CONFIDENTIAL

SCOPE OF WORK

I. Introduction

The State of South Carolina, through the State Budget and Control Board, Division of State Information Technology (DSIT), is soliciting proposals from highly qualified offerors for the development and implementation of a statewide Information Security (INFOSEC) program as well as help in immediately addressing serious information security vulnerabilities.

DSIT intends to award a firm, fixed price contract to a qualified offeror that can lead the state in efforts to improve its security posture and create an effective enterprise INFOSEC program. The selected offeror will, among other things, lead efforts to assess the state's current INFOSEC position and help the state immediately remediate the most serious issues; identify gaps in the state's current security systems, polices, processes; develop a roadmap for improving the state's INFOSEC posture; develop and implement an appropriate governance structure for managing the project and resulting INFOSEC program; and create a security framework to guide state agencies.

The selected offeror will be ineligible for subsequent contracts awarded to implement recommendations and/or to provide specific hardware and/or software proposed as solutions during any phase of the ensuing project or projects that result from this solicitation.

II. Background

Current Structure for Managing Cyber Security

The state of South Carolina's IT enterprise is highly decentralized, with over one hundred state agencies, universities and commissions operating individual networks and managing information security within a multitude of technical and administrative "silos". The Division of State Information Technology (DSIT) possesses no legislative authority to

perform effective enterprise information security governance. Indeed, such authority does not exist anywhere within the state's IT enterprise. DSIT functions as more of a vendor of connectivity services and related products within the state government IT marketplace, operating within a mandated cost-recovery funding model.

The South Carolina IT Solutions Committee (ITSC), a successor to the earlier Architecture Oversight Committee, engages a cross-section of state agency IT directors and staff to discuss, draft and publish IT policies, but as the committee enjoys no formal governance role, compliance with its policies is entirely voluntary.

III. Required Services

As stated in the introduction of this solicitation, DSIT intends to award a firm, fixed price contract to a qualified offeror that can lead the state in efforts to implement an effective enterprise INFOSEC program and help the state immediately remediate the most serious information security vulnerabilities.

The state requires that these two interrelated projects, (1) immediately addressing serious information security vulnerabilities and (2) developing and implementing an information security program; both be carried out in parallel in order to immediately begin to return security benefits to the state while also moving the state toward a more robust, programmatic approach to remaining secure in the future. In addition, the state requires that the information security program development and implementation project be phased into actionable segments so the state can begin to implement parts of the program as they are developed. These two projects are, of course, very inter-dependent and must keep each other informed as they progress.

In order to achieve these objectives, the selected offeror must lead the state in efforts to complete, at a minimum, the following tasks and activities:

<u>Organization and Planning</u>

1. Develop a comprehensive project plan for the entire project.
2. Develop a reporting and communication plan so that state leaders and stakeholders can be kept aware of INFOSEC plans and progress toward plan objectives
3. Using appropriate risk assessment/risk management methods, determine the state's current information security position in terms of people, process and technology.
    a. Define South Carolina's "to-be" or future state security position
    b. Identify gaps between the current and the "to-be" INFOSEC positions and develop an implementation plan for improvements, including associated cost estimates for work to be done and technology to be procured in later phases of this project.
    c. The implementation plan must place a priority on solutions and preventative measures with higher payoff in terms of higher risks which are easily achievable with minimal effort and expense.
4. Develop annual funding estimates for the creation and operation of the enterprise INFOSEC program, including all personnel and hardware/software costs (this cost estimate would include costs that might be attributable at the agency and central office levels).
5. It is important that South Carolina move as swiftly as possible to identify its most pressing information security needs and align any associated funding requests with the state's budget cycle. To that end, the offeror must deliver an interim report to the South Carolina Budget and Control Board for dissemination to the South Carolina General Assembly on or before May 1, 2013. This report will:
    a. Identify initial findings regarding South Carolina's current security position
    b. Outline and discuss initial strategies and recommendations for moving forward
    c. Provide FY14 budget estimates (July 1, 2013 – June 30, 2014) for implementing initial recommendations.

In order to complete this requirement, the successful offeror must be able to quickly complete a number of activities to assess, at a high level, South Carolina's current information security position. In addition to other activities offeror may propose in order to complete this specific requirement and deliver a report by May 1, 2013, the successful offeror must complete a minimum of 3 agency security assessments. The agencies to be assessed will be determined by DSIT.

Offeror must fully explain and describe in its response how these agency assessments and other proposed activities will be completed within the first 45 to 60 days of contract award, so that the required interim report will be delivered no later than May 1, 2013.

Governance

1. Propose and assist in implementing an appropriate governance model to oversee the creation of the INFOSEC program and to direct the ongoing management and operation of the INFOSEC function.

Risk Analysis

1. Create and assist the State in adopting a data classification schema that categorizes data based on its level of sensitivity, legal and regulatory compliance requirements, and the impact to the state or any of its agencies should that data be accessed, lost, altered or destroyed without authorization. An initial high level version of this schema may need to be completed first in order to meet the state's requirement for an immediate remediation of severe risks.
2. Conduct agency-level information security risk assessments. The state of South Carolina has more than 100 agencies, boards and commissions. In addition to the initial 3 agency assessments required by item #5 in the above section entitled Organization and Planning, a minimum of 15 additional agency assessments must be completed by offeror within 2 years of contract award. DSIT will

determine the agencies to be assessed. Plans, timelines and strategies for completing these 15 additional comprehensive assessments must be proposed in order to meet the state's longer term goals.

3. Provide a complete information security agency self-assessment procedure which the state may use in the future as a part of any ongoing risk assessment process.
4. Assist the state in implementing an ongoing data classification audit policy and procedure to ensure that appropriate controls are put in place and monitored for continuing operation.

Develop Statewide Security Framework

1. Develop a federated operating model for the management of information security for the state of South Carolina that can be effective within the state's decentralized agency management environment. The model must outline roles and responsibilities for security professionals at the state and agency levels and define lines of authority and reporting channels.
2. Develop enterprise security policies, procedures and best practices to guide state agencies in the development, management, and operation of a security program at the agency level
3. Develop and recommend procedures and practices to ensure that state agencies are complying with requirements of the enterprise INFOSEC program
4. Develop models and strategies that can be used to monitor the performance and success of the state's INFOSEC program.
5. Define cyber security professional positions needed at the state and agency level.
6. Develop a training program to raise awareness of cyber security policies, procedures, strategies and best practices.
7. Assist the state in efforts to develop the capacity to support and manage any new technology or solutions implemented throughout the course of this project.
8. Develop standards for hardware, software and solutions that will need to be procured to address identified security gaps. Standards

must be defined in terms of service levels and performance measures rather than by manufacturer or vendor.

IV. INFORMATION FOR OFFERORS TO SUBMIT

INFORMATION FOR OFFERORS TO SUBMIT -- GENERAL (JAN 2006)

Offeror shall submit a signed Cover Page and Page Two. Offeror should submit all other information and documents requested in this part and in parts II.B. Special Instructions; III. Scope of Work; V. Qualifications; VIII. Bidding Schedule/Price Proposal; and any appropriate attachments addressed in section IX. Attachments to Solicitations. [04-4010-1]

INFORMATION FOR OFFERORS TO SUBMIT -- EVALUATION (JAN 2006)

In addition to information requested elsewhere in this solicitation, Offerors should submit the following information for purposes of evaluation:

Technical Proposal

A. Describe your overall project management approach and methodology for providing the services required in this solicitation; Include timelines and a high level project plan and indicate milestones for key activities
B. Describe how you will lead the state to success in completing the required tasks outlined in Section III (Required Services) above. Clearly define roles and responsibilities and indicate if you will provide all services or if you plan to lead/train team of South Carolina state employees to complete some services.

V. QUALIFICATIONS

QUALIFICATION OF OFFEROR (JAN 2006)

CONFIDENTIAL

To be eligible for award of a contract, a prospective contractor must be responsible. In evaluating an Offeror's responsibility, the State Standards of Responsibility [R.19-445.2125] and information from any other source may be considered. An Offeror must, upon request of the State, furnish satisfactory evidence of its ability to meet all contractual requirements. Unreasonable failure to supply information promptly in connection with a responsibility inquiry may be grounds for determining that you are ineligible to receive an award. S.C. Code Section 11-35-1810. [05-5005-1]

QUALIFICATIONS -- REQUIRED INFORMATION

In order to evaluate your responsibility, offeror shall submit the following information or documentation for the offeror and any subcontractor, if the value of subcontractor's portion of the work exceeds 10% of your price (if in doubt, provide the information):
(a) Include a brief history of the offeror's experience in providing work of similar size and scope.
(b) Your most current financial statement, financial statements for your last two fiscal years, and information reflecting your current financial position. If you have audited financial statements meeting these requirements, you must provide those statements. [Reference Statement of Concepts No. 5 (FASB, December, 1984)]
(c) A detailed, narrative statement listing the three most recent, comparable contracts (including contact information) which you have performed and the general history and experience of your organization.
(d) A list of every business for which offeror has performed, at any time during the past three year(s), services substantially similar to those sought with this solicitation. Err on the side of inclusion; by submitting an offer, offeror represents that the list is complete.
(e) Clearly define and fully explain the depth of your experience and expertise in providing the services requested.
(f) Describe your experience working with State Government clients.

(g) Provide information related to your expertise working with clients that have a decentralized security management model, such as exists in the State of South Carolina.
(h) Provide information regarding the skill level and experience of key staff that will be dedicated to this project. Explain the role that key staff will play in delivering the required services outline in this solicitation.
(i) List of failed projects, suspensions, debarments, and significant litigation.

VI. TERM OF CONTRACT

MAXIMUM CONTRACT PERIOD - ESTIMATED (Jan 2006)

Start date: **03/05/2013** End date: **03/04/2018**. Dates provided are estimates only. Any resulting contract will begin on the date specified in the notice of award. See clause entitled "Term of Contract - Effective Date/Initial Contract Period". [01-1040-1]

TERM OF CONTRACT -- EFFECTIVE DATE / INITIAL CONTRACT PERIOD (JAN 2006)

The effective date of this contract is the first day of the Maximum Contract Period as specified on the final statement of award. **The initial term of this agreement is 3 year, 0 months, 0 days from the effective date.** Regardless, this contract expires no later than the last date stated on the final statement of award. [07-7B240-1]

TERM OF CONTRACT -- OPTION TO RENEW (JAN 2006)

At the end of the initial term, and at the end of each renewal term, **this contract shall automatically renew for a period of 1 year, 0 month(s), and 0 day(s)**, unless contractor receives notice that the state

elects not to renew the contract at least thirty (30) days prior to the date of renewal. Regardless, this contract expires no later than the last date stated on the final statement of award. [07-7B245-1]

VII. PRICE-BUSINESS PROPOSAL

PRICE PROPOSAL (JAN 2006)

Notwithstanding any other instructions herein, you shall submit the following price information as a separate document: [08-8015-1]

Offerors must provide the following:

A. Provide a total cost to provide the services requested in this RFP. Cost must be inclusive of all travel and other expenses.
B. Provide a breakout of the total cost on a contract year basis

Offerors may propose optional services/costs such as on-going program support. These costs should not be included in the offeror's total cost to provide the required services outlined in this solicitation. The State reserves the right to negotiate a price for proposed optional services during the contract period.

Sample Cost Table to be completed by Offeror:

Total Cost to Provide Required Services:	$0.00
Costs Year 1	$0.00
Costs Year 2	$0.00
Costs Year 3	$0.00
Optional Year 1	$0.00
Optional Year 2	$0.00

VIII. AWARD CRITERIA

CONFIDENTIAL

AWARD CRITERIA -- PROPOSALS (JAN 2006)

Award will be made to the highest ranked, responsive and responsible offeror whose offer is determined to be the most advantageous to the State. [06-6030-1]

AWARD TO ONE OFFEROR (JAN 2006)

Award will be made to one Offeror. [06-6040-1]

COMPETITION FROM PUBLIC ENTITIES (JAN 2006)

If a South Carolina governmental entity submits an offer, the Procurement Officer will, when determining the lowest offer, add to the price provided in any offers submitted by non-governmental entities a percentage equivalent to any applicable sales or use tax. S.C. Code Ann. Regs 117-304.1 (Supp. 2004). [06-6057-1]

EVALUATION FACTORS -- PROPOSALS (JAN 2006)

Offers will be evaluated using only the factors stated below. Evaluation factors are stated in the relative order of importance, with the first factor being the most important. Once evaluation is complete, all responsive offerors will be ranked from most advantageous to least advantageous. [06-6065-1]

Qualifications

40 points

The Offeror's financial responsibility and financial strength must reflect sound financial stability; the Offeror's experience and references should provide evidence of its depth and breadth of experience as well as evidence of successful past projects

Technical Proposal

35 points

The completeness and suitability of the Offeror's proposed technical solutions to meet or exceed the specified requirements.

Business Proposal

25 points

The total cost of the proposed solution on the business and financial operations of the State.

Comment [p1]: The points associated with each category will not be included in the issued RFP, per standard procurement practices.