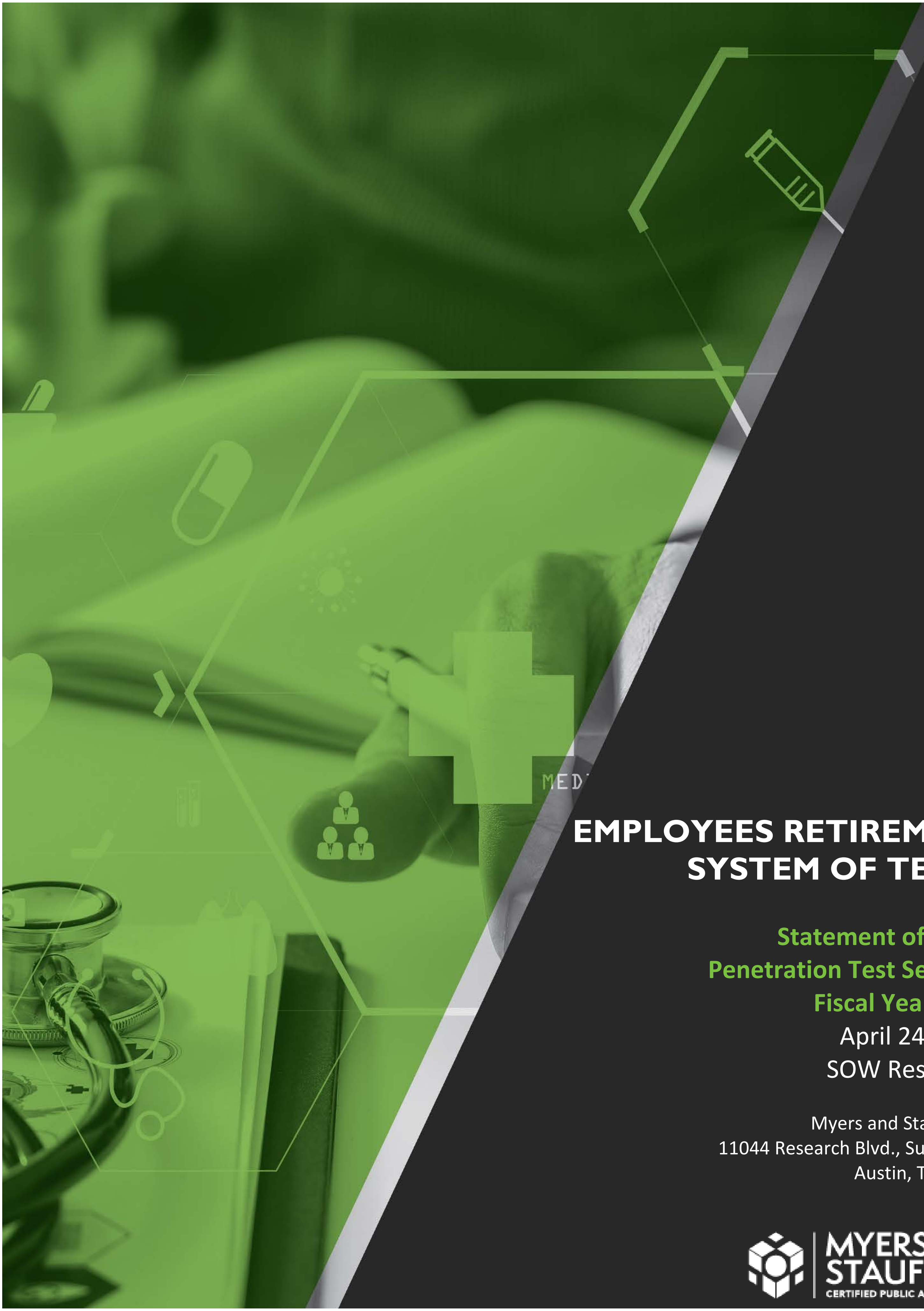


EMPLOYEES RETIREMENT SYSTEM OF TEXAS

Statement of Work
Penetration Test Services
Fiscal Year 2020

April 24, 2020

SOW Response

Myers and Stauffer LC
11044 Research Blvd., Suite C500
Austin, TX 78759

MYERS AND STAUFFER LC
CERTIFIED PUBLIC ACCOUNTANTS

MYERS AND STAUFFER LC
CERTIFIED PUBLIC ACCOUNTANTS

April 24, 2020

IS Administration
Employees Retirement System of Texas
200 E. 18th St.
Austin, TX 78701

Dear Members of IS Administration:

Myers and Stauffer LC is pleased to respond to the Employees Retirement System of Texas's (ERS) Statement of Work (SOW) to perform penetration testing services for three years, beginning in state fiscal year (FY) 2020. We are excited about the possibility of continuing our working relationship with ERS, and we are confident that our team has the resources to serve you effectively and efficiently.

As you will see, our experience is relevant to your needs and includes numerous cybersecurity assessments, including penetration testing services, for both public entities and government organizations across the country – including employee retirement systems.

Tiffany Garcia, Director, in our Austin, Texas office, will have overall responsibility for the services we provide to you. The Senior Manager assigned to you is Kim Bradley. Your project team consists of personnel and subject matter resources based in our Austin office. These professionals have the knowledge, skills, and experience to meet and exceed the needs described by ERS in the SOW. Specific to this engagement, our team has more than 15 years of experience providing cybersecurity assessment services to government agencies, including penetration testing, Internet (external) vulnerability assessments, network (internal) vulnerability assessments, and web application testing, as well as providing security-focused consulting services to governmental entities to assist in efforts to improve security, identify risk levels, and develop appropriate responses to mitigate risks. Our team members also have substantial experience providing services to assess information technology (IT) security for state agencies that are responsible for managing large investment portfolios to support their stakeholders, including with the ERS, [redacted]

If awarded, we will be performing this work under our current master contract with the Texas Department of Information Resources (DIR), contract # DIR-TSO-3748.

In conclusion, it is our most sincere hope that our response to the SOW clearly indicates that Myers and Stauffer is uniquely qualified to provide you with not only services that meet the specifications of the SOW, but also the insight, information, and open communication that will benefit the ERS. If you have any questions or require additional information, please contact me at 512.340.7423 or TGarcia@mslc.com.

Sincerely,

Tiffany Garcia, CISA, CICA
Director

Statement of Work
Penetration Test Services
FY 2020

ERS
EMPLOYEES RETIREMENT
SYSTEM OF TEXAS

Table of Contents

Introduction/Background

The Employees Retirement System of Texas (ERS) is a constitutional trust fund established as mandated by Article XVI, Section 67, Texas Constitution, and further organized pursuant to Subtitle B, Title 8, Texas Government Code, as well as 34 Texas Administrative Code, Sections 61.1, et seq. ERS administers a retirement and disability pension plan for state employees, law enforcement and custodial officers, elected state officials and two classes of judges (in this context, hereinafter referred to as Members). ERS invests state and Member contributions in the retirement trust funds and administers the trust funds with a fiduciary obligation to the members and retirees of ERS who are its beneficiaries. ERS also administers the Texas Employees Group Benefits Program, which consists of health benefits, life insurance, and other optional benefits, to participating individuals eligible to receive those benefits under applicable law.

Scope

ERS seeks the services of an experienced vendor to conduct external controlled penetration testing (CPT) for three years as set forth in the schedule of events section below. The vendor will assess and rate ERS's network security against:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.

To attempt to meet these objectives the vendor will test ERS's network security through public Internet connectivity. The results will assist ERS with improving its security posture based on its security needs.

The vendor will conduct the CPT based on the two objectives listed above and provide ERS with reports detailing the findings. The vendor will conduct the CPT from the publically accessible Internet using freeware, shareware, custom scripts, and commercially available software. The successful vendor will attempt to test and probe for security vulnerabilities and exploit vulnerabilities on all discoverable devices and hosts within the specified IP range and ERS's primary URLs and all sub-links attached to ERS's network. All discovered devices and hosts within ERS's network and system administrative control will be subject to testing on a 24/7 basis until complete, except for those specifically excluded by ERS, which will be provided to the awarded vendor. The vendor will focus only on those deemed vulnerable and exploitable.

Deliverables and Activities during the Engagement

Vendor will perform numerous activities required for the completion of the CPT, including:

- Use commercially available software, freeware, shareware, and custom scripts to conduct network reconnaissance, vulnerability analysis, and limited exploits of areas deemed most vulnerable.
- Conduct redundant automated vulnerability scanning of the network range and URLs provided by ERS.
- Probe for firewalls, intrusion detection systems, and access control lists and search for back doors.
- Collect user accounts and passwords, where accessible, and attempt privilege escalation. In most cases, this requires that software be transferred to, compiled on, or temporarily installed on ERS's systems. The vendor will attempt to remove all tools, utilities, and/or files, with the

exception of authorized artifacts or files/tools necessary to be shown or demonstrated in the subsequent technical report.

Other possible activities include:

Artifacts Left Behind

- Added user accounts (intrusion test accounts created during the CPT).
- Password modifications (changing end user passwords).
- Text files indicating that the vendor gained access (a new file created containing the text VENDOR WAS HERE).

Authorized Retrieval Items

- Mirroring or scraping the website (collecting all web pages and information associated with ERS's site).
- Collection of documents/files (may include files with doc, txt, xls, pdf, ppt, etc.,extensions).
- DNS zone files (transfer of internal Domain Name Service zone files that identify internal systems).
- Router/infrastructure equipment configuration files.
- Database query results.

Services That May Be Redirected

- DNS traffic.
- Intrusion detection systems (IDS).
- Login services.
- Printer/scanning storage devices.
- Simple Network Management Protocol (SNMP).
- System logging.

Services That May Be Stopped/Restarted

The following services may be stopped or restarted during the CPT, but only with prior approval by ERS:

- World Wide Web.

Reports and Meetings

1. ERS and the vendor will schedule and conduct meetings with appropriate business staff.
2. ERS will provide vendor with full access to the relevant functional, technical, and business resources with adequate skills and knowledge.
3. The vendor will have staff available to answer questions regarding billing and invoices.
4. The vendor will participate in meetings after each draft report is developed in order to determine the gaps which may remain in the final report.
5. The vendor will provide ERS with the following deliverables resulting from the test:
    a. Custom report providing ERS with findings, a summary of activities, vulnerabilities identified, and all exploit cases describing how objectives were met.
    b. Reports generated from the automated vulnerability scanning tools.

c. Analysis, descriptions of, and recommendations for protecting against confirmed vulnerabilities and exploits used during the CPT.
d. Custom report providing ERS with summary of vulneralability statistics and findings suitable for public release.

6. The vendor will provide reports and conduct activity using the dates listed in the "SCHEDULE OF EVENTS AND RESPONSE MILESTONES" section of the SOW.

Service Level Agreement

The vendor agrees to cease all CPT activities within five (5) minutes upon request by ERS. This is required due to the impact which scanning could have on ERS' production network. Failure to stop all CPT activities within five (5) minutes upon request which have an impact on ERS' network will result in a 25% reduction in payment to the vendor.

Period of Performance/Schedule

The term of service for this Statement of Work commences upon signature by all parties on the Signature Page and shall extend until acceptance of the Year Three final report, due to ERS by June 2, 2022, or as otherwise mutually agreed.

Points of Contact

The contact for this SOW solicitation will be the IS Administration section; they can be contacted at isadministration@ers.texas.gov.

After award, contract communications for this SOW must be directed to ERS Contract Manager:

Joanna Gonzalez
200 E. 18th Street, Austin, Texas 78701
512.867.7137
joanna.gonzalez@ers.texas.gov

After award, security issues must be coordinated with the ERS Chief Information Security Officer:

Matt Remiersma
200 E. 18th Street, Austin, Texas 78701
512.867.7308
matt.remiersma@ers.texas.gov

Invoices and Payment/Acceptance Criteria

The vendor agrees that ERS will review all draft reports submitted by the vendor and make all changes to the report which are in scope of the SOW within 10 business days. The vendor agrees that ERS is the sole determination of completeness on the report, and final acceptance of all work by the vendor and the final report is dependent upon acceptance by ERS.

ERS will pay an invoice for the services when the reports are submitted and accepted by ERS in accordance with the Prompt Payment Act.

The vendor must submit invoices to ERS by mail: P.O. Box 13207, Austin, Texas 78711-3207, or by email: ap@ers.texas.gov with cc: isadministration@ers.texas.gov.

ERS/Vendor-Furnished Equipment

The vendor must furnish all equipment, hardware and software, for the completion of the SOW.

Additional Requirements

1. ERS will review and approve vendor's standard Certificate of Insurance (COI) prior to the commencement of services.
2. The vendor agrees to sign a Non-Disclosure Agreement for the term of this engagement.
3. The vendor agrees to sign an ERS HIPAA Business Associate Agreement and Data Security and Breach Notification Agreement.
4. The vendor may not access ERS member information.
5. ERS acknowledges that, other services may be affected; ERS's emergency contact will be notified in all cases where services are no longer responding and that the vendor's CPT actions are the cause of this activity.
6. Vendor shall use the Internet for access to ERS's systems unless by prior approval by ERS.
7. ERS shall not employ special access restrictions against vendor that it does not apply to the rest of the public network over the course of regular business.
8. ERS may block all access to the vendor as a result of determining that the IP address is performing scanning. After the initial scan, if the CPT must proceed using the vendor IP range, ERS will add the IP address range to the non-shun (whitelist) within the ERS IDS/IPS or other firewalls upon notification to ERS.
9. Vendor will not conduct any deliberate Denial-of-Service attack.
10. If either party becomes aware of a service interruption, that party will notify the other party's emergency contact as outlined in the Service Level Agreement.
11. ERS will provide IP ranges to use for scanning.
12. ERS will provide IP ranges and addresses to exclude from scanning.
13. If the selected DIR Prime vendor decides to subcontract any part of the contract in a manner that is not consistent with DIR's HUB subcontracting plan (Appendix B of the DIR Cooperative Contract), the selected DIR Prime vendor must comply and submit a revised HUB subcontracting plan to DIR before subcontracting any of the work under the SOW. No work may be performed by a subcontractor before DIR has approved a revised HSP for the Cooperative Contract.
14. Vendor will perform FBI criminal background checks on assigned staff prior to the start of the engagement; only the outcome of the report may be shared with ERS.
15. House Bill (HB) 3834 requires any Vendor, or a subcontractor, officer, or employee of Vendor, who will have access to a state computer system or database, then the Vendor shall ensure that such officer, employee, or subcontractor has also completed the required cybersecurity training. ERS will accept proof of security awareness training from programs certified by the Texas Department of Information Resources. (https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Certified%20Training%20Programs.docx)

Vendor Response

Vendor should use this section to provide descriptions of any changes, assumptions, exclusions and clarifications to the SOW services.

Myers and Stauffer agrees to the additional requirements listed above, and has no changes, exclusions, or clarifications. Per the Assumptions/Requirements section of the SOW, Myers and Stauffer agrees to sign a Non-Disclosure Agreement for the term of this engagement, along with an ERS Health Insurance Portability and Accountability Act (HIPAA) Business Associate Agreement and Data Security and Breach Notification Agreement pending review from our legal counsel.

Staff Capabilities

Vendor should use this section to describe the staff assigned to the services and their qualifications.

At Myers and Stauffer, we know our engagements will not be successful unless we provide our clients with the highest-quality, responsive, and experienced professionals. We are committed to performing the work established in the SOW and have the available resources to efficiently and effectively manage this project. Our resources and experience allow us to quickly respond to multiple tasks, regardless of engagement size.

The ERS will be served by professionals on our Systems Integrity Team located in our Austin, Texas, office. These professionals have the knowledge, skills, and experience to meet and exceed the needs described by ERS in the SOW. Specific to this engagement, our team has more than 15 years of experience providing cybersecurity assessment services to government agencies, including penetration testing, Internet (external) vulnerability assessments, and network (internal) vulnerability assessments, as well as providing security-focused consulting services to governmental entities to assist in efforts to improve security, identify risk levels, and develop appropriate responses to mitigate risks. The individuals proposed for this engagement also performed the penetration testing services for ERS in FY 2019. Our team members also have substantial experience providing services to assess IT security for state agencies that are responsible for managing large investment portfolios to support their stakeholders, including with the ERS, [redacted] Our team has also performed numerous assessments of compliance with the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 and the NIST Cybersecurity Framework; Center for Internet Security (CIS) Benchmarks; Texas Administrative Code Chapter 202; Texas DIR Security Control Standards Catalog; and the HIPAA Privacy, Breach Notification, and Security Rules, to name a few.

Our team is comprised of dedicated and experienced security and IT audit professionals armed with the relevant major technical certifications including:

- Certified Ethical Hacker. (CEH)
- Certified Information Systems Security Professional (CISSP).
- Certified Information Systems Auditor (CISA).
- Certified Internal Auditor (CIA).
- Certified Internal Controls Auditor (CICA).
- Certified Public Accountant (CPA).

Our staff members are required to obtain extensive continuing education to keep up with the ever-changing field of IT. We have also been trained and certified in the use of Nessus® Scanner and other automated testing tools for vulnerability assessment, wireless security testing, and penetration testing.

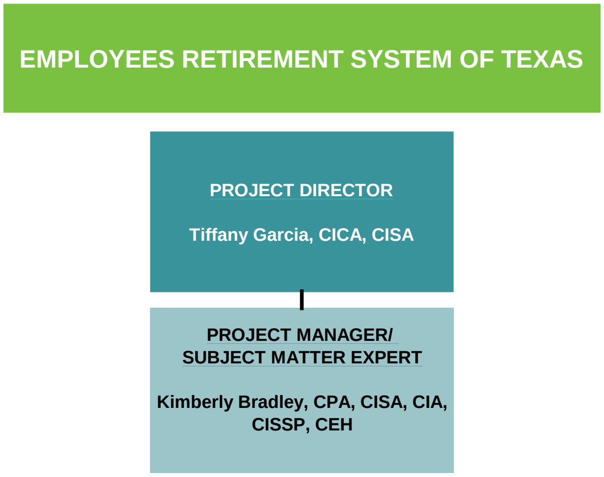
Project Director

For each large-scale project, we designate a Project Director, who will have overall responsibility for the contract, address all contractual issues, and guarantee top-quality service. The Project Director will also serve as the quality reviewer for the engagement to perform internal reviews of the work performed and of all deliverables. Ms. Tiffany Garcia, CICA, CISA, Director, will be the Project Director for this engagement with the ERS, if awarded. She has extensive experience performing IT and performance audits for the government sector, focusing on assessing the security and reliability of automated systems, and compliance with state and federal laws and regulations. She has led multiple projects for government clients that have included vulnerability assessments and/or penetration testing. She has also performed audits and various types of risk assessments for a range of industries, including oil and gas, manufacturing, industrial markets, investment firms, and financial services. Ms. Garcia has led and been responsible for several engagements [redacted], as well as the most recent ERS penetration testing services engagement. Ms. Garcia has demonstrated her knowledge in identifying, prioritizing, and managing risks to enhance performance and business value. In this capacity, she has assisted these entities in implementing effective internal controls and improving security over their IT systems, as well as helping them improve operations to become more effective and efficient.

Project Manager/Subject Matter Expert

For every engagement, we also designate a Project Lead/Manager who will lead and manage each project on a day-to-day basis, including managing all project activities, coordination, scheduling, planning, implementation, and reporting. We will assign Ms. Kimberly Bradley, CPA, CISA, CIA, CISSP, CEH, Senior Manager, as the Project Manager for the penetration testing services requested by ERS. She has more than 24 years of auditing and IT security experience primarily in state government, and more than 15 years of cybersecurity assessment and testing experience. She has led and performed numerous cybersecurity assessments, which have included vulnerability assessments, controlled penetration testing, social engineering testing, web application assessments, wireless assessments, and network device configuration assessments. Ms. Bradley serves as a subject matter expert for our cybersecurity testing and performed the penetration testing services for ERS in FY 2019. She will perform the controlled penetration testing services for this ongoing engagement with the ERS, if awarded.

The following organizational chart shows the key personnel who will perform the requested penetration testing services requested by the ERS.



EMPLOYEES RETIREMENT SYSTEM OF TEXAS

PROJECT DIRECTOR

Tiffany Garcia, CICA, CISA

PROJECT MANAGER/
SUBJECT MATTER EXPERT

Kimberly Bradley, CPA, CISA, CIA, CISSP, CEH

Service Capabilities

Vendor should use this section to describe the services to be provided. Please also provide redacted sample reports with your SOW submission.

General Approach to Services

During our more than 15 years providing IT risk assessment, audit, controls assessment, security assessment, cybersecurity testing, and IT risk assessments to government entities such as the ERS of Texas, we have developed and refined very successful plans and approaches in providing these services.

We will perform the engagement in three phases: Planning and Startup, Fieldwork, and Reporting.

Phase 1 – Planning and Startup

We would expect to start this phase upon execution of the contract with ERS. In general, our engagement planning phase will include ensuring we understand the engagement scope and objectives; gaining an understanding of the network environment being assessed; obtaining the technical information needed for the external network vulnerability assessment and controlled penetration testing; preparing the rules of engagement (ROE); and coordinating the external vulnerability assessment and penetration testing dates and times.

Phase 2 – Fieldwork

The fieldwork phase will include performing the work as identified in Phase 1 and as described further below in the External Penetration Testing and Web Application Testing sections.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]

- [redacted]
  - [redacted]
  - [redacted]

[redacted]

[redacted]

Phase 3 – Reporting

During the reporting phase, we will prepare all deliverables and provide them to the appropriate ERS contacts. To ensure deliverables are in the format desired by ERS, we will discuss and agree on deliverable formats with ERS early in the project.

During the reporting phase we will:

- Prepare a draft Executive Report and detailed Technical Report for ERS review and feedback.
- Conduct exit meeting or formal presentation of findings and recommendations (in person or via teleconference) with ERS representatives (if requested).
- Incorporate ERS feedback and provide the final reports no later than the agreed-upon delivery date.

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

See a redacted sample report located in *Appendix A: Sample Report* of our response.

Schedule of Events and Response Milestones

Please complete the table below with the dates for all activities.

Activity	Date
Testing Start Date – Year 1	[redacted]
Testing Stop Date – Year 1	[redacted]
Report Due Date – Year 1	[redacted]
Testing Start Date – Year 2	[redacted]
Testing Stop Date – Year 2	[redacted]
Report Due Date – Year 2	[redacted]
Testing Start Date – Year 3	[redacted]
Testing Stop Date – Year 3	[redacted]
Report Due Date – Year 3	[redacted]

<u>Note:</u> The testing start and stop dates and the timeframes outlined above encompass the various planning, fieldwork, and reporting activites for the project, for which the length of those activities may vary depending on various factors (e.g., fieldwork will start as soon as we obtain a signed Rules of Engagement, etc.). Also, the report due dates outlined above for each year are based on the expected vendor selection date of May 27, 2020, and the contract deadline of June 2, 2022, that are outlined in the SOW. We can coordinate with ERS to modify any of the testing start, testing stop, and report dates as or if needed each year to ensure we meet ERS's needs.

To further illustrate the activities performed as part of the engagement, we've included a sample milestone and timeline table below. Again, the length of these activities can vary (i.e. be shorter or longer) depending on timing and coordination with ERS.

Activity		Estimated Timeline
Planning and Startup	Conduct kick-off meeting and meetings with appropriate business staff as necessary.	Week 1
Planning and Startup	Obtain signed ROE and scan authorization.	Week 1
Fieldwork	Reconnaissance/discovery.	Week 2
Fieldwork	Perform assessment and penetration testing procedures on ERS external IP addresses and URLs.	Week 2 through 3/4
Fieldwork	Perform additional assessment and penetration testing procedures with IDS/IPS whitelisting if/as needed.	Week 2 through 3/4
Reporting	Draft report.	Week 4
Reporting	Provide draft report to ERS for review and comment/approval.	Week 5 and 6
Reporting	Conduct meetings, as necessary, to discuss results/draft report with ERS.	Week 5 and 6
Reporting	Incorporate any feedback/comments from ERS into draft report.	Week 5 and 6
Reporting	Finalize report and deliver final report to ERS.	Week 5 and 6

Pricing

The pricing listed below includes all the SOW costs – add lines, if necessary, for costs which should be considered but are not listed in the table. Finally, these are the fixed-fee, total, and complete costs to deliver the services described in the SOW.

Description	Cost
Penetration Test	
• Year 1 – Penetration test documentation and final report	[redacted]
• Year 2 – Penetration test documentation and final report	[redacted]
• Year 3 – Penetration test documentation and final report	[redacted]
Total – Penetration test documentation and final report (entire contract term)	[redacted]
Other costs (add lines if necessary)	
Total – Other Costs	*N/A*
Total – Entire Project	[redacted]

Change Requests

ERS and vendor affirm they are fully committed to completing this project on time and within budget. All scope changes must be reviewed by both ERS and vendor as soon as possible, but at least by the next status update meeting. The following outlines the change request procedure:

1. ERS and vendor will discuss the change request and mutually agree on the scope of the change.
2. ERS and the vendor's representative will document the change.
3. The vendor will determine the impact to the schedule and cost impact, if any.
4. ERS and vendor will make an addendum to the Statement of Work/contract.
   a. The vendor and ERS will sign the change request which contains the information listed in steps 1-4 above.
   b. Change orders and corresponding amendments will be submitted to DIR for their review and approval. An amendment to the SOW will hold the highest order of precedence in the SOW.
   c. ERS will execute the Purchase Order Change Notice (POCN) to the purchase order.

Myers and Stauffer understands and agrees to the above Change Request provisions.

Signatures/Acceptance

If awarded, we will be performing this work under our current master contract with the Texas DIR, contract # DIR-TSO-3748.

Accepted by: Myers and Stauffer LC Signature: Print Name: Tiffany Garcia Title: Director Date: April 23, 2020 DIR Contract #: DIR-TSO-3748	Accepted by: Employees Retirement System of Texas Signature: Print Name: Porter Wilson Title: Executive Director Date: ______________________________
	Accepted by: **Texas Department of Information Resources** Signature: ____ Print Name: Hershel Becker Title: Chief Procurement Officer Date: ______________________________

Appendix A: Sample Report

As requested in the Service Capabilities section of the SOW, we have included a redacted sample report for your review on the following pages.

No Name Agency
Vulnerability Assessment and Penetration Testing Services
Date

CONFIDENTIAL

This document is confidential and is not to be reproduced or distributed without the permission of No Name Agency management.

MYERS AND STAUFFER LC
CERTIFIED PUBLIC ACCOUNTANTS

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

TABLE OF CONTENTS

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]

[redacted]

[redacted]

[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted] [redacted]
- [redacted] [redacted]
- [redacted] [redacted]
- [redacted] [redacted]
  - [redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]