REQUEST FOR PROPOSAL

INFORMATION SECURITY PROGRAM PROVIDER

OCTOBER 18, 2013

Table of Contents

I. EXECUTIVE OVERVIEW

First Coast Technical College is in the process of identifying firms who offer services to assist us in establishing an information security program to secure student and proprietary data. The intent of the Request for Proposal (RFP) is to identify an Information Security Program provider that can satisfy the requirements defined in the RFP. The selection process also includes but is not limited to a review and evaluation of the responses and reference checks.

Selection of a vendor will be based on:

- Compliance with all the requirements of this RFP
- Vendor capabilities
- Client references
- Total cost of services

To facilitate the selection process and help FCTC better understand your company and its services, it is requested that you provide all the information requested in this document.

For you information, an overview of key project milestone dates is as follows:

Milestone	Completion Date
RFP Release	October 11, 2013
Questions on the RFP due	October 18, 2013
Resposnes to questions from vendors	October 23, 2013
RFP Responses Dues	November 12, 2013
RFP Analysis and Vendor Selection	November 13, 2013
FCTC Board Approval of Contract	November 19, 2013

II. BACKGROUND

A. Goals & Objective of Request

The primary goals and objective of the development of an Information Security Program are to:

1. Establish and manage an information security program
2. Identify and confirm FCTC's vulnerabilities to information systems from internal and external threats by actually attempting to penetrate defenses
3. Identify and confirm FCTC' vulnerabilities to information systems from internal and external threats by actually auditing the current architecture and system configuration
4. Minimize or eliminate business risks and exposures by identifying short and long term options and solutions for remediation of identified vulnerabilities
5. Determine the appropriate approach to develop or improve an existing information security program
6. Recognize solutions to risks, vulnerabilities, and/or threats

B. Project Scope

Scope Parameter	Description
Penetration Testing	**Internet-Facing Hosts** Unlimited IP addresses tested **Internal Hosts** Unlimited IP addresses tested
Information Security Program Creation and Management (Virtual CISO)	**Creation of Information Security Program** Establish Policies & Procedures to govern the security of the network and data **Information Security Program Management** Implement security bases upon created Policies & Procedures to reduce, transfer and mitigate risk

C. Project Deliverables

Deliverable	Description and Purpose
Penetration Analysis Report	Report highlights and documents key engagement findings, conclusions, and recommendations regarding the vulnerabilities found during testing Details the exposures associated with your infrastructure from an internal and external perspective
Final Presentation	A presentation for management at the conclusion of the project to review the following: Penetration analysis results Overview of the current environment security posture Recommended action plan
Security Policies & Procedures	Policies & Procedures relevant to FCTC's environment to reduce, transfer and mitigate risk to the network and student data
Corporate Security Assessment Report	Report highlights and documents key engagement findings, conclusions, and recommendations regarding the vulnerabilities found in all systems during testing Details the exposures associated with your infrastructure and systems

D. Project Assumptions

Assumptions
FCTC will identify a senior Executive Sponsor to support the engagement. The Executive Sponsor will serve as the point of coordination to engage FCTC's executive core team members at key points during the project.
FCTC will identify a Project Coordinator to provide operational assistance to the consulting team, to identify project participants, and to arrange meetings and associate logistics, etc.
Should an alternate representative (designee) be assigned to participate in any workshop, presentation, or session, all answers and decisions of the alternate will be deemed accurate and may be used in the analysis and assessment without further qualification or review.
FCTC will provide the consultant with timely responses to all requests for information, review, and resources, as well as workspace for the project team with the ability to access vendor systems through the Internet.
FCTC will confirm IP address ranges, provide telephone number ranges, and supply target lists.
FCTC has secured all necessary rights an permissions in the systems and facilities to permit the consultant to perform the service at the FCTC's address space.
FCTC will provide access to necessary personnel for data gathering activities, such as interviews to obtain insight into the application development processes and procedures, as well as the nature of the application.
Involvement of third parties shall require a third-party agreement to be signed, unless a Service Level Agreement exists and indicates FCTC's right to audit. This does not include resources owned by the third party on which multiple clients' data or services reside.
All work will occur within weekday business hours (i.e.., 7 AM - 7 PM local time). Exceptions will be made for automated data gathering (e.g., vulnerability scanning).
The actual Project Plan will based on a delivery schedule, including workshop dates, review activities, and presentation dates that will be mutually agreed and confirmed at the start of the project.

III. ANSWERING THE RFP

A. RFP QUESTIONS

Vendors may submit questions relating to this RFP to the FCTC contact. Questions must be submitted in writing. All questions must be submitted on or before the date listed below to the address listed below in order to be considered. A written response will be published in an RFP addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and non-binding.

Any questions regarding the content, scope or intent of this RFP should be directed vial mail or email to the attention of:

Jeannie Dopson
Chief Financial Officer
2980 Collins Avenue

St. Augustine, Florida 32084

Email: jeannie.dopson@fctc.edu
904-547-3500

All questions must be submitted in writing by the date specified in this document – Friday, October 18, 2013 at 5:00 p.m. EST. All questions submitted, along with the responses, will be submitted back to the group of prospective vendors as a group with the asking of the party de-identified. Each vendor must have a designate point of contact on the RFP. FCTC will forward the responses to vendor questions to that person.

B. RESPONSE SUBMISSION AND DEADLINE

RFP Proposal responses must be submitted no later than 5:00 p.m. on Tuesday, November 12. Responses may be submitted in a .pdf format via email to the FCTC Contact, Jeannie Dopson, at jeannie.dopson@fctc.edu or responses may be submitted via mail to the address listed above. RFP responses must be clearly labeled: Information Security Program RFP Response.

IV. VENDOR EVALUATION

A. Evaluation Criteria

To be evaluated as one of the potential vendors, each vendor must provide all of the information requested. Any information not provided that has been requested must have detailed explanation as to why that information was not submitted. Vendors failing to agree to the mandatory requirements of the RFP are subject to disqualification and their cost proposals will not be scored. Entering "Not applicable" is not acceptable. Vendors responding in a satisfactory format will be evaluated by the vendor selection team based on the areas listed below:

- Did the vendor meet all of the Mandatory Requirements as outlined in this RFP
- Did the vendor complete and submit the Certification and Signature Page (Appendix A)
- Vendor knowledge and experience
- Timeliness and comprehensiveness in responding to this RFP
- Ability of vendor to meet RFP requirements
- Client references
- Total cost (with appropriate detail)

FCTC will assemble an RFP Evaluation Team that will be comprised of persons knowledgeable in the terms and scope intended by the RFP. The evaluation criteria will be weighted by the selection team and applied to vendor responses in a uniform format to determine which vendor is the best business partner for FCTC.

V. VENDOR RFP RESPONSE

Please provide the following information. In your response, please be sure to specifically state which question is being answered (i.e., A1, B3, etc).

A. Executive Summary of Company Profile:

The executive summary should contain the following information:

1. Please describe the benefits you believe FCTC will achieve through partnering with your company. Where possible, quantify the expected benefits. This may include the results of other benefit analysis performed or client contact names that may be referenced.
2. Please provide a brief description of your company and its products and services.
3. Please confirm the specific products and services that you are including in order to satisfy the RFP.
4. Please describe any experience that your company has had working with government agencies and/or entities. Include the names of a least two (2) other organizations of a similar scope and size. You will need to include the name and contact information for a person or persons at those organizations that can be used as a professional reference. You are encouraged to advise that person(s) listed that they will be contacted by FCTC for reference verification.
5. Specify the name, title, address, email, telephone and fax numbers of the contact including brief bios that define education and experience. Also please include the steps that your company takes to ensure the integrity and experience of your staff, e.g. background checks, etc.
6. List any and/or all relationships with any third party vendors and/or subcontractors who may be included in your proposed solution(s).

B. Description of Products and Services:

The products and services included in your response should address the following:

B1. Detailed description of proposed solution/services

B2. Known vulnerabilities and solutions

B3. Software tools that you will be using

B4. Methodology of non-software based vulnerability assessments, e.g. site inspections, intrusion testing, social engineering, etc.

B5. Minimum information that vendor will need to get started

B6. A description of you Quality Control Process

B7. A description of the team that the vendor will assign to the project including brief resumes outlining the experience and qualifications of team members

B8. The required professional references as requested in Section A, #4 of this RFP.

C. Cost

Please provide a cost proposal as part of your response. The cost(s) should be submitted as a fixed fee. See Appendix B for Cost Proposal Form.

APPENDIX A: CERTIFICATION AND SIGNATURE PAGE

By signing below, I certify that I have reviewed this RFP solicitation in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this bid or proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; and that I am authorized to bind the bidder in a contractual relationship.

_____

(Company)

_____

(Authorized Signature)

_____

(Representative Name, Title)

_____

(Phone Number)

_____

(Date)

APPENDIX B: COST PROPOSAL

Service	Year	Cost
Information Security Program/Virtual CISO	1	$
Information Security Program/Virtual CISO	2	$
Information Security Program/Virtual CISO	3	$
Yearly Penetration Testing	1	$
Yearly Penetration Testing	2	$
Yearly Penetration Testing	3	$