RFP SUBMISSION

A COMPREHENSIVE PROJECT

SUBMITTED TO THE

INFORMATION SYSTEMS AND CYBERSECURITY PROGRAM

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE ASSOCIATE'S DEGREE

by

Jesse Cabrera
Nicholas Rasa
Gerardo Cruz Conejo
Henry Jensen

Prepared for:
Melinda Wilson

Lone Star College

Houston, TX

December 2023

December 12, 2023

Texas State Government
Department of Finance and Administration
Jeremy Irons
1100 Congress Ave
Austin, TX 78701

Dynamic Defense, LLC
48 Security Way
Houston, TX 77001

RE: 427.04-107-08 – INFORMATION SECURITY ASSESSMENT SERVICES (ISAS)

Dear Mr. Irons,

Dynamic Defense LLC seeks to provide our dynamic security services to help you achieve superior technology defense for your company's goals. With over 18 years of experience providing vulnerability assessments, penetration testing, risk assessment, business continuity/ disaster recovery planning, we are your best defense against ever evolving threats. Last year was our record-breaking year, with us having annual sales exceeding 1.3 million dollars. Dynamic Defense is positioned to help you with your request for Vulnerability/ Risk assessment and Penetration testing.

In working with Dynamic Defense, you will benefit from our talented team's combination of quality certifications. Such as Certified Systems security Professional (CISSP), Certified Information Security Manger (CISM) and other top level technology certifications. Other benefits of working with us on this project include:

- **Competitive Pricing.** For our full services, the cost is estimated at between $1.3-1.5 million. Prices will shift accordingly based on preference for services.
- **Manageable Timelines.** For our full services, the timeline is estimated at between 9-10weeks (about 2 months). The timeline will shift accordingly based on preference for service.
- **Proven results.** Here is a list of our recent clients who were satisfied with our results. We can provide references (points of contact) if you would like to get their feedback on our company.

Compression Service Inc, - Vulnerability and Risk assessment
TGI Industries – Penetration Testing / Disaster Recovery
Amtrak – Business Continuity/ Disaster recovery/ Risk assessment/ Pen Testing

The combination of our qualified team and their certifications, accompanied by years of proven results, means each of our clients will experience top-level technology security services at a competitive price, in a timely manner. Should you have any questions regarding this proposal, please contact our COO – Nicolas Rasa at (281) 353-4555 or NRasa@DynamicDef.com.

Sincerely,
Jesse Cabrera
CEO, Dynamic Defense LLC

Cost Proposal

Item	Number of Specialists Required	Specialist Hourly Rate	Timeline	Total Labor Cost	Tool Costs, Administrative Costs, and Others	Total Cost
Penetration Testing	6	$225	2 Weeks	$108,000	$102,000	$210,000
Triple-Point Security Assessment	6	$315	2 Weeks	$151,200	$148,800	$300,000
Privacy Gap Assessment	4	$275	1 Week	$44,000	$66,000	$110,000
Compliance Auditing	6	$400	3 Weeks	$288,000	$12,000	$300,000
Rectification of Vulnerabilities	6	$130	3 Weeks	$93,600	$241,400	$335,000
BCP, BIA, DR Planning	4	$195	2 Weeks	$62,400	$12,600	$75,000
Employee Training Course (9 Week License)	N/A	N/A	N/A	N/A	N/A	$135,000

Total Projected Cost: $1,465,000

Projected Timeline

Week	1	2	3	4	5	6	7	8	9
Penetration Testing									
Triple-Point Security Assessment									
Privacy Gap Assessment									
Compliance Auditing									
Rectification of Vulnerabilities									
BCP, BIA, DR Planning									
Employee Training Course (9 Week License)									

Projected Timeline: 9 Weeks

Table of Contents

Cost Proposal ***.....1***

Projected Timeline *2*

Our Dynamic Project Team **6**

Dynamic Defense LLC 6
Jesse Cabrera - CEO 7
Jacob Thompson - CIO 7
Henry Jensen - CISO 7
Izdarely Martinez - CFO 7
Nicholas Rasa – COO 7
Gerardo Cruz – Project Manager 7

Technical Proposal & Evaluation Guide *9*

Section A – Mandatory Requirements *9*

A.2 ..... **9**

A.3 ..... **13**

A.4 ..... **13**

A.5 ..... **13**

Section B – Qualifications & Experience *13*

B.1 ..... **13**

B.2 ..... **14**

B.3 ..... **14**

B.4 ..... **14**

B.5 ..... **14**

B.6 ..... **14**

B.7 ..... **14**

B.8 ..... **14**

B.9 ..... **14**

B.10 ..... **15**

B.12 ..... **15**

B.14 ..... **15**

B.15 ..... **18**

Section C – Technical Approach *18*

C.1 ..... **18**

C.2 ..... **18**

C.3 ..... **19**

C.4 ..... **19**

C.5 ..... **19**

C.6 ..... **19**

C.7 ..... **19**

C.8 ..... **19**

C.9 20
C.10 20
C.11 20
Section D – Security Gap Analysis *20*
D.1 20
D.2 20
D.3 21
D.4 21
D.5 21
D.6 21
D.7 21
D.8 21
D.9 22
D.10 22
Section E – Privacy Data *22*
E.1 22
E.2 22
E.3 23
E.4 23
E.5 23
E.6 23
E.7 23
E.8 23
Section F – Security Assessment *24*
F.1 24
F.2 24
F.3 24
F.4 25
F.5 25
F.6 25
F.7 25
Section G – Security Assessment Report *26*
G.1 26
G.2 26
G.3 26

G.4 27
G.5 27
G.6 27
G.7 27
G.8 27
Section H – Mitigating Risks *28*
H.1 28
H.2 28
H.3 28
H.4 29
H.5 29
H.6 29
H.7 29
Section I – BIA, BCP, and DRP *30*
I.1 30
I.2 30
I.3 30
I.4 30
I.5 30
I.6 30
I.7 31
I.8 31
I.9 31
Section J – Layered Security Solution *32*
J.1 32
J.2 32
J.3 32
J.4 32
J.5 32
J.6 32
J.7 33
J.8 33
J.9 33

Our Dynamic Project Team

Dynamic Defense LLC

Founded in 2005 in Houston, TX by a few brilliant bright minds. Dynamic Defense was created with the goal of creating a respectable and reliable security company. Focused on providing the leading defense in the technology industry. Our team has backgrounds

Certifications Our Experts Hold:
Global Information Assurance Certification (GIAC)
Certified Information Systems Security Professional (CISSP)
Certified Information Security Manager (CISM)
GIAC Security Essentials Certification (GSEC)
Project Management Professional (PMP)
Offensive Security Certified Professional (OSCP)

ranging from military, law enforcement and highly skilled Tech Gurus. Our founding team has brought forth a multi-million-dollar security company. Being recognized as Tech Todays magazines “New Super-Star Security Group of 2023”. Who are we? We are your best choice at defense!

Jesse Cabrera - CEO

With a combination of 18 years of military, technology and leadership experience, Jesse stands out as an effective CEO. Holding certifications such as CISSP, EHC and GIAC. Jesse brings dynamic leadership as well as astounding results to his clients. His team is a representation of that leadership. Providing top-of-the-line quality service to their clients. Each with credible certifications and experience. This decorated veteran stands out amongst the competition. (10-point Veteran Preference certified)

Jacob Thompson - CIO

Jacob has 15 years of IT management experience with the last 4 being in a direct CIO role. He currently holds CISSP, CISA, CEH, PMP, and ITIL certifications. Jacob has worked in various industries including energy, healthcare, and education. Starting as an IT auditor, Jacob worked his way up through the ranks and is passionate about securing IT infrastructure. Jacob has also been a part of several company’s IPO and the many challenges that entails.

Henry Jensen - CISO

Henry Jensen has 25 years total experience in information systems, the last 15 of which being in cybersecurity. He holds CISSP, OSCP, GLEG and GSTRT qualifications, and brings a keen eye into the threat defense game, with his background in penetration testing. Henry has experience – both hands on and administrative – in the consumer, energy, and manufacturing sectors.

Izdarely Martinez - CFO

Izdarely Martinez has 20 years of experience as a chief financial officer. As a CFO Izdarely must be aware of different types of cyberattacks to ensure that the company’s financial data is not at risk. She holds various certifications such as CCISP, CEH, CFR, and A+. Izdarely has years of experience tracking cash flow, financial planning, and analyzing the company’s financial strengths and weaknesses.

Nicholas Rasa – COO

Nicholas Rasa has 22 years of cybersecurity experience, with 8 years of leadership experience. He holds Security+, CCISP, PMP, CISM certifications. He also holds the TS/SCI clearance from his work overseas for the U.S. government. Nick has years of experience of working closely with clients to provide high level security solutions.

Gerardo Cruz – Project Manager

Gerardo Cruz has 20 years as a cybersecurity project manager. Organizing, creating, and executing highly effective projects that have helped hundreds of organizations, from a small mom-and-pop store to organizations that hire 20,000+ employees. Gerardo holds different

certifications that make qualified to create plans in any kind of situation. He holds an A+ certification, DevNet, Security +, and CCISP.

“Dynamic Defense LLC Lives up to their name. From professionalism to exceptional results. The service provided by this company. It was nothing short of dynamic!” – James Bond, Compression Services Inc.

Technical Proposal & Evaluation Guide

Section A – Mandatory Requirements

A.2

WELLS FARGO

To: Whom it may concern

Re: Dynamic Defense LLC

We Would advise that Jesse Cabrera in representation of the Dynamic Defense LLC has maintained a business Checking/ Saving/ Credit account with our office since 08/01/2005. All accounts are currently in good standing. We can confirm that all accounts held by Dynamic Defense LLC have been conducted properly up to our satisfaction.

If needed my authorization code number is *#32456839*.

In best regards,

James Mattias

Regional Bank Manager

Experian

11/17/2023

To whom it may concern,

Re: Credit Reference Request on behalf of:

Dynamics Defense LL

111 HQ St

Houston, TX

77302

In reference to Dynamics Defense LLC. We can confirm the FICO score of 802. The credit history for Dynamic defense has been exemplary. With no missed payments of defaults of any payments. The credit age for this account is 18 years, 6 months and 3 days.

Credit Rating: AAA

Thomas Jefferson

Experian Credit Expert

Austin, Tx

EQUIFAX

11/17/2023

To whom it may concern,

Re: Credit Reference Request on behalf of:

Dynamics Defense LL

111 HQ St

Houston, TX

77302

In reference to Dynamics Defense LLC. We have confirmed the FICO score of 802. The credit history, age and record of on time payments on has met all requirements. We can confirm good standings for all accounts.

Credit Rating: AAA

Tommy Jones

Supervisor to Credit Operations

Equifax

ACORD

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 11/17/2023

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

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

PRODUCER	CONTACT NAME: Jesse Cabrera
Max Todwell EXT 576 PROP Unsur, INC Memphis, TN 87566	PHONE (A/C, No, Ext): 281-222-6161 FAX (A/C, No): E-MAIL ADDRESS: JCabrera@DynamicDefense.com

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : WEGOTYOU Insurance	29785
INSURER B :	
INSURER C :	
INSURER D :	
INSURER E :	
INSURER F :	

INSURED: Dynamic Defense LLC, 111 HQ ST Houston, TX 77302

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

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

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X COMMERCIAL GENERAL LIABILITY CLAIMS-MADE X OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: POLICY PRO-JECT LOC OTHER:	x	x	AV2202012345	01/01/2020	01/01/2025	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG	$ 1,000,000 $ 500,000 $ 10,000 $ 5,000 $ 2,000,000 $
	AUTOMOBILE LIABILITY ANY AUTO OWNED AUTOS ONLY HIRED AUTOS ONLY SCHEDULED AUTOS NON-OWNED AUTOS ONLY						COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	$ $ $ $
	UMBRELLA LIAB OCCUR EXCESS LIAB CLAIMS-MADE DED RETENTION $						EACH OCCURRENCE AGGREGATE	$ $
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N / A					PER STATUTE OTH-ER E.L. EACH ACCIDENT E.L. DISEASE - EA EMPLOYEE E.L. DISEASE - POLICY LIMIT	 $ $ $

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

Technology Security firm who conducts Security assesement.

CERTIFICATE HOLDER

Jesse E Cabrera.

CANCELLATION

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

AUTHORIZED REPRESENTATIVE: MAX TODWELL

ACORD 25 (2016/03) The ACORD name and logo are registered marks of ACORD

A.3

This statement affirms that Dynamic Defense and its staff have no conflicts of interest according to this RFP. No employees are employed by any department of the State Government.

A.4

This statement affirms that Dynamic Defense and its staff do not have any active managed-security service provider contract(s) with any State Government Agency at this time.

A.5

As per the RFP, here is a brief list of just a few government Entities/ Corporations that have a minimum of 5,000 employees. That Dynamic Defense has done vulnerability assessment or Penetration testing for:

- Texas Department of Agriculture – 100,000 active employees
- TDI Industries –15,300 active employees
- Amtrak – 6,800 active employees

Section B – Qualifications & Experience

B.1

Dynamic Defense is a Limited Liability company. Our base of operations is located at 111 HQ St. Houston, TX 77302. Our point of contact is Jesse Cabrera and can be reached 281-222-6161.

362

Projects Completed

12

Clients in Your State

B.2

Dynamic Defense has not had any mergers, acquisitions, or sales of the company within the last ten years.

B.3

Dynamic Defense employees and all affiliates have undergone scrutinous background checks. None have any convictions, pleads of guilty, or nolo contendere to any felonies.

B.4

Dynamic Defense has no pending litigation against itself. Nor does it plan on having any soon.

B.5

Dynamic Defense has not had any filings of Bankruptcy, or involuntary or voluntary proceedings in the last ten years. Our financial strategy has kept our financial growth steady.

B.6

Dynamic Defense has not had any pending or in-progress Securities Exchange Commission investigations. There is nothing to limit our performance in a contract under this RFP.

B.7

Dynamic Defense has been in business for over 18 years. Our annual gross sales have passed one million dollars. Our astounding results of delivering our variety of security services. Have got us a multitude of high-level recommendations from prominent organizations/ entities. With a highly qualified team we are ready to meet all requirements and services requested by your RFP.

B.8

Dynamic Defense has been performing vulnerability/ risk assessment, penetration testing and business continuity/ disaster recovery planning for as long as we have been in business. After 18 years of providing top level services. We have only become more efficient.

B.9

Dynamic Defense currently is made up of 32 employees. Including our founding team. We have 3 locations. Our base HQ is stationed in Houston, Tx. Followed by two locations in Florida and North Dakota. Our client base at this time has grown from seven to ten prominent clients. Ranging in size of the organizations.

B.10

Dynamic Defense has a founding team of six incredible members (Jesse Cabrera CEO, Jacob Thompson CIO, Henry Jensen CISO, Izdarely Martinez CFO, Nicholas Rasa COO, Gerardo Cruz Project Manager) Followed by a highly trained Project team. Consisting of 26 individuals, carrying multiple certifications. As well as a big portion being made of military veterans. We strive to give back to those who gave their all. Gerado Cruz leads three team leaders. Who then lead a team of professionals specializing in each one of our areas of service?

B.12

Based on the minimum requirements of the RFP. Dynamic Defense does not plan on using subcontractors or third-party affiliates. That being said, we are not against partnering with professionals. To achieve the goals of our clients.

B.14

Below is a list of three customer references of clients. Where we have completed services like the ones requested in the RFP.
1)Texas Department of Agriculture – Services provided Vulnerability/ Risk assessments and penetration testing. Point of Contact: John Mayer/ 713-36-9679/JM@TDA.GOV
2)TDI Industries- Services provided Vulnerability/ Risk assessments/ penetration testing/ Business continuity/ Disaster Recovery planning. Point of contact: Thomas Edison/ 832-245-9876/ TEdison@TGI.com
3)Amtrak-Services provided Disaster Recovery, Business Continuity planning, Penetration testing. Point of contact: Timothy DeWilliams/ 832-445-678/ TDWilliams@ Amtrak.com

REFERENCE INFORMATION QUESTIONNAIRE
Proposer's Name: Dynamic Defense LLC
Reference (Client Organization) Name: Texas Department of Agriculture
Person Responding to this Request for: John Mayer
Reference Information: 713-336-9679/ JM@TDA.GOV
Printed Name John Mayer
Signature (MUST BE THE SAME AS THE SIGNATURE
ACROSS THE ENVELOPE SEAL)
Person's Title: Head of Contract Development
Date Reference Form Was Completed: 11/15/2023
NOTE: Reference should complete responses to the seven items that appear on the following pages. If completed using a Word document, use as much space as required. If completed manually, record response in space provided.

1. Describe the services provided by the vendor to your organization.

Services provided Vulnerability/ Risk assessments and penetration testing.
2. Please rate your overall satisfaction with the vendor on a scale of 1 to 5, with 1 being “least satisfied” and 5 being “most satisfied.”
5
3. If you answered 3 or less to the previous question, what could the vendor have done to improve the rating?
N/A

4. Please indicate your level of satisfaction with the Proposer’s project management structures, processes, and personnel. Use a scale of 1 to 5; with 1 being “least satisfied,” and 5 being “most satisfied.”
5
5. Rate your level of satisfaction with the vendor’s line-level staff (e.g., business and systems analysts). Use a scale of 1 to 5; with 1 being “least satisfied” and 5 being “most satisfied.”
5
6. As far as you know, has the vendor remained (or did the vendor remain) in compliance with the contract throughout their provision of services to your organization? If not, please explain.
Yes, Vendor remained in compliance.
7. Would you use the services of the vendor again? Indicate on a scale of 1 to 5: with 1 being “absolutely not” and 5 being “absolutely yes.
5

REFERENCE INFORMATION QUESTIONNAIRE
Proposer’s Name: Dynamic Defense LLC
Reference (Client Organization) Name: TDI Industries
Person Responding to this Request for: Thomas Edison
Reference Information: 713-336-9679/ JM@TDA.GOV
Printed Name Thomas Edison
Signature (MUST BE THE SAME AS THE SIGNATURE ACROSS THE ENVELOPE SEAL)
Person’s Title: Gulf Coast Supervisor
Date Reference Form Was Completed: 11/15/2023
NOTE: Reference should complete responses to the seven items that appear on the following pages. If completed using a Word document, use as much space as required. If completed manually, record response in space provided.

1. Describe the services provided by the vendor to your organization.

Services provided Vulnerability/ Risk assessments and penetration testing
2. Please rate your overall satisfaction with the vendor on a scale of 1 to 5, with 1 being “least satisfied” and 5 being “most satisfied.”
5
3. If you answered 3 or less to the previous question, what could the vendor have done to improve the rating?
N/A
4. Please indicate your level of satisfaction with the Proposer’s project management structures, processes, and personnel. Use a scale of 1 to 5; with 1 being “least satisfied,” and 5 being “most satisfied.”
5
5. Rate your level of satisfaction with the vendor’s line-level staff (e.g., business and systems analysts). Use a scale of 1 to 5; with 1 being “least satisfied” and 5 being “most satisfied.”
5
6. As far as you know, has the vendor remained (or did the vendor remain) in compliance with the contract throughout their provision of services to your organization? If not, please explain.
Yes, Vendor remained in compliance.
7. Would you use the services of the vendor again? Indicate on a scale of 1 to 5: with 1 being “absolutely not” and 5 being “absolutely yes.
5

REFERENCE INFORMATION QUESTIONNAIRE
Proposer’s Name: Dynamic Defense LLC
Reference (Client Organization) Name: Amtrak
Person Responding to this Request for: Timothy DeWilliams
Reference Information: 832-445-678/ TDWilliams@ Amtrak.com
Printed Name Timothy DeWilliams
Signature (MUST BE THE SAME AS THE SIGNATURE
ACROSS THE ENVELOPE SEAL)
Person’s Title: Business Acquisition Manager
Date Reference Form Was Completed: 11/15/2023
NOTE: Reference should complete responses to the seven items that appear on the following pages. If completed using a Word document, use as much space as required. If completed manually, record response in space provided.

1. Describe the services provided by the vendor to your organization.

Services provided Vulnerability/ Risk assessments and penetration testing

2. Please rate your overall satisfaction with the vendor on a scale of 1 to 5, with 1 being “least satisfied” and 5 being “most satisfied.”

5

3. If you answered 3 or less to the previous question, what could the vendor have done to improve the rating?

N/A

4. Please indicate your level of satisfaction with the Proposer’s project management structures, processes, and personnel. Use a scale of 1 to 5; with 1 being “least satisfied,” and 5 being “most satisfied.”

5

5. Rate your level of satisfaction with the vendor’s line-level staff (e.g., business and systems analysts). Use a scale of 1 to 5; with 1 being “least satisfied” and 5 being “most satisfied.”

5

6. As far as you know, has the vendor remained (or did the vendor remain) in compliance with the contract throughout their provision of services to your organization? If not, please explain.

Yes, Vendor remained in compliance.

7. Would you use the services of the vendor again? Indicate on a scale of 1 to 5: with 1 being “absolutely not” and 5 being “absolutely yes.

5

B.15

Dynamic Defense is a Limited Liability company. Our base of operations is located at 111 HQ St. Houston, TX 77302. Our point of contact is Jesse Cabrera and can be reached 281-222-6161.

Section C – Technical Approach

C.1

Dynamic Defense has meticulously studied the intricacies of the State’s requirements and project schedule. Our team recognizes the importance of adhering to the outlined schedule to ensure the timely delivery of our services. We have set key milestones in place, and identified potential challenges that may arise.

C.2

Dynamic Defense’s approach to completing the scope of services is built around a strategic alignment of resources, and our knowledge of technology. We have developed a plan that outlines each step we will take to complete the required objectives within the project schedule.

We will provide a roadmap that highlights the key deliverables and milestones that are essential to achieving success.

C.3

We currently have several certified project managers on our team that know exactly what it takes to deliver high level projects within a specific window of time. We put emphasis on open communication, risk mitigation and a flexible approach to adapt to unforeseen challenges that may arise.

C.4

We use cutting edge technology and tools in order to conduct our penetration tests and vulnerabilities assessments. Using industry wide best practices to identify and analyze vulnerabilities in the state's systems. We will provide a detailed breakdown of our findings, and then move forward with a fix for any flaws that may be discovered. The specific methodologies may include phishing, vishing, penetration tests on networks, and simple database attacks.

C.5

We will assess your employees in potential training areas, by using various phishing methods to see how susceptible they may be to these types of attacks. Next, we will attempt to gain access to your network through various forms of attacks. Finally, we will finish off with injection type attacks to test the vulnerability of your databases. Once our testing is done, we will provide a detailed report about our findings and what suggestions we have for your company moving forward.

C.6

We can assess a wide range of systems for vulnerabilities. This includes but is not limited to, operating systems, databases, applications, and networks. We will showcase our ability to comprehensively evaluate and secure the different components that make up the state's infrastructure.

C.7

Reviewing code is a critical aspect of our provided cybersecurity services. We use a combination of automated tools, and manual inspection. We like to prioritize identifying vulnerabilities early in the development lifecycle.

C.8

When delivering our code review services, our approach is to identify vulnerabilities early in the development lifecycle. The code will be subject to automated tools combing through the lines of code, and then manually looked over by 3 different sets of eyes to ensure every possible vulnerability is discovered. Our findings will be categorized based on the severity of the vulnerabilities that are documented with clear recommendations for mitigation. We ensure our reports are accessible, easy to read, and valuable to those involved in the project.

C.9

Our code review currently offers reports for the following languages:
Java, C++, Python, JavaScript, PHP, TypeScript, Bash, YML, JSON

C.10

Due to the sensitive nature of code review reports we cannot provide an actual report we have made. We assure you that our reports are up to the industry standard and follow the template below:

1. Executive Summary
2. Scope of Code review
3. Tools and services used to review code.
4. Findings and Vulnerabilities
5. Severity classification
6. Recommendations
7. Plan to implement improvements.

C.11

Our commitment to security extends to our own personnel. Our rigorous process for background checks includes the following: Criminal background checks, education verification, reference checks, and security clearance.

Section D – Security Gap Analysis

D.1

Our organization will create a personalized plan after thorough analysis of your systems. We will define objectives, gather existing policies and standards set by your organization, identify applicable standards, conduct gap analysis, document findings, prioritize and plan remediation, implement changes, monitor and review, and documentation and reporting.

D.2

Ensuring our IT security policies align with HIPPA requirements, our team does a detailed and focused approach to your organization to protect sensitive healthcare data.

D.3

Ensuring that IT security policies align with the Payment Card Industry Data Security Standard (PCI DSS) involves a comprehensive approach due to the sensitivity of cardholder data. Our organization must first understand the PCI DSS requirements, we will then assess your current policies, involve relevant stakeholders, update or develop new policies, implementation of safeguards, educate the staff, begin monitoring and auditing, conduct regular assessments and updates, concluding by documenting and reporting our findings.

D.4

Safeguarding citizen privacy data in accordance with State Government Privacy Laws requires a meticulous and comprehensive approach. Our organization would begin by understanding State Government Privacy Laws, assessment of current practices, stakeholder involvement and policy definition, establish data classification and access controls, data minimization and retention policies, training and awareness programs, implement technical Measures, monitoring and compliance audits, documentation and reporting, periodic review and updates.

D.5

Establishing administrative controls is a must as management must be able to maintain their state's AUP and be able to communicate with their team what the correct procedures are. First, we need to establish how many people work in the organization or what the rough estimate is as that way we can determine how to better assign and create the controls. Once the controls have been created, we begin to train management on how to effectively use the system and personally shadow them while they learn to implement the system with the rest of their employees.

D.6

In order to monitor the traffic that is coming in through the servers we will be utilizing packet sniffers like Wireshark. Once that has been implemented, we will train the administrative team how to monitor their servers. In order prevent any data leakage or loss of confidential data, employees must partake in training that will establish a zero-tolerance policy of them clicking random links as that can be ways for the system to be compromised.

D.7

The state must notify their key heads of any changes that are going to occur so they can then let their staff know as well, a trickledown effect. This way, the change manager can support the staff through the coming changes and can mitigate any resistance that might occur. A vision must also be created of what we are trying to achieve, what problems are being resolved and how it will improve the organization. Once that is set, the changes will be implemented, managers must be active in this role to make sure it runs smoothly by aiding their employees where it might be needed to keep everyone happy. The changes must now be embedded in and solidified to ensure all workflows are moving forward. Once it is all done, we will review and analyze to see if any changes need to be made.

D.8

The current issues impacting all organizations when it comes to employees or users having remote access is how can we make sure that it is only them that has access to their devices. Of

course, human error always play a big part of data being leaked, whether it be by the user losing their device or leaving it unattended whether at home or in a public place or utilizing public wifi. Our organization recommends implementations multiple 2 step authentication for all applications that an employee uses. As most people tend to have their personal cellphones, they can have a key sent to them each time they try to access an application to confirm it is truly them.

D.9

Our approach when it comes to defining and created a business continuity plan and a disaster recovery plan is to look for a fast and easy way to get your business back up and running, as we know time is money, and the less time your organization spends down the better for everyone. While we make sure that it is fast and easy we also look to making sure that it is price appropriate to what the budget is while maximizing efficiency. Our team would help the state by creating a training seminar or program for the employees so they are aware what the protocol is when the system fails, and what must be done to get the system up and running.

D.10

Most gaps found were due to unauthorized access, data leakage, and human error. The way to address these gaps would be to implement stricter rules when it comes to using remote access and distributing employees with equipment they can take home. There should be duo factor authentication that is mandatory for all employees to access their work from home stations. Other policies will be creating more complex passwords, instead of an 8-letter password, it should be at least 12-letters making it even more complex. Continuous education should be done to keep the employees aware of the dangers of clicking links that appear on unknown emails. The cybersecurity team will conduct random phishing emails to catch any staff that are now adhering to the training. All these policy changes are easy to roll out nationwide and can be expected to have little to no pushback from the employees.

Section E – Privacy Data

E.1

Dynamic Defense is ISO 27018 certified in the Protection of Personally Identifiable Information (PII) and will utilize the latest standards set forth by the Department of Health and Human Services regarding Personal Health Information (PHI) and Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance. Dynamic Defense has a comprehensive checklist for verifying the storage and transmission of PII. This checklist has been audited and verified completely by third party experts.

E.2

Dynamic Defense employs an internal general counsel to ensure all local, state, and federal laws are met. Dynamic Defense always utilizes the standards and guidelines recommended in the NIST Privacy Framework and NIST 800-122.

E.3

Dynamic Defense will read and audit all internal IT policies and recommend changes said policies as needed. We also offer services to write new IT policies for any gaps identified in the privacy data assessment.

E.4

Dynamic Defense matches our proven record of controls with existing controls at the organization to verify they are not only documented but are implemented properly. Controls without proper use are no good to the organization.

E.5

Dynamic Defense will conduct a full privacy data assessment included in this proposal. This assessment will look at all existing policies, procedures, controls, and random checks throughout the organization's network. The privacy data assessment allows our team to identify gaps related to PII and PHI.

E.6

Once the privacy data assessment is complete, Dynamic Defense will provide a list of recommendations for closing these gaps. Our detailed reports provide your team with severity level along with estimated costs and timelines. This report includes a comprehensive plan for completion, saving you time and money rather than relying on a third party to complete these steps.

E.7

Dynamic Defense will write and update policies in compliance with the NIST Privacy Framework and NIST publication 800-122. Our policies will also be reviewed by our internal legal team. We also provide a service to allow a third-party vendor of your choice to audit these as well. As an added touch they will be custom branded to your organization's standards.

E.8

Dynamic Defense is committed to remaining up to date with the latest state and federal laws and regulations related to private data. For example, our team has had training for the recent passage and upcoming implementation of the Texas Data Privacy and Security Act (TDPSA). We are happy to report our systems and processes were already approved by the state to be following the TDPSA. Included in your contract, Dynamic Defense will also provide updates for no more than one calendar year from assessment completion in the event new privacy related laws or regulations are passed on the local, state, or federal level.

Section F – Security Assessment

F.1

Dynamic Defense utilizes the latest penetration tools and techniques. We will perform tests on hardware, software, network, and physical layers within your IT infrastructure. Our test is guaranteed to cover all seven of the common domains of modern IT infrastructures. Dynamic Defense is also updated daily on the latest emerging threats and will include tests for those found during your security assessment phase.

F.2

Dynamic Defense has reviewed the existing policies detailed in the original RFP and finds them to be following industry standards. Therefore, this security assessment will only recommend controls and policies for those gaps listed in the RFP.

F.3

Dynamic Defense utilizes multiple industry standard sources for the collection and organization of known threats to organizations. We will sort this list based on the findings in the security assessment and will only keep the relevant information. A full list will be available upon request. Our report presented will use a 1-5 scale system with 1 being low severity and 5 being critical issues.

F.4

Dynamic Defense utilizes the latest penetration testing tools and techniques to identify holes within IT infrastructure. We are able to scan all network devices, servers, endpoints, printer, and any other device connected to your network. Our tools will scan those devices for known vulnerabilities and attempt to compromise these devices. While the full scan is intrusive and is recommended to be performed after hours, we also run smaller scans during normal business hours in an attempt to gain a full picture of the vulnerability scope. These scans will not cause any noticeable impact to your users, systems, or any related business operations.

F.5

Dynamic Defense compiles all data into two separate reports. One is a detailed list of all found vulnerabilities. We will sort this list based on the findings in the security assessment and will only keep the relevant information. A full list will be available upon request. Our report presented will use a 1-5 scale system with 1 being low severity and 5 being critical issues.

The second is a high-level overview of the risks for presentation to senior leadership.

F.6

As stated earlier, our lists are ranked on a 1 to 5 scale. These rankings are prioritized by their ability to cause the loss of private data and system downtime. The rest of the algorithm is an internal calculation we have worked to build and protect but will gladly discuss with your teams in person should any questions arise.

F.7

Our formal reporting will include all the above in various formats. These formats can be used in whichever capacity is appropriate for the potential reader. We understand that not everyone wants to read the sheer amount of data that can be generated in a full security assessment. Any potential problems that are discovered and reported will have digital links on how to resolve these issues through your own IT teams. We also include links to MITRE and NIST for further information regarding known and discovered threats.

Section G – Security Assessment Report

G.1

Each identified risk will be categorized into one of seven IT Infrastructure domains, and then given a numerical ranking, 1-5, based on severity. The measure of severity will be subjective and based on the combined experience of firm members, while taking into consideration the likelihood of exploitation, potential impact, data sensitivity, ease of detection, mitigation difficulty, dependencies on other risks, regulatory compliance impact, and other factors that may present themselves.

G.2

Our qualitative risk assessment methodology aims to provide a nuanced look at the state of IT infrastructure security, and to clarify any risks identified in the IT infrastructure. Our approach includes, for each identified risk: an impact assessment, a likelihood of exploitation assessment, a categorization based on type of risk (to identify possible risk trends), stakeholder input regarding rectification, and all with an emphasis on clear documentation.

G.3

Identifying the highest priority resources is centered to our approach to Dynamic Defense. To determine which resources are of highest priority to include in a qualitative risk assessment, we perform an inventory of all assets prone to attack. Then, assets are prioritized based on their criticality, dependencies, and other key factors. This systematic evaluation ensures a focused and effective risk assessment process.

G.4

We start by conducting domain-specific risk identification scans. As mentioned in F.4, Dynamic Defense employs multipoint inspection tools that are able to scan all devices on the network at once and attempt to compromise them using known techniques. By using these tools, we can look at risks in the context of their greater IT infrastructure domain. Each identified risk's impact will be weighed using the combined experience of firm members, taking into consideration the likelihood of exploitation, potential impact, data sensitivity, ease of detection, mitigation difficulty, dependencies on other risks, regulatory compliance impact, and other factors that may present themselves.

G.5

Our prioritization method ranks risk both in the context of each IT infrastructure domain, and across the entire IT infrastructure. Severity assessments within a domain are ranked numerically, 1-5, based on the previously mentioned criterion. On the holistic scale, risks are measured similarly, on a 1-5 scale. However, there is nuance in the holistic scoring. Risks in certain domains may pose a greater threat to the organization merely by virtue of which domain they lie. Dynamic Defense's proprietary internal scoring metrics weigh these concerns on the holistic scale to provide a clearer view of which threats are more severe.

G.6

Once risks are sorted based on severity and impact, we carefully assess response options. In our assessment of which remedial activities will have the most impact and greatest return on investment, we coordinate with shareholders and IT Administrators. We take a tailored approach when responding to each problem, ensuring that remedial activities are effective and meet the needs of the organization, all while ensuring cost-effectiveness.

G.7

Dynamic Defense's attitude when providing risk assessment reports is "Information overload." We focus on comprehensive documentation, ensuring that every single detail and nuance of every single identified risk is thoroughly documented. Furthermore, Dynamic Defense's approach emphasizes clarity and transparency in reporting.

G.8

Upon identification and categorization of risks, Dynamic Defense will provide a risk assessment report that outlines any potential security vulnerabilities found in the qualitative risk assessment. The report will have two parts – a section with a holistic view of risk across all IT infrastructure domains, and a section with domain-specific risks. Both sections will be organized similarly; risks will be sorted based on severity, with the most severe at the top of the report. Each risk entry will have a risk score, 1-5, how the risk was discovered, which systems are affected by the specific risk in question, potential interdependencies, other specific considerations that lead to that risk having that score, and suggested mitigation techniques. Furthermore, each risk entry will contain a subjective, qualitative return-on-investment calculation. Each risk will be listed twice in the report – once in the IT domain specific to it, and once in the holistic risk section.

Section H – Mitigating Risks

H.1

Dynamic Defense's approach to utilizing the qualitative risk assessment report involves a systematic process to ensure that all risks have been identified. We use risk prioritization to show the impact each risk may have on the company. This involves categorizing risks into high, medium and low priority when considering factors such as likelihood, impact and vulnerabilities identified. For each prioritized risk we develop a tailored mitigation strategy. We will describe how we allocate resources effectively to address the most critical risks first. We will continuously monitor the mitigation efforts over 6 months after the project is finished to ensure the effectiveness of mitigation efforts.

H.2

Our prioritized risk response report builds on the information and recommendations from the qualitative risk assessment. The first step is to consolidate the information including identified risks, vulnerabilities and recommended mitigations. Based on the synthesized data we will create a ranked list of risks. Next, we will detail the actions, controls and measures that are recommended to combat the identified risks.

H.3

Dynamic Defense uses the following list when determining which risks warrant a response:
Business Impact- making sure the business' essential operations can withstand outages.
Regulatory compliance- risks that may lead to non-compliance or legal requirements.
Reputation risk (PR risks)- recognizing the long-term impacts of negative PR, like data leaks.
Critical asset protection- making sure that critical assets receive priority.

H.4

When identifying the best response for each risk, Dynamic Defense takes the following into consideration. Risk assessment, we reassess the risk and consider the effectiveness. Cost-Benefit analysis, to ensure the response is economically viable and aligns with the state's budgetary constraints. We use a continuous improvement approach to refine our strategies by learning from our past responses.

H.5

Dynamic Defense uses a holistic evaluation to determine the most overall security protection across all domains in the IT infrastructure. We assess risks that in one domain may have a cascading effect on others. Integrated security solutions address multiple vulnerabilities and risks across all domains simultaneously. We emphasize implementing controls that offer broad protection, which enhances the overall security of the entire IT infrastructure.

H.6

Our outline for how we approach implementation of selected risk responses. We start with sequencing each risk response based on prioritization and dependencies. We then consider the potential cross-domain impact of each risk response, to ensure that a change in one domain does not create vulnerabilities in another. Then we test each risk response to ensure its effectiveness, prior to deployment. Finally, we document each risk response to provide clear guidelines for implementation, monitoring and management of the risk response.

H.7

Our formal risk response report is a detailed document that includes the following information. In our report, we provide a clear explanation of each selected response, with expected outcomes and how it aligns with the state's objectives. We will describe how the report covers responses to security risks across the seven domains of IT infrastructure. We include metrics and performance indicators to measure the effectiveness of implemented responses. Our formal risk response report is documentation of actions taken as well as a guide for future security enhancements.

Section I – BIA, BCP, and DRP

I.1

Dynamic Defense will ensure operational continuity during and after any disruptive events by identifying the effects of a disruptive event on the functions of the business to provide strategies to mitigate the risk to the business.

I.2

Dynamic Defense will identify business critical applications and functions for the organization by gathering a good team that will access the correct information. Establishing the value of the BIA to the management team to schedule and prepare BIA interviews to share and analyze data. To prepare a report for the company and discuss where we need to help the organization.

I.3

Dynamic Defense will conduct a formal business Impact analysis to identify business-critical applications and functions by helping the organization determine the potential risk and effects in case of any negative events and have a formal plan to be able prevent the attack by looking into the financial, reputation, regulatory, social, production output, and Environmental.

I.4

Dynamic Defense will use the BIA to identify the resources necessary to ensure operational continuity by making a contact list to help the organization prioritize their resources to ensure that the critical operations are working during disruptive events. Equipment for data backup and restoration channels installed to help the organization.

I.5

Dynamic Defense will utilize the BIA and identified critical resources list to develop a BCP to determine the strategies to reduce risk, develop a response and recovery options. Lastly, train and educate others on the plan to be able to implement, test, and revise the plan.

I.6

Dynamic Defense will utilize the output of the BIA and BCP to prepare a cost and resources estimate of the requirements to create the BCP and DRP. The estimate will include a cost

proposal for identifying the task, deliverables, and man-hours required to perform the identified task.

I.7

Dynamic Defense will utilize the BIA, BCP, and identified critical resource list to develop a disaster recovery plan by conducting a risk analysis and being able to assess the vulnerabilities to identify the critical business processes and set recovery objectives to establish activation protocol.

I.8

The way Dynamic Defense will approach the determining cost and resources necessary to carry out the DRP is the 3 main components. First Standardized communication is one of the most critical of a disaster recovery plan. The second objective is to prepare staff to monitor metrics as soon as possible. The last component will be a backup plan in case data is breached.

I.9

The approach Dynamic Defense will take is by testing the BCP and DRP to ensure that it is effective and appropriate to protect operational continuity in case of various interruptions. Auditing objectives and scope the first component of the BCP and DRP. Which are audit methodology and tools and audit the findings and recommendations. Report any action plan to follow up and review with the team to be able to audit cycle and frequency for BCP and DRP.

Section J – Layered Security Solution

J.1

Dynamic Defense will implement a layered security solution to provide protection for critical resources and data. This process requires 3 elements of layered security and is also known as defense in depth. These 3 elements include perimeter defense, proactive monitoring, and security training. Which will ensure each defensive component protects a specific area that can be exploited or hacked.

J.2

Dynamic Defense will identify the most sensitive resources and data that require specific protection from attack or failure is to convert sensitive information into a coded form. Making it unreadable for anyone to understand without a decryption key that only Dynamic Defense will provide to workers who are authorized and able to decode the data to be readable.

J.3

Dynamic Defense will describe the approach for ensuring multiple controls to protect each identified resource or data collection to satisfy mandated security requirements will include encryption backup, disaster recovery plan, access control, networking security, and physical security will help ensure that security is at its top performance when it comes to sensitive information.

J.4

Dynamic Defense will determine the most likely attack paths for each
sensitive resource or data collection will be to set up a system that will detect when an attacker enters the network. The attack path enables movement between assets and sees what the attacker is trying to do. When we get a hold of the attacker, we will do everything to keep the system safe.

J.5

Dynamic Defense will determine where to place controls across the seven domains of the typical IT infrastructure to provide multiple layers of security protection: Human, Perimeter, Network, endpoint, application. Data. Mission Critical Assets, and the idea is that if hackers want to access our data, they have to break through multiple layers first making it much more difficult.

J.6

Dynamic Defense will ensure that each sensitive resource or data collection is protected by multiple controls so that any control failure or compromise does not expose the protected resources or data collection using passwords, multi- factor authentication, and role-based action control. We will ensure

that these will work only with those with proper authorization who can access sensitive data. Reducing the risk of data breaches and unauthorized access.

J.7

The state can evaluate the effectiveness of each control in layered security by evaluating the layered security based on how closely the performance of the layered security controls aligns with the organization security plan and the organization's ability to manage risk.

J.8

The approach we use to document each layer security control is by taking into consideration the cost implementation for each layer, using multi-factor authentication, locked doors in any area with computer equipment, and encrypting data servers.

J.9

Dynamic Defense will assess the layered security solution to ensure it maintains its design ROI and provides the desired level of protection by considering the total cost of implementing, possibility risk reduction, and the impact on the operations efficiency.