TECHNICAL RESPONSE

RFI – Cyber-Security Assessment, Remediation, and Identity Protection Monitoring, and Restoration Service
Department of Management Services

Submitted to:
Department of Management Services
Attention to: Joel Atkinson, Associate Category Manager
joel.atkinson@dms.myflorida.com

Submitted by:

PATHUSA
Premier IT Services

Specialists in Applications Development and Networking Services"

ePATHUSA, Inc.
6600 Westown Parkway, Suite 245
West Des Moines, IA 50266
William Keleture
wkeleture@epathusa.net
www.ePATHUSA.net
515-309-2073 (Phone)
630-884-3700 (Fax)

Small Disadvantaged Business (SDB)
DUNS No: 011683428
Tax Payer Identification Number: 86-1138597

NAICS Code:, 541511, 541512, 541513, 541519, 541611, 541612, 541614, 541618, 561311, 561320

Minority-Women Owned Business Enterprise (MWBE Certified)

GSA Contract Holder	Contract No. GS-35F-152BA SIN 132-51 - Information Technology (IT) Professional Services Period of Performance: 14 Jan 2014 to 14 Jan 2019

TECHNICAL RESPONSE

Cyber-Security Assessment

IV. RESPONSE:

As part of the Cyber Security Assessment, ePATHUSA is and can provide pre-incident services to the following;

1- Pre-Incident Services:

a) Incident Response Agreements – Terms and conditions in place ahead of time to allow for quicker response in the event of a cyber-security incident. Yes

b) Assessments – Evaluate a State Agency's current state of information security and cyber-security incident response capability. Yes

c) Preparation – Provide guidance on requirements and best practices. Yes

d) Developing Cyber-Security Incident Response Plans – Develop or assist in development of written State Agency plans for incident response in the event of a cyber-security incident. Yes

e) Training – Provide training for State Agency staff from basic user awareness to technical education. Yes

TECHNICAL RESPONSE

RFI – Cyber-Security Assessment, Remediation, and Identity Protection Monitoring, and Restoration Service
Department of Management Services

Submitted to:
Department of Management Services
Attention to: Joel Atkinson, Associate Category Manager
joel.atkinson@dms.myflorida.com

Submitted by:

PATHUSA
Premier IT Services

Specialists in Applications Development and Networking Services"

ePATHUSA, Inc.
6600 Westown Parkway, Suite 245
West Des Moines, IA 50266
William Keleture
wkeleture@epathusa.net
www.ePATHUSA.net
515-309-2073 (Phone)
630-884-3700 (Fax)
Small Disadvantaged Business (SDB)
DUNS No: 011683428
Tax Payer Identification Number: 86-1138597

NAICS Code:, 541511, 541512, 541513, 541519, 541611, 541612, 541614, 541618, 561311, 561320

Minority-Women Owned Business Enterprise (MWBE Certified)

GSA Contract Holder	Contract No. GS-35F-152BA SIN 132-51 - Information Technology (IT) Professional Services Period of Performance: 14 Jan 2014 to 14 Jan 2019

TECHNICAL RESPONSE

Cyber-Security Assessment

TABLE of CONTENTS

PART 1 – PURPOSE 1

PROJECT APPROACH 1
PROJECT SCOPE 6
RESPONSIBILITIES 6
VALUE PROPOSITION 6
ANTICIPATED DIFFICULTIES AND RESPONSES 7
DELIVERABLES 7

PART 2 – TECHNICAL CAPABILITIES 7

September 3, 2015

Joel Atkinson

RFI – Cyber Security Assessment

Dear Joel:

Many businesses and organizations suffer security paralysis, a condition in which it is impossible to prioritize areas for remediation due to limited resources. Others attempt to apply a set of best practices in the hope that what worked for another organization or business will work for them. Unfortunately, neither of these approaches is a rational strategy for protecting information assets or maximizing the value returned from investments in security.

The best approach would be for an organization to pursue an internal cyber security assessment. ePATHUSA will use a five step assessment plan to help Department of Management Services lay out the foundation for a meaningful security strategy that include;

1. Identify information assets. ePATHUSA will look at the information that the DMS handles for example, social security numbers, payment cards, patient records, human resources data.
2. Locate information assets. ePATHUSA will identify and list where each item on the information asset lists reside with the organization for example, file server, workstations, laptops, removable media, PDAs, and phone, databases.
3. Classify information assets. Assign a rating to information asset list, consider scaling it from 1 – 5.
4. Conduct a threat modeling exercises. Rate the threats that top rated information assets face.
5. Finalize data and plan. This will include threats to organization assets at stake as well as a broad spectrum of possible contingencies for the organization.

After completing a review of current security controls and along with a review and rating of potential threats/vulnerabilities, a series of actions should be determined to reduce risk (threats exploiting vulnerabilities) to and acceptable level. These actions should include putting into place missing security controls, and/or increasing the strength of existing controls.

Security controls should ideally reduce and/or eliminate vulnerabilities and meet the needs of the business. Cost must be balanced against expected security benefit and risk reduction. Typically, security remediation efforts and actions will be focused on addressing identified high risk threat/vulnerabilities

ePATHUSA team stands dedicated to helping the Department of Management Services fulfill the Cyber Security Assessment objectives including:

- Develop a foundation of Security Policies, Practices and Procedures, especially in the area of Change Control
- Establish and enforce a globally-accepted password policy
- Address vulnerability results in order of high risk to low risk
- Establish an Operations group facilitated discussion to improve processes and communications, and to eliminate any misunderstandings
- Establish router configuration security standards, forming baseline practices

- Harden servers on the internal network
- Redesign the internet perimeter, incorporating concepts of N-tier architecture and “defense in depth” into the redesign of the Internet perimeter and Enterprise Architecture
- Complete Computer Security Incident Response Team (CSIRT) capability

We are committed to providing the services detailed in this proposal for the fees described and with the personnel listed in our response.

We look forward to working closely with you on this initiative.

Thank you for your consideration

Hari Nallure

hnallure@epathusa.net

Phone: 515-991-1461

Part 1 – Purpose

The purpose of this RFI is to respond to Department of Management Services regarding a qualified contractor to provide Cyber-Security Assessment, Remediation, and Identity Protection Monitoring, and Restoration Service engineering and support services for a wide variety of networks, servers, and applications.

Project Approach

Project Background

This statement sets forth the scope of services, deliverables, roles and responsibilities, anticipated schedule, cost and other information associated with the services that vendor will provide to Department of Management Services in accordance with the established terms and conditions of the contract.

Approach

1- Assessment

2- Why do assessment?

3- Risk Management Framework

4- Assessment methodology phases

5- Technical assessment technique

Assessment:

-Determine how effectively an entity being assessed meets specific security objectives

-Gain understanding and achieve clarification, or obtain evidence

-Three types of assessment methods

a- Testing: exercise one or more assessment objects to compare actual and expected behaviors

b- Examination: check, inspect, review, observe, study, or analyze assessment objects

c- Interviewing: conduct discussions

Why do assessment?

- Help confirm that systems are properly secured
- Identify any organization security requirements that are not met, and other security weaknesses that should be addressed
- Meet requirements to periodically assess systems

Risk Management Framework:

Security Life Cycle

CATEGORIZE Information System

1- Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

SELECT Security Controls

2- Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

IMPLEMENT Security Controls

3- Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings

ASSESS Security Controls

4- Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, and meeting security requirements for information system).

AUTHORIZE Information System

5- Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation

MONITOR Security Controls

6- Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Assessment methodology phases:

1- Planning:

- Gather information needed for assessment execution and develop the assessment approach

2- Execution:

- Identify vulnerabilities and validate them when appropriate

3- Post-Execution:

- Analyze identified vulnerabilities to determine root causes, establish mitigation recommendations, and develop a final report

4- Several accepted methodologies for conducting different types of security assessments

Technical assessment techniques

Review Techniques

a- Examination techniques, generally conducted manually

b- Evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities

c- Techniques include

d- Documentation review

e- Log review

f- Rules set and system configuration review

g- Network sniffing

h- File integrity checking

i- Target Identification and Analysis Techniques

a. Testing techniques, generally performed using automated tools

b. Identify systems, ports, services, and potential vulnerabilities

c. Techniques include

i. Network discovery

ii. Network port and service identification

iii. Vulnerability scanning

iv. Wireless scanning

v. Application security examination

d- Target Vulnerability Validation Techniques

i. Testing techniques that corroborate the existence of vulnerabilities

ii. May be performed manually or with automated tools

ii. Techniques include

1. Password cracking

2. Penetration testing

3. Social engineering

4. Application security testing

Combinations of techniques

1- No one technique can provide a complete picture of the security of a system or network

2- Organizations should combine appropriate techniques

a- One technique often relies on others

b- Multiple ways exist to meet an assessment requirement, such as determining whether patches have been applied properly

c- Organizations have the flexibility to choose the techniques that best meet their requirements

Baseline Security Best Practices Assessment:

What	Review entity's security policies, procedures and documentation to determine security posture with respect to ISO 17799. This assessment is based solely on review session(s) and documentation review. No testing or technical reviews are performed.
How	1. Complete baseline assessment checklist with agency contacts. 2. Review requested information. 3. Identify gaps and weaknesses. 4. Issue general findings report.
Who	1. Complete baseline assessment checklist with agency contacts. 2. Review requested information. 3. Identify gaps and weaknesses. 4. Issue general findings report.
Requested Information	1. Organizational roles and responsibilities; 2. Risk management plans. 3. Policies, procedures, standards, and guidelines relevant to ISO 17799; 4. General network and system documentation; 5. Continuity plans; 6. Prior security assessment findings; 7. Asset classification scheme 8. High level asset list and asset classification
Time	Four hours to facilitate the completion of the general assessment checklist and eight hours to document results.
1. Security Policy & Organization Review	
What	Review entity's security policies, procedures and organizational structure and assess against Commonwealth requirements and industry best practices.
How	1. Develop request for information checklist. 2. Review requested policies and procedures from entity contact. 3. Conduct sessions to review entity's policies and procedures. 4. Compare gathered policies and procedures to Commonwealth policies and industry best practices 5. Identify policy and procedure gaps and weaknesses. 6. Issue technical report
Who	1. Assessment team. 2. Chief Security Officer / IT Security Manager - personnel with knowledge of entities policies and procedures.

Requested Information	1. Policies and procedures for security and information technology processes. 2. Guidelines and standards. 3. Organizational charts and roles and responsibilities documentation - IT and business including segments, departments, teams, boards of directors. 4. IT governance structure. 5. Segregation of duties strategy.
Time	Two hours for interviews, eight hours to review documentation and eight hours to document results.
2. Physical and Environmental Security Assessment	
What	Review entities physical and environmental security controls.
How	1. Develop request for information checklist. 2. Review requested documentation from entity contact. 3. Conduct walkthrough with person(s) responsible for managing physical and environmental security. 4. Review documentation with key contacts. 5. Conduct interview utilizing physical and environmental security assessment checklist. 6. Identify gaps and weaknesses. 7. Issue technical report.
Who	1. Assessment team. 2. Facilities management / physical security - personnel with knowledge of the physical security of information processing location and related policies and procedures.
Requested Information	1. Facility plans and schematics. 2. Listing of physical data center access and environmental controls. 3. Physical and environmental related policies and procedures including access, guest access, new resource provisioning, termination procedures, access in the event of a disaster, etc. 4. Emergency evacuation procedures.
Time	One hour for walkthrough, two hours to review assessment checklist and four hours to document results.

3. Incident Response Plan Review	
What	Review overall incident response plan for relevance, completeness, compliance with policy and applicable statutes, regulations and standards.
How	1. Develop request for information checklist. 2. Review requested information from entity contact. 3. Conduct session to review role definitions and alternates, incident categorization and SLA's escalation. 4. Conduct session(s) to review intervention process and roles. 5. Conduct session to review incident response tracking and evidence

	retention. 6. Issue technical report.
Who	1. Assessment team. 2. Incident response manager 3. Compliance officer and/or representative of legal team 4. Other managers (IT, HR…) depending on role definitions.
Requested Information	1. Incident Response Plan and related procedures. 2. Organization chart.
Time	Four hours to review documentation, eight hours to conduct review sessions and eight hours to document results.

Project Scope

In-Scope Process

In-scope consists of support tasks and duties needed to successfully fulfill Department of Management Services support related assessment responsibilities of planning, operations, maintenances, cost reduction methodologies, and other IT ad hoc request.

Responsibilities

ePATHUSA will provide resources with experience in the technology and industry involved with the project. The Department of Management Services is ultimately the expert in its business. The activities under this SOW involve a collaborative effort by the parties. ePATHUSA will rely upon the DMS in the activities listed in this SOW. The results and benefits of such efforts will be based, in part upon the information materials and guidance provided by Department of Management Services.

The Department of Management Services is responsible for the accuracy and completeness of information, data and materials provided for the development, support as well as any incremental release or instances which may be developed during the period of performance. ePATHUSA shall have no obligation to independently verify the accuracy or completeness of the information, data or materials provided by DMS.

ePATHUSA is entitled to rely upon decisions and all deliverables and documents approved and accepted by Department of Management Services.

Value Proposition

ePATHUSA team that will be presented will have an extensive experiences and proven track record in cyber security assessment, support, as well as forwarding suggestions for improvements in a timely manner.

ePATHUSA value proposition is rooted and committed to our core values that will be needed to achieve best delivery to Department of Management Services.

Anticipated Difficulties and Responses

Based on our many years of personnel and subcontractor experience in planning, designing, developing, and implementing Cyber Security assessments, we anticipate difficulties due changing Cyber Security as well as rapid change and obsolescence in technology. To keep up and understand the details of new cyber security and develop technology choices guided by business goals can mitigate many of the risks produced by the rapid changes in Cyber Security.

Responses:

By setting up planning, development, and test environments, the exchange of information is allowed to flow more easily. The less confusion there is during Cyber Security assessment, the better suited the Department of Management Services will be to move forward in developing the new Cyber security infrastructure.

Deliverables

ePATHUSA's delivery approach to this effort will be based on our many years of experience in planning, developing and supporting Cyber Security infrastructure for **Metropolitan Atlanta Rapid Transit Authority (MARTA), Genova Technologies, and Net Integrated Consulting (NIC).** We possess the processes and the infrastructure to effectively institute best practices. Our team member can not only perform Cyber security assessment requirements, but also the need to capture innovation and efficiencies to reduce Cyber Security infrastructure contract support cost.

Part 2 – Technical Capabilities

ePATHUSA will present a team member with a broad spectrum of experience and direct relevance in all aspects of the SOW, and has a solid reputation for performance and cooperation with State, Federal and industry partners. The team member will provide the planning, development and cyber security assessment for this project.