-AZ-002	Testing for bypassing authorization
Authorization Testing	APP-AZ-002	Testing for bypassing authorization
Authorization Testing	APP-AZ-003	Testing for horizontal/vertical privilege escalation
Business Logic	APP-BL-001	Testing for business logic
Data Validation Testing	APP-DV-001	Reflected cross-site scripting
Data Validation Testing	APP-DV-002	Stored / persistent cross-site scripting
Data Validation Testing	APP-DV-003	DOM-based cross-site scripting
Authorization Testing	APP-AZ-003	Testing for horizontal/vertical privilege escalation
Business Logic	APP-BL-001	Testing for business logic
Data Validation Testing	APP-DV-001	Reflected cross-site scripting
Data Validation Testing	APP-DV-002	Stored / persistent cross-site scripting
Data Validation Testing	APP-DV-003	DOM-based cross-site scripting
Data Validation Testing	APP-DV-004	Cross-site flashing
Data Validation Testing	APP-DV-005	SQL injection
Data Validation Testing	APP-DV-006	LDAP injection
Data Validation Testing	APP-DV-007	ORM injection
Data Validation Testing	APP-DV-008	XML injection

Data Validation Testing	APP-DV-009	SSI injection
Data Validation Testing	APP-DV-009	SSI injection
Data Validation Testing	APP-DV-010	Xpath injection
Data Validation Testing	APP-DV-011	IMAP/SMTP injection
Data Validation Testing	APP-DV-012	Code injection
Data Validation Testing	APP-DV-013	OS commanding
Data Validation Testing	APP-DV-014	Buffer overflow
Data Validation Testing	APP-DV-015	Incubated vulnerability
Data Validation Testing	APP-DV-0016	HTTP smuggling and splitting
Denial-of-Service Testing	APP-DS-001	SQL wildcard attacks
Denial-of-Service Testing	APP-DS-002	Locking customer accounts
Denial-of-Service Testing	APP-DS-003	Testing for DOS buffer overflow
Denial-of-Service Testing	APP-DS-004	User-specified object allocation
Denial-of-Service Testing	APP-DS-005	User input as loop counter
Denial-of-Service Testing	APP-DS-006	Writing user provided data to disk
Denial-of-Service Testing	APP-DS-007	Failure to release resources
Denial-of-Service Testing	APP-DS-008	Too much data in session
Web Service Testing	APP-WS-001	Information gathering
Web Service Testing	APP-WS-001	WSDL testing
Web Service Testing	APP-WS-001	XML structural testing
Web Service Testing	APP-WS-001	XML content-level testing
Web Service Testing	APP-WS-001	HTTP GET parameters / REST
Web Service Testing	APP-WS-001	Malicious SOAP requests
Web Service Testing	APP-WS-001	Replay testing
Ajax Testing	APP-AJ-001	Ajax vulnerabilities
Ajax Testing	APP-AJ-002	Ajax testing/malicious request

Comprehensive List of Tools Used in Testing

COMPREHENSIVE LIST OF TOOLS USED IN TESTING

In-House Developed Tools

Our custom tools are built using hundreds of hours of in-house development. Currently, our basic tools will bypass Windows defender and antivirus, and some Endpoint Detection & Response (EDR) tools.

As a research-focused organization or pen testing teams spend a dedicated amount of time each day investigating the next-level, exploit, preparing for an upcoming hacking demo, designing new scripts and tools, connecting with other pen-testers in their network, and working on their research projects. All RedTeam security consultants have individual research projects that they are responsible for. A recent successful collaboration with several of the pen testers included what they call a "NUK". This tool was especially valuable during COVID when teams could no longer go onsite for pen-testing engagements. Instead, they shipped the proprietary NUK to our clients who plugged them into their network. Through secure code on the NUK, RedTeam established persistence on the network and could begin its internal scanning.

Commercial Tools and Open-source Tools

In addition to our in-house developed tools, we we utilize the following tools while conducting your penetration testing services.

Network Testing

Nessus	onesixtyone	Dnsenum	Custom Tools
Nessus	onesixtyone	Dnsenum	Custom Tools
Nmap	Firewalk	Commando VM	Raspberry pi
Wireshark	Sslscan	AppScan	MITM6
Metasploit	Tcpdump	Masscan responder	Yersinia
OpenVAS	Dsniff	Bettercap	crackmapexec
EvilWinRM	hping3	testssl.sh	Social Engineering Toolkit
Maltego			

Wi-Fi

Aircrack- ng suite	Raspberry pi	bettercap	Wifite
EAPHammer	Hostpad-wpe	Kismet	Wireshark

Web App Testing / API

AppScan	WebInspect	Burp Suite Pro	Sqlmap
Hashcat	SOAPUI	Swagger	

RedTeam

Covenant	Silenttrinity	GoPhish
Covenant	Silenttrinity	GoPhish
Raspberry pi	Maltego	Custom Tools

Exhibit B

Federal Clauses

RedTeam Collaborative LLC dba RedTeam Security, (“hereinafter Contractor”), understands and acknowledges that this Agreement may be totally or partially funded with federal and or state funds from the Department of Homeland Security and or the Office of the Governor. As a condition of receiving these funds, Contractor represents that it is and will remain in compliance with all federal and or state terms as stated below. These terms flow down to all third party contractors and their subcontracts at every tier that exceed the simplified acquisition threshold, unless a particular award term or condition specifically indicates otherwise. The Contractor shall require that these clauses shall be included in each covered transaction at any tier.

1. ADA Access.

The Contractor agrees to comply with all applicable provisions of section 504 of the Rehabilitation Act of 1973, as amended, with 29 U.S.C. § 794, which prohibits discrimination on the basis of disability; with the Americans with Disabilities Act of 1990 (ADA), as amended, 42 U.S.C. §§ 12101 et seq., which requires that accessible facilities and services be made available to individuals with disabilities; and with the Architectural Barriers Act of 1968, as amended, 42 U.S.C. §§ 4151 et seq., which requires that buildings and public accommodations be accessible to individuals with disabilities, and any subsequent amendments to these laws; (4) U.S. DOJ regulations, "Nondiscrimination on the Basis of Disability in State and Local Government Services," 28 C.F.R. Part 35; (5) U.S. DOJ regulations, "Nondiscrimination on the Basis of Disability by Public Accommodations and in Commercial Facilities," 28 C.F.R. Part 36; (6) U.S. General Services Administration (U.S. GSA) regulations, "Accommodations for the Physically Handicapped," 41 C.F.R. Subpart 101-19; (7) U.S. EEOC, "Regulations to Implement the Equal Employment Provisions of the Americans with Disabilities Act," 29 C.F.R. Part 1630.

2. Child Support.

Per Texas Family Code 231.006, a child support obligor or business entity remains ineligible to receive payments from state funds under a contract to provide property, materials, or services; or a state funded loan until: (1) all arrearages have been paid; (2) the obligor is in compliance with a written repayment agreement or court order as to any existing delinquency; or (3) the court of continuing jurisdiction over the child support order has granted the obligor an exemption from ineligibility as part of a court-supervised effort to improve earnings and child support payments.

Before payment can be released Contractor will supply County with the name and social security number of the individual or sole proprietor and each partner, shareholder, or owner with an ownership interest of at least 25 percent of the business entity.

Under Section 231.006, Family Code, the Contractor certifies that the individual or business entity named in this contract, bid, or application is not ineligible to receive the specified grant, loan, or payment and acknowledges that this contract may be terminated and payment may be withheld if this certification is inaccurate.

3. Civil Rights/Nondiscrimination Requirements.

Contractor will comply, with the nondiscrimination requirements which may include the Civil Rights Act of 1964 (42 USC § 2000d); the Civil Rights Act of 1968 (42 USC § 3601 et seq.); the Rehabilitation Act of 1973 (29 USC § 794); the Americans with Disabilities Act (ADA) of 1990 (42 USC § 12131-34); the Education Amendments of 1972 (USC §§ 1681, 1683, 1685-86); Title IX of the Education Amendments of 1972 (Equal Employment in Education Act) (20 USC § 1681 et seq.); the Age Discrimination Act of 1975 (42 USC §§ 6101-07); Titles I, II and III of the Americans with Disabilities Act; the Drug Abuse and Treatment Act of 1972 (PL 92-255); the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970 (PL 91-616); Sections 523 and 527 of the Public Health Service Act of 1912 (42 USC §§ 290dd-3 and 290ee-3); and 28 CFR 38 (Equal Treatment for Faith-Based Organizations); see Ex. Order 13279 (equal protection of the laws for faith-based and community organizations) and Ex. Order 13559 (fundamental principles and policymaking criteria for partnerships with faith-based and neighborhood organizations).

More specifically, Contractor will comply with:

a. Americans with Disabilities Act of 1990. Contractor must comply with the requirements of Titles I, II, and III of the Americans with Disabilities Act, Pub. L. No. 101-336 (1990) (codified as amended at 42 U.S.C. Sections 12101- 12213), which prohibits recipients of federal funds from discriminating on the basis of disability in the operation of public entities, public and private transportation systems, places of public accommodation, and certain testing entities.

b. Civil Rights Act of 1968. Contractor must comply with Title VIII of the Civil Rights Act of 1968, Pub. L. No. 90- 284, as amended through Pub. L. 113-4, which prohibits recipients of federal funds from discriminating in the sale, rental, financing, and advertising of dwellings, or in the provision of services in connection therewith, on the basis of race, color, national origin, religion, disability, familial status, and sex (see 42 U.S.C. Section 3601 et seq.), as implemented by the U.S. Department of Housing and Urban Development at 24 C.F.R. Part 100. The prohibition on disability discrimination includes the requirement that new multifamily housing with four or more dwelling units-i.e., the public and common use areas and individual apartment units (all units in buildings with elevators and ground-floor units in buildings without elevators)-be designed and constructed with certain accessible features. (See 24 C.F.R. Section 100, Subpart D).

c. Limited English Proficiency

Contractor must comply with Title VI of the Civil Rights Act of 1964 (42 U.S.C. Section 2000d et seq.) prohibition against discrimination on the basis of national origin, which requires that recipients of federal financial assistance take reasonable steps to provide meaningful access to persons with limited English proficiency (LEP) to their programs and services. For additional assistance and information regarding language access obligations, please refer to the DHS Recipient Guidance at https://www.dhs.gov/guidance-published-help-department-supported-organizations-provide-meaningful-access-people-limited and additional resources on http://www.lep.gov.

d. Civil Rights Act of 1964-Title VI. Contractors must comply with the requirements of Title VI of the Civil Rights Act of 1964 (codified as amended at 42 U.S.C. Section 2000d et seq.), which provides that no person in the United States will, on the grounds of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving federal financial assistance. DHS implementing regulations for the Act are found at 6 C.F.R. Part 21 and 44 C.F.R. Part 7.

e. Rehabilitation Act of 1973. Contractor must comply with the requirements of Section 504 of the Rehabilitation Act of 1973, (29 U.S.C. Section 794), as amended, which provides that no otherwise qualified handicapped individuals in the United States will, solely by reason of the handicap, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving federal financial assistance.

f. Nondiscrimination in Matters Pertaining to Faith-Based Organizations. It is DHS policy to ensure the equal treatment of faith-based organizations in social service programs administered or supported by DHS or its component agencies, enabling those organizations to participate in providing important social services to beneficiaries. Contractors must comply with the equal treatment policies and requirements contained in 6 C.F.R. Part 19 and other applicable statutes, regulations, and guidance governing the participations of faith-based organizations in individual DHS programs.

g. Education Amendments of 1972. Contractors must comply with the requirements of Title IX of the Education Amendments of 1972, Pub. L. No. 92-318 (1972) (codified as amended at 20 U.S.C. Section 1681 et seq.), which provide that no person in the United States will, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any educational program or activity receiving federal financial assistance. DHS implementing regulations are codified at 6 C.F.R. Part 17 and 44 C.F.R. Part 19.

h. Age Discrimination Act of 1975. Contractor must comply with the requirements of the Age Discrimination Act of 1975 (Title 42 U.S. Code, Section 6101 et seq.), which prohibits discrimination on the basis of age in any program or activity receiving federal financial assistance.

4. Compliance with Federal Law, Regulations, and Executive Orders.

Contractor's attention is called to the fact that this Agreement between County and Contractor will be subject to financial assistance contracts between the County and various State or Federal agencies. The Agreement to be awarded, therefore, is subject to the terms of these agreements and will not proceed without these agreements having been duly executed. The Contractor will be required to comply with, in addition to other provisions of the agreement, the conditions required by applicable federal regulations. Contractor will comply will all applicable federal law, regulations, executive orders, policies, procedures, and directives.

5. Contracting with Small, Minority Firms, Women's Business Enterprises and Labor Surplus Area Firms.

Contractor will take all necessary, affirmative steps to assure that qualified small and minority businesses, women's business enterprises, and labor area surplus firms are used when possible by:

a) Placing small and minority businesses and women's business enterprises on solicitation lists;
b) Assuring that it solicits small and minority businesses and women's business enterprises whenever they are potential sources;
c) Dividing total requirements, *when economically feasible*, into smaller tasks or quantities to permit maximum participation by small and minority businesses and women's business enterprises;
d) Establishing delivery schedules, *where the requirement permits*, which encourage participation by small and minority businesses and women's business enterprises;
e) Utilizing the assistance, as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce;
f) Contractor must require subcontractors to take the five affirmative steps described in a-e above.

6. Cooperation with Monitoring, Audits and Records Requirements.

The Contractor agrees to cooperate with the Office of the Governor and any relevant federal agency generally, including on any compliance review or complaint investigation conducted by the Federal sponsoring agency or the Office of the Governor and on all grant monitoring requests, including requests related to desk reviews, enhanced programmatic desk reviews, and/or site visits.

The Contractor shall maintain adequate records that enable the Office of the Governor and any relevant federal agency to complete monitoring tasks, including to verify all reporting measures, requests for reimbursements, and expenditure of match funds related to this Grant Agreement. The Contractor shall maintain such records as are deemed necessary by the Office of the Governor, the State Auditor's Office, other auditors of the State of Texas, the federal government or such other persons or entities designated or authorized by the Office of the Governor to ensure proper accounting for all costs and performances related to this Grant Agreement.

The Office of the Governor may request documented proof of payment. Acceptable proof of payment includes, but is not necessarily limited to, a receipt or other documentation of a paid invoice, a general ledger detailing the specific revenue and expenditures, a monthly bank statement evidencing payment of the specific expenditure, bank reconciliation detail, copies of processed checks, or a printed copy of an electronic payment confirmation evidencing payment of the specific expenditure to which the reimbursement relates.

The Contractor authorizes DHS, the Office of the Governor, the Texas State Auditor's Office, the Comptroller General of the United States, and any relevant federal agency, and their representatives, the right to audit, examine, and copy all paper and electronic records, books,

documents, accounting procedures, practices, and any other requested records, in any form; relevant to this Agreement and will make them readily available upon request. The Contractor will similarly permit access to facilities, personnel, and other individuals and information as may be necessary.

If requested, the Contractor shall submit to the Office of the Governor a copy of its most recent independent financial audit, any audited financial statements, related management letters and management responses of Contractor, and financial audit documents or portions thereof that are directly related to the Contractor's performance of its obligations under this Agreement.

The Office of the Governor may make unannounced monitoring visits at any time but will, whenever practical as determined at the sole discretion of the Office of the Governor, provide the Contractor with up to five (5) business days advance notice of any such examination or audit. Any audit of records shall be conducted at the Contractor’s principal place of business and/or the location(s) of the Contractor's operations during the Contractor's normal business hours. The Contractor shall provide to the Office of the Governor or its designees, on the Contractor's premises, private space, office furnishings (including lockable cabinets), telephone services and Internet connectivity, utilities, and office-related equipment and duplicating services as the Office of the Governor or its designees may reasonably require to perform the audits described in this section.

In addition to the information contained in the required reports, other information may be required as requested by the Office of the Governor, including the Office of the Governor asking for more information regarding project performance or funds expenditures. In the event the Office of the Governor requires additional information regarding the information or data submitted, the Contractor will promptly provide the additional information. The Contractor also agrees to assist the Office of the Governor in responding to questions and assisting in providing information responsive to any audit, legislative request, or other inquiry regarding the grant award. Upon the request of the Office of the Governor, the Contractor must submit to the Office of the Governor any additional documentation or explanation the Office of the Governor may desire to support or document the requested payment or report submitted under this Agreement.

If after a written request by the Office of the Governor or a relevant federal agency, the Contractor fails to provide required reports, information, documentation, or other information within reasonable deadlines set by the Office of the Governor or the relevant federal agency, as required by this Agreement, or fails to fulfil any requirement in this section, then the Office of the Governor may consider this act a possible default under this Agreement, and the Contractor may be subject to sanctions including but not limited to, withholdings and/or other restrictions on the access to funds; referral to relevant agencies for audit review; designation of the Contractor as a high-risk Contractor; or termination of awards.

7. Debt to State

The State shall not be responsible for any debts associated with this Agreement.

8. DHS Specific Acknowledgements and Assurances.

All Contractors, successors, transferees, and assignees must acknowledge and agree to comply with applicable provisions governing DHS access to records, accounts, documents, information, facilities, and staff.

a. Contractor must cooperate with any compliance reviews or compliance investigations conducted by DHS.
b. Contractor must give DHS access to, and the right to examine and copy, records, accounts, and other documents and sources of information related to the federal financial assistance award and permit access to facilities, personnel, and other individuals and information as may be necessary, as required by DHS regulations and other applicable laws or program guidance.
c. Contractor must submit timely, complete, and accurate reports to the appropriate DHS officials and maintain appropriate backup documentation to support the reports.
d. Contractor must comply with all other special reporting, data collection, and evaluation requirements, as prescribed by law or detailed in program guidance.

9. Drug-Free Workplace Regulations.

Contractor must comply with drug-free workplace requirements of 2 C.F.R. Part 3001, which adopts the Government-wide implementation (2 C.F.R. Part 182) of Sec. 5152-5158 of the *Drug-Free Workplace Act of 1988* (41 U.S.C. §§ 8101-8106).

10. Examination of Records.

The Contractor agrees to provide County, the Office of the Governor and U.S. Department of Homeland Security, the Comptroller General of the United States or any of their authorized representatives access to any books, documents, papers and records of the Contractor which are directly pertinent to the Agreement for the purposes of making audits, examinations, excerpts and transcriptions. The Contractor agrees to permit any of the foregoing parties to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed.

The Contractor agrees to comply and will require all subcontractors of any tier to comply with the record retention requirements in accordance with 2 C.F.R. 200.333. The Contractor agrees to retain, and will require its subcontractors of all tiers to retain, complete and readily accessible records related in whole or in part to the contract, including, but not limited to, all books, records, accounts, statistics, leases, subcontracts, arrangements other third party arrangements of any type, reports, and supporting materials related to those records required under the Agreement for a period of not less than three years after the date of termination or expiration of the Agreement, except in the event of litigation or settlement of claims arising from the performance of the Agreement, in which case Contractor agrees to maintain same until County, the Office of the Governor and U.S. Department of Homeland Security, the Comptroller General, or any of their duly authorized representatives, have disposed of all such litigation, appeals, claims or exceptions related thereto.

11. Federal Debt

Contractor is required to be non-delinquent in their repayment of any federal debt. Examples of relevant debt include delinquent payroll and other taxes, audit disallowances, and benefit overpayments. (See OMB Circular A-129).

12. Fly America.

The Contractor agrees to comply with Preference for U.S. Flag Air Carriers (air carriers holding certificates under 49 U.S.C. Section 41102) for international air transportation of people and property to the extent that such service is available, in accordance with the International Air Transportation Fair Competitive Practices Act of 1974 (49 U.S.C. Section 40118) and the interpretative guidelines issued by the Comptroller General of the United States in the March 31, 1981 amendment to Comptroller General Decision B-138942.

And with 49 U.S.C. 40118 (the "Fly America" Act) in accordance with the General Services Administration's regulations at 41 C.F.R. Part 301-10, which provide that recipients and sub-recipients of Federal funds and their contractors are required to use U.S. Flag air carriers for U.S. Government-financed international air travel and transportation of their personal effects or property, to the extent such service is available, unless travel by foreign air carrier is a matter of necessity, as defined by the Fly America Act. The Contractor shall submit, if a foreign air carrier was used, an appropriate certification or memorandum adequately explaining why service by a U.S. flag air carrier was not available or why it was necessary to use a foreign air carrier and shall, in any event, provide a certificate of compliance with the Fly America requirements. The Contractor agrees to include the requirements of this section in all subcontracts that may involve international air transportation.

13. Government-wide Debarment and Suspension.

The Contractor shall comply and facilitate compliance with the U.S. Office of Management and Budget (U.S. OMB) “Guidelines to Agencies on Governmentwide Debarment and Suspension (Nonprocurement),” 2 C.F.R. part 180. A contract award in any tier must not be made to parties listed on the government wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 C.F.R. § 180 that implement Executive Orders Nos. 12549 (3 C F R part 1986 Comp., p. 189) and 12689 (3 C.F.R. part 1989 Comp., p. 235), “Debarment and Suspension.” SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order No. 12549. These provisions apply to each contract at any tier of $25,000 or more, and to each contract at any tier for a federally required audit (irrespective of the contract amount).

This certification is a material representation of fact relied upon by the County. If it is later determined that the Contractor did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to DHS and County, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.

Contractor agrees to comply with the requirements of 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The Contractor further agrees to include a provision requiring such compliance in its lower tier covered transactions.

14. Health and Human Services, Public Safety or Law Enforcement Agency Compliance

Contractor certifies that it as owner, operator or administrator of a facility has not had any licenses, certificates, or permits revoked by any health and human service agency or public safety or law enforcement agency.

15. Program Fraud, False Claims Act and Program Fraud Civil Remedies.

Contractor understands that County does not tolerate any type of fraud, waste or misuse of funds. Contractor shall comply with the requirements of the False Claims Act (31 U.S.C. Section 3729-3733) which prohibits the submission of false or fraudulent claims for payment to the federal government. Contractor understands and agrees that misuse of funds may result in a range of penalties, including suspension of current and future funds, suspension or debarment from federal and state grants, recoupment of monies provided under an award, and civil and/or criminal penalties. (See 31 U.S.C. Section 381-3812 which details the administrative remedies for false claims and statements made.)

The Contractor agrees to include the above clause in each subcontract financed in whole or in part with funds from this Agreement.

16. Domestic Preferences for Procurements.

As appropriate and to the extent consistent with law, Contractor shall to the greatest extent practicable, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). The requirements of this section must be included in all subawards including all contracts and purchase orders for work or products procured with federal funds. For purposes of this clause, (1) “Produced in the United States” means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States. (2) “Manufactured products” means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

17. Reporting of Fraud, Waste, and Abuse.

In the event, County becomes aware of any allegation or a finding of fraud, waste, or misuse of funds received for the performance of this Agreement, the County is required to immediately notify OOG of said allegation or finding and to continue to inform OOG of the status of any such on-going investigations. The County must promptly refer to OOG any credible evidence that a principal, employee, agent, subrecipient, contractor, subcontractor, or other person has -- (1)

submitted a claim for award funds that violates the False Claims Act; or (2) committed a criminal or civil violation of laws pertaining to fraud, conflict of interest, bribery, gratuity, or similar misconduct involving award funds. County must also immediately notify OOG in writing of any misappropriation of funds, fraud, theft, embezzlement, forgery, or any other serious irregularities indicating noncompliance with grant requirements.

The County shall report any possible fraudulent or dishonest acts, waste, or abuse to OOG's Fraud Coordinator or Ethics Advisor at (512) 463-1788 or in writing to: Ethics Advisor, Office of the Governor, P.O. Box 12428, Austin, Texas 78711.

18. Restrictions and Certifications Regarding Non-Disclosure Agreements and Related Matters.

Contractor certifies that they have not required any employee or contractor to sign an internal confidentiality agreement or statement that prohibits or otherwise restricts, or purports to prohibit or restrict, the reporting (in accordance with law) of waste, fraud, or abuse to an investigative or law enforcement representative of a state or federal department or agency authorized to receive such information.

19. National Environmental Policy Act.

Contractor must comply with the requirements of the National Environmental Policy Act (NEPA) and the Council on Environmental Quality (CEQ) Regulations for Implementing the Procedural Provisions of NEPA, which requires recipients to use all practicable means within their authority, and consistent with other essential considerations of national policy, to create and maintain conditions under which people and nature can exist in productive harmony and fulfill the social, economic, and other needs of present and future generations of Americans.

20. No Obligation by Federal Government.

The Federal Government is not a party to this Agreement and is not subject to any obligations or liabilities to the County, Contractor, or any other party pertaining to any matter resulting from the Agreement.

21. Notice of Funding Opportunity.

All of the instructions, guidance, limitations, and other conditions set forth in the federal Notice of Funding Opportunity (NOFO) for this program are incorporated here by reference in the award terms and conditions.

22. Political Activities.

Contractor must comply with 31 U.S.C. Section 1352, which provides that none of the funds provided under a federal financial assistance award may be expended by the recipient to pay any person to influence, or attempt to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee or a Member of Congress in

connection with any federal action related to a federal award or contract, including any extension, continuation, renewal, amendment, or modification.

23. Best Practices for Collection and Use of Personally Identifiable Information (PII)

If Contractor collects Personally Identifiable Information (PII), they are required to have a publically-available privacy policy that describes standards in the usage and maintenance of PII they collect. DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual. Recipients may also find the DHS Privacy Impact Assessments: Privacy Guidance and Privacy template as useful resources respectively.

24. Prohibited Telecommunications and Video Surveillance Services and Equipment.

Contractor understands and acknowledges that under 2 CFR 200.216, the County is prohibited from using federal funds to procure, obtain, extend or renew a contract to procure or obtain covered telecommunications equipment or services, including telecom equipment produced by Huawei Technologies Company or ZTE Corp. (or subsidiaries or affiliates of such entities).

Contractor, therefore, certifies that they are in compliance with the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018), and that in the performance of this agreement, it will not provide equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. As described in Public Law 115-232, section 889, covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

> **(i)** For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).
>
> **(ii)** Telecommunications or video surveillance services provided by such entities or using such equipment.
>
> **(iii)** Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

25. Prompt Payment.

The Contractor is required to pay its subcontractors performing work related to this Agreement for satisfactory performance of that work no later than 30 days after the Contractor's receipt of payment for that work from County. In addition, the Contractor is required to return any retainage

payments to those subcontractors within 30 days after the subcontractor's work is satisfactorily completed.

26. Procurement of Recovered Materials.

Contractor must comply with Section 6002 of the Solid Waste Disposal Act, Pub. L. No. 89-272 (1965) (codified as amended by the Resource Conservation and Recovery Act, 42 U.S.C. section 6962). The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 C.F.R. Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition.

27. Retention of Records

The Contractor agrees to maintain fiscal records and supporting documentation for all expenditures related to this Agreement pursuant to 2 CFR 200.333, UGMS, and state law. Contractor must retain, and will require its subcontractors of all tiers to retain, these records and any supporting documentation for a minimum period of not less than three (3) years after the date of termination or expiration of the Agreement or any litigation, dispute, or audit arising from the performance of the Agreement. Records related to real property and equipment acquired with grant funds shall be retained for three (3) years after final disposition. If requested by the Office of the Governor's Homeland Security Grant Division (HSGD), the County may direct the Contractor to retain documents for a longer period of time or transfer certain records to HSGD custody when it is determined the records possess longer term retention value.

28. Rights to Inventions Made Under a Contract or Agreement.

Contractor is subject to the Bayh-Dole Act, 35 U.S.C. section 200, unless otherwise provided by law. Contractors are subject to the specific requirements governing the development, reporting, and disposition of rights to inventions and patents resulting from federal financial assistance awards located at 37 C.F.R. Part 401 and the standard patent rights clause located at 37 C.F.R. Section 404.14.

29. SAFECOM

Any emergency communication equipment and its related activities provided as a part of this Agreement must comply with the SAFECOM Guidance for Emergency Communication Grants, including provisions on technical standards that ensure and enhance interoperable communications.

30. Termination for Cause and Termination for Convenience.

Contractor understands that all contracts in excess of $10,000, including subcontracts, must address termination for cause and for convenience by the non-Federal entity including the manner by which it will be effected and the basis for settlement.

31. Terrorist Financing.

Contractor must comply with E.O. 13224 and U.S. law that prohibit transactions with, and the provisions of resources and support to, individuals and organizations associated with terrorism.

32. Text Messaging While Driving.

Contractor is encouraged to adopt and enforce policies that ban text messaging while driving as described in E.O. 13513, including conducting initiatives described in Section 3(a) of the Order when on official government business or when performing any work for or on behalf of the federal government.

33. Trafficking Victims Protection Act.

Contractor will comply with the requirements of Section 106(g) of the Trafficking Victims Protection Act (TVPA) of 2000, as amended (22 U.S.C. 7104) which prohibits grant award recipients or a sub-recipient from awarding funds to a private entity or individual who has (1) engaged in severe forms of trafficking in persons during the period of time that the award is in effect; (2) procured a commercial sex act during the period of time that the award is in effect or (3) used forced labor in the performance of the award or subawards under the award. Contractor shall inform County immediately upon receipt of any information from any source alleging a violation of a prohibition of the TVPA. Violation of this clause, may result in termination of this Agreement.

34. USA Patriot Act of 2001.

Contractor must comply with requirements of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), which amends 18 U.S.C. Sections 175-175c.

35. Use of DHS Seal, Logo and Flags.

Contractor must obtain permission from DHS, prior to using the DHS seal(s), logos, crests or reproductions of flags or likenesses of DHS agency officials, including use of the United States Coast Guard seal, logo, crests or reproductions of flags or likenesses of Coast Guard officials.

36. Veteran Preference.

The Contractor shall give a hiring preference, to the extent practicable, to veterans (as defined in 5 USC Section 2108) who have the requisite skills and abilities to perform the construction work required under the contract. This subsection shall not be understood, construed or enforced in any manner that would require an employer to give preference to any veteran over any equally qualified

applicant who is a member of any racial or ethnic minority, female, an individual with a disability, or former employee.

37. Whistleblower Protections.

Contractor must comply with the statutory requirements for whistleblower protections (if applicable) at 10 U.S.C Section 2409, 41 U.S.C. 4712, and 10 U.S.C. Section 2324, 41 U.S.C. Sections 4304 and 4310.

CERTIFICATE OF INTERESTED PARTIES

FORM 1295

Complete Nos. 1 - 4 and 6 if there are interested parties.
Complete Nos. 1, 2, 3, 5, and 6 if there are no interested parties.

OFFICE USE ONLY
CERTIFICATION OF FILING

Certificate Number:
2021-829218

Date Filed:
12/03/2021

Date Acknowledged:
12/14/2021

1 Name of business entity filing form, and the city, state and country of the business entity's place of business.

RedTeam Security
Saint Paul, MN United States

2 Name of governmental entity or state agency that is a party to the contract for which the form is being filed.

Fort Bend County

3 Provide the identification number used by the governmental entity or state agency to track or identify the contract, and provide a description of the services, goods, or other property to be provided under the contract.

34279
Cyber Security Training & Planning

4 Name of Interested Party	City, State, Country (place of business)	Nature of interest (check applicable)	
		Controlling	Intermediary
RedTeam Security	Saint Paul, MN United States	X	

5 Check only if there is NO Interested Party. ☐

6 UNSWORN DECLARATION

My name is _____, and my date of birth is _____.

My address is _____, _____, _____, _____, _____.
(street) (city) (state) (zip code) (country)

I declare under penalty of perjury that the foregoing is true and correct.

Executed in _____County, State of _____, on the _____day of _____, 20_____.
(month) (year)

_____
Signature of authorized agent of contracting business entity
(Declarant)