

**STATE OF ALABAMA  
DEPARTMENT OF FINANCE  
INFORMATION SERVICES DIVISION**

**INVITATION TO BID FOR**

**TEMPORARY PROFESSIONAL SERVICES**

**IT CYBER SECURITY**

**9 July 2009**

## **SECTION I INTRODUCTION**

**I.1. Statement of Purpose:** The State of Alabama, hereafter referred to as State, Department of Finance – Information Services Division (ISD) hereafter referred to as ISD, has established a need for a contract for Temporary IT Cyber Security Specialist functions only to be staffed as needed with outsourced IT Cyber Security Specialist personnel. The purpose of this Invitation to Bid (ITB) is to obtain competitive bids from interested vendors, for the purpose of establishing a Purchasing Contract (Contract Release Order – CRO and Statement of Work - SOW) for the levels of Temporary IT Cyber Security Specialist specified in this ITB, with award to a single vendor, for a period of one year from date of award to be used as necessary to fulfill the needs of ISD. ISD will have an option to issue up to four (4) additional 12 month renewals, with the same terms and conditions as the original. The hourly price may increase by no more than 2% above the previous year's rate for years 2 through 5. Additional contract renewals, if said option is exercised by ISD, would begin the day after the last contract term expires.

**I.2. Scope:** This ITB solicits the delivery of temporary services of IT Cyber Security Specialists that will work under the guidance and direction of the ISD Chief Information Security Officer (CISO) in concert with one of the Universities in Alabama currently designated by the National Security Agency (NSA) as a National Centers of Academic Excellence in IA Education (CAEIAE) university to implement vulnerability management processes to enhance the IT security of systems supporting the State of Alabama. The National Cyber Security Division (NCSA) of the Department of Homeland Security (DHS) developed guidance and tools to assist critical infrastructure owners and operators in assessing and managing their cyber risks. One of these tools, the Cyber Security Vulnerability Assessment (CSVA), enabled ISD to self-assess their overall cyber security posture.

The CSVA tool was used to assess the State of Alabama cyber infrastructure vulnerability by evaluating the State of Alabama network and server security policies and procedures. The findings indicate that there are several security practices that ISD performs very well including physical and environment controls, system acquisition, and security policies in general; however, critical gaps were identified in risk and vulnerability management. The temporary IT Cyber Security Specialists required by this ITB will be used to design and implement a vulnerability management program.

The scope of this Cyber Security Specialists ITB is to provide a wide range of cyber security capabilities ranging from basic security policy development up to and including a multi-faceted automated enterprise vulnerability management capability within the State of Alabama cyber infrastructure that supports all enterprise managed information systems. This ITB includes a range of capabilities including three primary security objectives that will improve the ability of the State of Alabama cyber infrastructure to withstand cyber-attack:

- Harden the state's cyber infrastructure by ensuring systems and applications are patched against known vulnerabilities that attackers are likely to exploit.
- Examine closely the state cyber risk posture and provide appropriate mitigating actions.
- Implement end devices to protect against the risk of data loss.

These combined objectives will provide ISD with a sustainable vulnerability management capability to monitor and protect the State of Alabama computing environment from the threat of cyber-attack.

Vulnerability management is a process that can be implemented to make IT environments more secure. The temporary IT security specialists must provide the capability to design and implement a full range of vulnerability management functions including:

- Policy definition which enhances existing policy and may include device configurations, user identity and resource access.
- Baseline the environment to identify vulnerabilities and policy compliance.
- Prioritize mitigation activities based on external threat information, internal security posture and asset classification.
- Shield the environment, prior to eliminating the vulnerability, by using desktop and network security tools.
- Mitigate the vulnerability and eliminate the root causes.
- Maintain and continually monitor the environment for deviations from policy and to identify new vulnerabilities.

**I.3. ITB Requirements:** The Bidder must bid an hourly rate for each separate level of Security Specialist. The listing of bid line items is included in section III and the complete basic description of project requirements by line item is included in Section VII: General Statements of Work (SOWs) and Other Requirements.

## SECTION II

### General Information

**II.1. ITB Contact Information:** All questions concerning purchasing procedures related this ITB must be submitted in writing to the below.

NOTE: If sending correspondence by USPS overnight, FedEx, UPS or other overnight services use ZIP CODE 36104!

Jennifer Loretz, Buyer  
State of Alabama, Department of Finance  
Division of Purchasing  
RSA Union, Suite 192  
100 N. Union St.  
Montgomery, AL 36130  
E-mail: [Jennifer.Loretz@purchasing.alabama.gov](mailto:Jennifer.Loretz@purchasing.alabama.gov)  
FAX Number: (334) 242-4419

All questions concerning line item requirements or special terms and conditions defined herein must be submitted in writing to:

Art Bess, Assistant Director  
Information Services Division  
64 North Union Street, Room 200  
Montgomery, Alabama 36130 - 2626  
Fax (334) 353-9301  
Email: [art.bess@isd.alabama.gov](mailto:art.bess@isd.alabama.gov)

From the date of issuance of this ITB until the awards are made and announced all questions concerning this ITB shall be directed to the points of contact listed above. It is not permissible for any Bidder, or any entity working on behalf of a Bidder, to solicit information regarding this ITB from any government source (Federal or State) other than from the official points of contact listed above. Any unauthorized solicitations for information that are reported are grounds for disqualification of the Bidder's bid.

**II.2. Vendor Qualifications:** All vendors must meet the following minimum qualifications:

1. Bidder must include documentation showing that the bidder grossed an average minimum of \$3 million annually from the sale of professional security consulting services within the U.S., during the past three years.
2. Bidder must include an audited financial statement for the most recent fiscal year demonstrating a history of profitability and financial stability. (Bidder may submit financial information in a sealed envelope only to be opened at the time of bid evaluation)
3. Bidder must include in its response a statement that it understands that the timing of the payment cycle for the State of Alabama, Department of Finance (ISD) to the awarded vendor may not be in harmony with the vendor's payroll policy and that the ISD expects the vendor to compensate its' employees engaged on this contract in a timely manner

- according to a regular and standard payroll cycle such as weekly; Bi-weekly; or monthly.
- a. Bidder **must** provide its current payroll policy with respect to the frequency of payroll payments to its employees and contract personnel.
4. Bidder must include documentation showing that the bidder has demonstrated proficiency in grant writing for the public sector within the past three years.
  5. Bidder must include documentation showing that the bidder has experience and demonstrated proficiency in the use of the following toolset in making an assessment of an organization's overall cyber security posture within the past three years:
    - a. Cyber Security Vulnerability Assessment (CSVA)
    - b. HP Web Inspect
    - c. AppDetective
    - d. eEye Retina
    - e. Lumension Patchwork
    - f. Tenable Nessus
    - g. Tenable Passive Vulnerability Scanner
    - h. PowerGrep
    - i. Ecora
  6. Bidder must have a minimum of three (3) years experience in providing the following aspects of Information Security:
    - a. Policy definition including defining the desired state for device configurations, user identity and resource access.
    - b. Developing a Baseline of the environment to identify vulnerabilities and policy compliance.
    - c. Prioritizing mitigation activities based on external threat information, internal security posture and asset classification.
    - d. Shielding the environment, prior to eliminating the vulnerability, by using desktop and network security tools.
    - e. Mitigating the vulnerability and eliminating the root causes. Maintaining and continually monitoring the environment for deviations from policy and to identify new vulnerabilities.
  7. Bidder must have a minimum of Five (5) years experience Developing and Implementing:
    - a. Automated Enterprise Vulnerability Management Programs
    - b. Enterprise Risk Management Programs.
    - c. Enhanced Endpoint Security Control Capabilities.

**II.3. Incorrect Bid Information:** If ISD determines that a Bidder has provided, for consideration in the evaluation or award process any false or incorrect information which the Bidder knew or should have known was materially incorrect, that bid shall be declared non-responsive, and the bid will be disqualified.

**II.4. Quantity:** The exact quantity of purchases for each line item on this solicitation is not known. ISD does not guarantee that the ISD will buy any amount. CRO will be placed by ISD as needed at the direction of the ISD CISO. Minimum order amounts are not applicable to this bid.

**II.5. Proposal of Alternate Services:** Bids of alternate services (i.e., bids that offer something different from that requested by the ITB) shall be declared non-responsive and be disqualified.

**II.6. Insurance:** The successful Bidder is required to carry and to provide certificates of the following insurance coverage during the term of the purchase order:

**II.6.1. Workmen's Compensation:** Workmen's compensation as required by the laws of Alabama, the state in which the work is being performed.

**II.6.2. General Liability and Property Damage:** Comprehensive general liability and property damage insurance with bodily limits of \$300,000 per each occurrence and property damage limits of \$100,000 per each occurrence. Evidence of said coverage must be included in the bid and reference this ITB number.

**II.6.3. Failure to Provide Continuous Insurance Coverage:** Should the CONTRACTOR fail to provide continuous insurance coverage as described above, the contract may be terminated.

**II.6.4. Limited Liability:** CONTRACTOR services hereunder shall be on a best efforts basis under supervision except as provided for in Sections II.8.1 and II.8.2 above respecting personal injury and property damage. ISD will not be liable for any direct, indirect, special, or consequential damages (including loss of profits) arising out of the performance of services by CONTRACTOR under this CONTRACT.

## **II.7. Conflict of Interest and Bid Restrictions:**

**II.7.1. Required Alabama Disclosure Statement:** By submitting a bid, the Bidder certifies that no amount shall be paid directly or indirectly to an employee or official of the State of Alabama as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Bidder in connection with the procurement under this ITB. Act 2001-955 requires the winning Bidder to submit an Alabama Disclosure Statement within ten days of purchase order award. Bidders may go to the site below to download a copy of the Alabama Disclosure Statement:

[http://www.ago.state.al.us/ag\\_items.cfm?Item=70](http://www.ago.state.al.us/ag_items.cfm?Item=70)

**II.7.2. ITB Amendment and Cancellation:** ISD reserves the unilateral right to amend this ITB in writing at any time. ISD also reserves the right to cancel or reissue the ITB at its sole discretion. Any changes or modifications to this ITB will be made by a written addendum issued by the Department of Finance's Division of Purchasing. Bidders shall respond to the final written ITB and any exhibits, attachments, and amendments.

**II.7.3. Contract Restrictions:** The contract established as a result of award may only be used for acquisition of Temporary IT Security Specialist personnel as stated in this ITB. Use of this contract to provide positions, other than those specified may result in contract termination.

**II.7.4. Disclosure of Bid Contents:** Upon submission, all bids become the property of the State of Alabama. Upon contract award, all information contained in the bids will become public information.

**II.7.5. News Releases and Public Announcements:** News releases or other public announcements pertaining to this acquisition may only be made with prior written consent and approval of text by the Finance Director of the State of Alabama.

**II.8. Sufficient Appropriation:** ISD relies on grants and federal funding for a significant portion of ISD's resources. Positions specified in the CRO may not be filled if federal funds have not been obtained. Any CRO order placed as a result of the ITB process may be terminated if sufficient appropriations or authorizations do not exist. Such termination will be effected by sending written notice to the CONTRACTOR. ISD's decision as to whether sufficient appropriations and authorizations are available will be accepted by the CONTRACTOR as final.

**II.9. Bid Awards and Governing Law:** This procurement is governed by Section 41-16-20, et seq., Code of Alabama (1975), and the administrative regulations of the Department of Finance, Division of Purchasing. ISD may award a CONTRACT by accepting the **lowest responsible bid** that meets all the specifications for all services required by this ITB. ISD reserves the right to incorporate standard State of Alabama contractual provisions into any Contract executed as a result of any bid submitted in response to this ITB. Appropriate State of Alabama Purchasing laws, terms, and conditions will apply, including a limitation on the term of the CONTRACT to five years, including renewal periods. The award of the CONTRACT will be reviewed by legal counsel of the Department of Finance as to compliance with State of Alabama laws and the terms and conditions of this ITB.

**II.10. The State of Alabama retains the right to reject any and all bids.**

## **SECTION III**

### **Bid Format and Content**

#### **III.1. Response Preparation and General Bid Format Requirements:**

**III.1.1. Bid Responses:** All bid responses must be in the same numerical paragraph labeling, format and sequence as shown in this document.

**III.1.2. Bid Preparation Costs:** ISD will not pay any costs associated with the preparation, submittal, or presentation of any bid.

**III.1.3. Response Submissions and Bid Format:** The bidder must submit one original and two copies of their bid response. Each document must be signed and duly notarized. In addition to all other requested information, Bidders must submit three (3) soft copies of their bid proposal on CD or DVD media for use during bid evaluation. Bid must be in the same format and sequence as presented in this ITB. Bid responses must be clearly labeled to indicate the corresponding paragraph that the response is referring to. The bid must contain a brief statement from the bidder in response to each requirement (by paragraph I.1., I.2., etc.) describing how the Bidder intends to meet each of the requirements of the Invitation to Bid. Simple statements such as “Acknowledged” or “Understand” are not sufficient to meet this requirement. The bid must contain an explanation of how the Bidder will meet each of the requirements specified in the ITB. A bidder may not submit their own contract terms and conditions in a response to this ITB. If a bid contains supplemental terms and conditions, ISD, at its sole discretion, may determine the bid to be a non-responsive counter-offer, and the bid may be rejected.

**III.1.4.** Line item bids must be prepared in response to the General Statement of Work (Section VII) which is to the Bidder a straightforward and complete generic description of the various Cyber Security Specialist qualifications and expertise of their personnel. Failure to follow the specified format of the bid sheet, to label the responses correctly, or to address all of the requirements may, at ISD’s discretion, result in the **disqualification of the Bid**.

**III.1.5.** Bids must not contain extraneous information. All information presented in a Bid must be relevant in response to a requirement of this ITB, must be clearly labeled. Any information not meeting these criteria shall be deemed extraneous and shall in no way contribute to the evaluation process.

**III.2. Bid Responses Requirements:** The Bidder must respond to all line items with their maximum hourly dollar rate whenever they meet EVERY requirement listed in the respective general SOW’s for that line item. The rates bid must be all inclusive including all expenses of providing that line item classification to ISD for an unspecified period of time. The maximum hourly dollar rate must be entered on Table 3 as the \$ per Hourly Rate Bid. Bidders are required to use this rate and perform the calculations indicated in Table 3 to determine the Overall Priced Percentage of Utilization.

**III.2.1. Bid Line Items:** Each line item is listed below. The general Statement(s) of Work for each line item is included in Section VII.

<b><u>Line# -- Item Description</u></b>	<b><u>SOW #</u></b>	<b><u># Positions</u></b>	<b><u>Job Classification</u></b>
001 – ISD Cyber Security	09-001	As Required	Program Manager
002 – ISD Cyber Security	09-002	As Required	Project Manager
003 – ISD Cyber Security	09-003	As Required	Sr. Systems Analyst
004 – ISD Cyber Security	09-004	As Required	Systems Consultant/Analyst
005 – ISD Cyber Security	09-005	As Required	Sr. Systems Engineer
006 – ISD Cyber Security	09-006	As Required	Technical Writer

## SECTION IV Evaluation process

**IV.1. ITB Evaluation Requirements:** The first evaluation criteria will be overall per hourly cost which will be computed as an **Overall Priced Percentage of Utilization shown in Table 3 of paragraph IV.1.2.** The low bid will then undergo a Qualification Review based on the bidders’ fulfillment of the requirements of **Sections III, IV and VII** of this ITB. In the event the low bid does not address all elements of the evaluation requirements, the bid will be “Disqualified” and the next lowest bid will be considered. This process will be continued in successive order until the lowest bid is determined to meet all bid requirements. If ISD determines that none of the bids meet the requirements of this ITB, ISD retains the right to cancel this ITB and at ISD’s sole discretion, may or may not re-bid this proposal.

**IV.1.1. Overall Priced Percentage of Utilization computation:** Due to the wide variance in anticipated utilization, the determination of Overall Priced Percentage of Utilization will be computed using the following estimated **Utilization Percentages.** For the purposes of evaluating this ITB, the overall per hourly cost will be computed as the sum; of the product of each individual per-hourly cost, multiplied by the respective utilization percentage shown in Table 1 below.

Service Provided	Utilization Percentage
Program Manager – ISD-09-001	3%
Project Manager – ISD-09-002	16%
Sr. Systems Analyst – ISD-09-003	16%
Systems Consultant/Analyst - ISD-09-004	32%
Sr. Systems Engineer - ISD-09-005	32%
Technical Writer - ISD-09-006	2%

**Table 1**

**For example:**

Line Item	Per-Hourly Rate Bid	Utilization Percentage	Priced Percentage of Utilization
<b>Program Manager – ISD-09-001</b>	\$120	3%	\$3.09
<b>Project Manager – ISD-09-002</b>	\$110	16%	\$17.51
<b>Sr. Systems Analyst – ISD-09-003</b>	\$100	16%	\$15.92
<b>Systems Analyst - ISD-09-004</b>	\$85	32%	\$27.06
<b>Sr. Systems Engineer - ISD-09-005</b>	\$65	32%	\$20.69
<b>Technical Writer - ISD-09-006</b>	\$50	2%	\$0.96
		<b>Overall Priced Percentage of Utilization</b>	<b>\$85.23</b>

**Table 2**

In the example shown above (Table 2), the Overall Priced Percentage of Utilization for this bid is \$85.23. Each bid must be computed in a similar manner to determine the lowest bid.

**IV.1.2. Overall Priced Percentage of Utilization Bid.** The table shown below (Table 3) is provided for Bidders to fill-in the \$ Per Hourly Rate Bid for each line item. (**NOTE:** per paragraph VI.6.3., travel expenses must be included in the Per Hourly Rate Bid) Bidders must then fill-in the \$ Priced Percentage of Utilization amount resulting from the computation of their bid rate times the Utilization percentage for each line item. Sum this column and enter the **Overall Priced Percentage of Utilization.** This dollar amount will form the basis of determining the low bid for this ITB. The low bid that otherwise meets all the requirements of this ITB will be awarded the bid.

**All Bidders must complete the Overall Priced Percentage of Utilization for their respective bid in the table shown below.**

Line Item	\$ Per-Hourly Rate Bid	Utilization Percentage	\$ Priced Percentage of Utilization
Program Manager – ISD-09-001	\$____.____	3%	\$____.____
Project Manager – ISD-09-002	\$____.____	16%	\$____.____
Sr. Systems Analyst – ISD-09-003	\$____.____	16%	\$____.____
Systems Analyst - ISD-09-004	\$____.____	32%	\$____.____
Sr. Systems Engineer - ISD-09-005	\$____.____	32%	\$____.____
Technical Writer - ISD-09-006	\$____.____	2%	\$____.____
		<b>Overall Priced Percentage of Utilization</b>	\$____.____

**Table 3**

**IV.2. Security Specialist Bid Evaluation Requirements:** The information required below, submitted by the Bidder, will be used in addition to pricing and other ITB response requirements during the evaluation process. The following are minimum requirements that must be met by bidder. **Bidder must include documentation substantiating these requirements.**

1. Bidder must include documentation showing that the bidder has demonstrated proficiency in providing an automated enterprise vulnerability management program as specified in VII.1.1 of this document.
2. Bidder must include documentation showing that the bidder has demonstrated proficiency in providing an automated enterprise vulnerability management program as specified in VII.1.2.1 of this document.
3. Bidder must include documentation showing that the bidder has demonstrated proficiency in providing an Enterprise Risk Management Program as specified in VII.1.2.2 of this document.

4. Bidder must include documentation showing that the bidder has demonstrated proficiency in providing an Enhanced Endpoint Security Control Capability as specified in VII.1.2.3 of this document.

**IV.2.1.** Bidder must provide documentation for all cyber security vulnerability management projects where the bidder has provided professional cyber security specialists in the past 3 years. Information provided must include:

1. Client Name, Address and Telephone Number.
2. Scope of the project.
3. Name of IT security specialist(s).
4. Responsibilities of the IT security specialist(s).
5. Length of project.
6. Project outcome to include if project requirements and timelines were satisfied.
7. Provide documentation for role of the bidders company in providing IT security specialist(s) to client sites for a period of not less than 3 years prior to the date of issuance of this ITB.

8. Bidder must have a minimum of 3 years experience working with one of the Universities in Alabama currently designated by the National Security Agency (NSA) as a National Centers of Academic Excellence in IA Education (CAEIAE) University implementing vulnerability management processes.
9. Cyber security projects where work was done for State of Alabama agencies.
10. Bidder must have a minimum of 3 years experience in providing cyber security personnel.
11. Bidder's annual revenues from providing temporary cyber security personnel and percent of revenues from all sources.
12. Bidder must have corporate headquarters in Alabama. Must submit business address and licensing information with the bid response.
13. Bidder may not use sub-contractors.
14. Bidder must provide written acknowledgement that any candidate for the skill levels submitted in response to this bid have been employed by the bidder for a minimum of one year.
15. Any other information pertinent to evaluation of this ITB.

**IV.2.2.** In addition to the documentation stated above, the bidder must agree in their bid response to abide by the following requirements if awarded the resulting contract:

1. Upon receipt of the CRO and SOW the awarded contractor must provide three (3) candidate resumes and Candidate Data Sheets (CDS) to ISD within 10 calendar days.
2. Must have the selected candidate available to commence work no later than 15 business days after notification of selection by ISD.
3. Bidder must require all candidates for cyber security specialist to have been trained in, certified or been exposed to cyber security vulnerabilities, principles and practices methodology prior to submittal of the candidate for any CRO/SOW issued by ISD.
4. Bidder will be responsible for the accuracy and completeness of duties in cyber security work history of the candidates submitted.

## **SECTION V**

### **General Terms and Conditions**

**V.1. Issuance of Contract Release Orders (CRO) and Statement of Work (SOW):** ISD will initiate a CRO through State Purchasing to the appropriate CONTRACTOR for a specific line item (Security Specialist). The CONTRACTOR will offer to the up to three (3) candidates as specified in the CRO and SOW that could match the requirements as specified. ISD reserves the right to interview any or all candidates submitted. After consideration of the qualifications of the candidate, ISD will notify the CONTRACTOR with a letter of acceptance of the candidate that meets all the qualifications of the CRO and SOW. If none of the candidates are acceptable ISD will request more candidates and the CONTRACTOR will respond accordingly by submitting more candidates with the Candidate Data Sheets (CDS) found in Attachment A. If CONTRACTOR is unable to offer an acceptable candidate, ISD will void the award of the ITB to CONTRACTOR and award to next lowest Bidder. If there is not one then the ISD may re-bid the CONTRACT.

**V.2. ISD Contract and Contract Release Order Terms and Conditions:** The CRO between ISD and the CONTRACTOR will follow the format specified by the State of Alabama and contain the terms and conditions set forth in this ITB. The contents of this ITB, as revised and/or supplemented and the successful CONTRACTOR bid will be incorporated into and become part of the terms and conditions of any resulting CONTRACT and any duly issued CRO.

**V.3. Candidate Data Sheet Information Review:** The Candidate Data Sheets (CDS) (See Attachment A), submitted in response to a SOW, must be complete as requested and include sufficient detail information to indicate the candidate meets or exceeds every requirement as defined in the SOW. If the information on the CDS is incomplete or does not indicate the candidate meets or exceeds every requirement as defined on the SOW the candidate will be considered non-responsive and will be rejected. If the candidate appears to be qualified based on the information provided in the CDS, ISD may conduct a further validation of the CDS. If the validation of the CDS does not confirm the candidate meets or exceeds every requirement as defined on the SOW the candidate will be considered non-responsive and will be rejected. In the event that a security specialist must be replaced, that replacement individual must meet the same criteria as the original employee, thereby ensuring that the original employee is replaced with another employee with commensurate experience and qualifications.

**V.4. Nondiscrimination:** No person shall be excluded from participation in, be denied benefits of, be discriminated against in the admission or access to, or be discriminated against in treatment or employment in State contracted programs or activities on the grounds of handicap and/or disability, age, race, color, religion, sex, national origin, or any other classification protected by federal or State of Alabama Constitutional or statutory law; nor shall they be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of contracts with the State or in the employment practices of the State's Bidders. Accordingly, all Bidders entering into contracts with the State shall, upon request, be required to show proof of such nondiscrimination and to post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.

**V.5. Knowledge Transfer:** CONTRACTOR agrees to require their personnel to make a good faith effort to convey knowledge and provide on-the-job training, to appropriate employees prior to the termination of the CRO. CONTRACTOR agrees to require their personnel to make a good faith effort to train appropriate employees in the use and maintenance of any software developed during the course of the CRO. ISD agrees to make a good faith effort to identify the appropriate ISD employees and to provide such employees in a timely manner with necessary prerequisite training and with adequate on-the-job training time

**V.6. Documentation:** CONTRACTOR agrees to require their personnel to develop and provide documentation sufficient to provide ISD with a history of the related activities and audit trail of the project managed as required in the course of the CRO. ISD agrees to schedule reasonable work hours for CONTRACTOR personnel to develop and provide documentation sufficient to document the activities of CONTRACTOR personnel during the course of the CRO.

**V.7. Limitations of Charges - Quality of Work:** CONTRACTOR agrees to perform the work specified in the CRO/SOW in accordance with industry standards and agrees that ISD has final acceptance of work products. ISD will indicate the accomplishment of work by signing the time sheets for the work period.

**V.8. Confidentiality of State of Alabama Materials or Information:** All materials or information (e.g., verbal, written or electronic) furnished by relating to State of Alabama business functions or processes shall be considered “proprietary and confidential” by the CONTRACTOR personnel and its designees. Materials include, but are not limited to, memoranda, organization charts, official correspondence, e-mail, telephone correspondence, internet/intranet activity, studies, plans, reports, surveys, analyses, and/or projections (except such information and materials as may already be public knowledge or established to be in the public domain). CONTRACTOR personnel and its designees shall not disclose any of such materials or information without written approval. Breach of confidentiality may result in disciplinary action and/or criminal prosecution pursuant to the rules and regulations of the State of Alabama ISD Security policy and procedures manual (up to and including termination) and as governed by the laws of the State of Alabama (up to and including fines and/or imprisonment).

**V.9. Disposition of materials upon termination or expiration of CRO-Contract:** Upon termination or expiration of the CRO, all software, documentation, secure access control cards, building keys, or materials belonging to the CONTRACTOR, ISD, or State of Alabama shall be returned to the respective owner thereof and no copies shall be retained by the non-owning party.

**V.9.1. Contractor Software or Documentation:** Software or documentation developed by the contractor prior to this CRO or developed by the contractor outside of this CRO and used by the contractor to fulfill its obligation under this CRO will remain the exclusive property of the contractor. ISD, the State of Alabama and its employees will treat as “Confidential” all software or documentation referred to in this paragraph (except such information as may be established to be in the public domain) and shall not disclose to third parties any of such contractor products without the contractor’s prior written approval.

**V.9.2. Software and Documentation Deliverables:** Software or documentation developed for the State of Alabama by contractor personnel while performing services for the State of Alabama on an hourly rate basis pursuant to this CRO shall be the exclusive property of the State of Alabama provided that such software is not derived from software previously developed by the contractor.

**V.10. Special Actions to be taken for Termination of Contractor Personnel:** Upon ISD notifying the CONTRACTOR of the need to terminate one or more of their employees for any valid reason, the CONTRACTOR will send a manager to the ISD or State of Alabama site and they will obtain all items as noted above that are the property of ISD or the State of Alabama. The manager will secure these items including all files, software and intellectual property belonging to the State of Alabama that may be in the CONTRACTOR's work area or resident on the CONTRACTOR's computer, email or disks and ensure that the property is returned to the ISD Chief Information Security Officer (CISO). The manager will then retrieve their CONTRACTOR's personal belongings and escort the terminated employee(s) from the premises with instructions not to return to the site under penalty of trespass.

**V.11. Personnel Rotation and Status Conversion:**

**V.11.1. Personnel Rotation:** CONTRACTOR agrees not to replace any CONTRACTOR personnel obtained under any CRO during the performance of any CRO without first obtaining consent from the ISD Chief Information Security Officer.

**V.11.2. Requested Removal of Contractor Personnel:** ISD may direct the immediate removal of an individual by the CONTRACTOR with (continuation of work order) or without (termination of work order) replacement. Such action shall be taken only when in the opinion of ISD such individual's performance is unacceptable, conduct is disruptive, or is otherwise in the best interest of ISD or the State of Alabama. The CONTRACTOR shall remove such individual immediately and in an effective manner upon notification of such directed removal by ISD.

**V.12. Restriction of Non-compete Agreements:** The CONTRACTOR agrees to enter into an appropriate agreement with the individuals set forth in a CRO to allow those individuals to enter into discussions with ISD representatives, and to accept employment with ISD or any other agency of the State of Alabama, without the risk of suit by the CONTRACTOR under the terms of any covenant not to compete that the CONTRACTOR may hold.

**V.13. Restriction of Recruiting ISD or other State of Alabama Personnel:** During the term of this CONTRACT, the CONTRACTOR shall not solicit to hire, either directly or indirectly, any ISD or other State of Alabama personnel. For a period of twelve (12) months after the termination of this CONTRACT, the CONTRACTOR shall not solicit to hire, either directly or indirectly, any ISD or other State of Alabama personnel the CONTRACTOR may have come in contact with as a result of this CONTRACT without the written consent of the ISD Chief Information Security Officer.

**V.14. Termination of Contract Release Order:** Any CRO may be terminated by either party by written notice in the event the other party fails to perform its obligations as stated in this ITB and the duly issued respective CRO. No notice of termination shall be given unless the party in

default has been given prior written notice of its default and has failed to cure said default within thirty (30) days of notice, except in the case of an overdue invoice. Upon notification, ISD shall pay such overdue invoice within thirty (30) days, or the CONTRACTOR shall have the right to terminate the CRO forthwith and to recover for all services and products performed and delivered prior to the date of termination.

**V.15. Contractor Personnel Benefits:** The CONTRACTOR acknowledges that CONTRACTOR Personnel are not entitled to any benefit, compensation, or allowance provided for merit system employees of the State of Alabama.

**V.16. Inspection:** All work under a CRO shall be subject to inspection by the ISD Chief Information Security Officer, or his designated representative, at any reasonable time and place. Any inspection by ISD shall be performed in such a manner so as not to unduly delay the work.

**V.17. Other Contracts:** It is agreed that the CRO is subject to re-negotiation to comply with the requirements of any applicable federal or State of Alabama law or regulation.

## **SECTION VI**

### **Special Terms and Conditions**

**VI.1. Location and Work Space:** All CONTRACTOR staff retained pursuant to the CONTRACT will be assigned to the ISD Chief Information Security Officer (CISO) and will be based in Alabama at sites designated by ISD. The specific requirements of each project will be defined by the CRO. Security vulnerability projects routinely require daily face to face interaction between project members. ISD will normally provide the CONTRACTOR staff with a work space, access to telephones, office supplies, and connections to the relevant State LAN/WAN and/or mainframe environment. There may be occasions where it is more advantageous or specific projects may require the CONTRACTOR to provide support for the CONTRACTOR staff. In that case, the terms and conditions of this support will be governed by the CRO.

**VI.2. Work Hours, Absences and Restrictions:** Although Normal State working hours are 8:00 a.m. to 5:00 p.m., Monday through Friday, ISD does not anticipate that the Security Specialists will be required to work a normal 40 hour week. The high skill levels stated in this ITB may only require that the Security Specialists work occasionally for a few hours at a time. Although every outsourced IT position is subject to an overtime requirement (including but not limited to longer work days, weekends, and holidays) ISD is not obligated to provide supervision outside of normal ISD working hours. The ISD Chief Information Security Officer (CISO) will determine the structure of the workday and the number of hours to be worked per week. ISD reserves the right to modify the work hours in the best interest of the project. Required overtime will be determined and pre-approved by the ISD CISO and will be compensated at the normal rate established in the CRO between ISD and the CONTRACTOR. The CONTRACTOR staff shall observe the same standard holidays as ISD employees: New Year's Day, Martin Luther King Jr./Robert E. Lee Day, Presidents' Day, Confederate Memorial Day, National Memorial Day, Jefferson Davis' Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving, and Christmas (generally two (2) or more days); approximately twelve (12) total days. ISD does not compensate CONTRACTOR for holiday pay.

**VI.2.1. Absences:** The ISD Chief Information Security Officer (CISO) intends to integrate the CONTRACTOR staff into the STATE workforce under his control in order to accomplish the requirements of each specific project as required. Therefore, CONTRACTOR personnel must acquire permission from the ISD CISO for all absences. The ISD Chief Information Security Officer (CISO) has the authority to deny any request for leave that may impact the scheduled completion of a specific project.

**VI.2.2. Work-Place Restrictions:** All state facilities are non-smoking buildings. Each building has area(s) designated for smoking and this is generally a loading dock, parking garage, etc. CONTRACTOR personnel will be paid for time at their place of work and will not be compensated for smoke breaks, regardless of duration. CONTRACTOR personnel will make arrangements for accounting for this time with their respective manager.

**VI.3. Training:** If CONTRACTOR staff personnel are assigned to an ISD project or support area and the technology associated with their assignment changes, the CONTRACTOR is

responsible for training of their staff personnel in the new or changed technology. This responsibility includes all fees associated with the actual training course, travel expenses, and also the hours the individual spends in training. The maximum liability to the CONTRACTOR firm for training hours for any individual will be two weeks per year.

**VI.4. ISD and State of Alabama Rules:** CONTRACTOR personnel assigned to ISD are bound by the State of Alabama rules for computer and Internet usage and will be required to sign Alabama Computer Access Security, Privacy, and Code of Conduct agreements, as required of ISD employees (See Attachment B). Some positions may have additional requirements such as criminal background checks, and drug screenings as is the case of the CRO's of Information Services Division. Any such special requirement will be defined by the in the statement of Work (SOW). CONTRACTOR will be responsible for any costs associated with ensuring their personnel meet all requirements prior to assignment to ISD.

**VI.5. Right to Refuse Contractor Personnel:**

**VI.5.1. Work History with ISD:** ISD reserves the right to refuse, at its sole discretion, any candidates provided by the CONTRACTOR that has an unfavorable work history with the State of Alabama. Reasons could include, but are not limited to, unprofessional departure from prior position(s), requested removal due to low performance or disruptive behavior, discovered unsatisfactory deliverables after departure of person, or potential of candidate to cause disruption or delay to project progress.

**VI.5.2. Other Work History or Personnel Issues:** ISD reserves the right to refuse, at its sole discretion, any candidates provided by the CONTRACTOR whose history indicates a problem with violence, unethical or unlawful behavior, professional instability, inability to work in a professional manner, or any other behavior or personality trait that would cause disruption or delay to project progress.

**VI.6. ITB Line Items - Statement of Work (SOW):**

**VI.6.1. Statement of Work Requirements:** The requirements for each line item will be defined in the Statement of Work (SOW) documents. All Security Specialist line items are listed in Section IV with the corresponding general SOW in Section VII. Requirements include all special, general and educational expertise expected of the CONTRACTOR personnel. CONTRACTOR must provide individuals that meet or exceed the stated minimums for EVERY requirement listed on the SOW.

**VI.6.2. Multiple Positions per SOW:** Each Statement of Work represents one job classification but may be used to fill multiple positions. The requirements defined on a SOW apply to all positions being filled through that SOW.

**VI.6.3. Travel Requirements:** The CRO may indicate the requirement for travel as a condition of the position. Bidders and Candidates should be aware of this requirement and only bids conforming to willingness to travel should be submitted for that CRO. CONTRACTOR is responsible for any and all travel expenses incurred by CONTRACTOR personnel in performance of the duties specified in the Statement of Work. ISD anticipates that travel

expenses shall be no more than five percent (5%) of the total cost of any CRO issued as a result of this ITB. Bidders must consider this requirement in their calculations when computing their personnel costs and include these travel expenses in the per hourly bid rate shown in paragraph IV on Table 3. ISD will not otherwise reimburse CONTRACTOR for any additional travel expenses. Where travel of CONTRACTOR personnel is specified in the CRO, all necessary and reasonable travel by CONTRACTOR personnel directly relating to any security vulnerability project will be approved in advance of such travel by the ISD CISO. Travel to the work site and back to home station by CONTRACTOR personnel is not reimbursable by State of Alabama.

#### **VI.7. ISD Contract:**

**VI.7.1. Contract Release Order (CRO) Project Price:** The CRO will fix the duration of the assignment and the maximum amount of money to be paid in compensation (the “CRO Project Price”) for the services requested on a particular CRO. This amount cannot be exceeded without a mutually agreed upon amendment. Such an amendment, if deemed necessary by the, would increase the maximum potential compensation due the CONTRACTOR for the work in question, and extend the CRO project end date if necessary.

**VI.7.2. Time Sheets:** Time sheets shall be filled out by CONTRACTOR Personnel, approved by the manager overseeing the project, and signed by the ISD CISO to indicate ISD’s acceptance of all work performed during the time sheet period.

**VI.8. Invoicing and Payments for Services:** The services shall be provided and invoiced at the respective hourly rate and hours worked, up to the CRO Project Price stated in the CRO. Half-hour increment is acceptable. For all services, fees, expense amounts, and reimbursements allowed through the CRO the CONTRACTOR shall prepare and submit BI-MONTHLY (or as requested by) invoices to ISD. Said invoices shall be accompanied by time sheets and such supporting documents as ISD reasonably may require. ISD will pay to the CONTRACTOR the invoice amounts on “due upon receipt basis.” Said payments shall be subject to adjustment for amounts found to have been improperly invoiced. For each CRO, ISD will track the expenditures against the CRO Project Price, and not pay CONTRACTOR invoices that exceed this dollar cap. It is ISD’s sole option to either amend the CRO Project Price to accommodate completion of any work in-progress, or to allow that CRO to expire. ISD shall not be liable to pay the CONTRACTOR for any hours worked in excess of the most current approved CRO Project Price.

**VI.9. Work Visas and Two-Week Notices:** ISD expects CONTRACTORs to select Security Specialists to be ready to begin work on the Project Begin Date stated in the CRO. Historically, activities such as securing work visas and turning in two-week notices have delayed start dates. CONTRACTORs must take these sorts of delays into account when reviewing their complement of Security Specialists that have those attributes that will enable them to begin work on the stated Project Begin Date. Availability of candidates will be one of the primary factors of selection by ISD.

**VI.10. Performance Evaluations:** CONTRACTOR’s performance in meeting the objectives stated in this ITB will be evaluated at regular intervals commensurate with the completion of stated deliverables. In addition, each individual assigned to under a CRO/SOW will, at ISD’s

discretion, be evaluated on a regular basis. The first evaluation, at ISD's option, will occur at the end of the fifth working day. If performance at that time is deemed to be unacceptable, ISD will notify the CONTRACTOR of the problems and request that the individual be terminated. ISD will not pay for the hours worked due to failure to perform. ISD will notify the CONTRACTOR as to why the performance was unacceptable in writing (a fax or e-mail, with voice confirmation, will suffice). In this event, ISD will not be liable to the CONTRACTOR for any costs or damages--including, but not limited to, hourly Payment Rate payments, travel expenses, relocation fees, etc.--related to that individual's assignment at ISD. ISD will provide such notification, or email, to the CONTRACTOR no later than the end of the fifth day of the individual's assignment.

**VI.10.1.** A second evaluation, at ISD's option, will occur at the end of one calendar month. If there are sufficient performance problems identified at this time ISD will notify the CONTRACTOR per paragraph III.10. of the problems and request that the individual be terminated. ISD will make the determination if any acceptable work was performed and pay only for the hours that acceptable work was performed. ISD shall make the determination if the work was acceptable.

**VI.10.2.** Subsequent evaluations, at ISD's option, may occur every six months.

**VI.11. Termination of Contract Personnel:** The termination of an individual will not necessarily result in the termination of the CONTRACTOR that supplied the individual to the CRO/SOW. ISD's decision will depend upon the circumstances such as whether or not the terminated individual was the only individual on the CONTRACT in question.

**VI.12. Replacement Personnel:** In the event an individual has been terminated or has voluntarily withdrawn from an assignment, ISD has several options:

**VI.12.1.** ISD can request the CONTRACTOR replace the individual with an individual of equal or greater qualifications. The pay rate shall remain the same. The first 80 hours of work performed by the new CONTRACTOR replacement will be billed at one-half the awarded hourly rate to allow the replacement employee to get up-to-speed on what the previous Security Specialist had or had not accomplished per ISDs requirements.

**VI.12.2.** If the CONTRACTOR is unable to find an acceptable replacement, ISD can void the award to the current CONTRACTOR and award to next lowest Bidder, or issue a new Invitation to Bid.

**VI.12.3.** Replacement of personnel will be at the sole discretion of ISD; ISD is not obligated to replace terminated or withdrawn individuals.

**VI.13. Additional Policies and Procedures:** ISD will, as required, promulgate additional policies and procedures, manual or electronic, to govern the work environment, work conditions and position duties, throughout the life of the CONTRACT resulting from this ITB. ISD also reserves the right to amend existing policies and procedures at any time if such is deemed to be in the best interest of the project or respective task in question.

## **SECTION VII**

### **General Statements of Work and Other Requirements**

**VII.1. Cyber Security Specialists General Requirements:** The cyber security specialists will report to the ISD Chief Information Security Officer to provide cyber security and vulnerability/risk assessment services for all aspects of information security for the State of Alabama. The goal is to provide a wide range of cyber security capabilities ranging from basic security policy development up to and including a multi-faceted automated enterprise vulnerability management capability within the State of Alabama cyber infrastructure that supports all enterprise managed information systems. This ITB includes three security objectives that will improve the ability of the State of Alabama cyber infrastructure to withstand cyber-attack:

- Harden the state’s cyber infrastructure by ensuring systems and applications are patched against known vulnerabilities that attackers are likely to exploit.
- Examine closely the state cyber risk posture and provide appropriate mitigating actions.
- Implement end devices to protect against the risk of data loss. These combined objectives will provide ISD with a sustainable vulnerability management capability to monitor and protect the State of Alabama computing environment from the threat of cyber-attack.

Vulnerability management is a process that can be implemented to make IT environments more secure. The temporary IT security specialists required by this ITB will design and implement a vulnerability management program including:

- Policy definition is the first step and includes defining the desired state for device configurations, user identity and resource access.
- Baseline the environment to identify vulnerabilities and policy compliance.
- Prioritize mitigation activities based on external threat information, internal security posture and asset classification.
- Shield the environment, prior to eliminating the vulnerability, by using desktop and network security tools.
- Mitigate the vulnerability and eliminate the root causes.
- Maintain and continually monitor the environment for deviations from policy and to identify new vulnerabilities.

#### **VII.1.1 The Cyber Security Specialists must provide the capability to:**

- **Develop and Implement an automated Enterprise Vulnerability Management Program**
  - Provide Commercial off-the-shelf (COTS) Information Assurance Vulnerability Assessment (IAVA) Patch software infrastructure in order to distribute system and application hot fixes
  - Research and review IAVA Patch Products to recommend/select best product for the State of Alabama computing environment
  - Provide the ability to “push” updates monthly via third party software and provide the support to sustain the application and monthly processes

- Establish an IAVA test lab to test updates prior to deployment in the operational environment
- Define how software upgrades and/or patches for the system applications will be provided and deployed to multiple servers, workstations, etc
- Provide Vulnerability Assessment capability, configuration management, and establish interfaces with all required hardware and software
- Establish proper architecture; test and ensure COTS IAVA Patch Products successfully perform all required functions
- Provide a complete set of supporting documentation
- **Develop and Implement Enterprise Risk Management Program**
  - Review organizational policies, standards, procedures, and critical business functions
  - Review network architecture and network operations center; focus on security, performance, functionality, and implementation of state and organizational policies, standards, and procedures
  - Deploy the tools needed to automate, expedite, and repeat as required the assessment process
  - Scan the organization’s network for vulnerabilities; identify false positives
  - Scan the organization’s network for settings of devices; policy and device enforcement
  - Scan the organization’s web services and databases
  - Identify / review the current security on the network - establish the security baseline
  - Identify / review the level of security and compliance of the web services
  - Identify / review the level of security and compliance of the databases
  - Assess all vulnerabilities identified; confirm and prioritize vulnerabilities by degree of risk
  - Assess implementation level of current state and organizational security policies and standards
  - Follow up with awareness level training to inform the IT user community of the security threats, security responsibilities (policies), and security requirements (standards)
- **Develop and Implement Enhanced Endpoint Security Control Capability**
  - Develop a data map for both data in motion and at rest; identify the end points most susceptible to data leakage
  - Design employee awareness programs to educate staff on patterns of prevention and develop security awareness – the recognition of sensitive data and its storage and handling
  - Program an automatic system shutdown or lockout after a specified time, requiring user credentials to resume operating the device
  - Encrypt sensitive data on all end-devices including full-disk, boot-level encryption
  - Enforce policy on a content-sensitive basis including logging, alerting, encrypting, and blocking the download based on keywords, file types and other criteria
  - Ensure contracts with 3rd parties that access sensitive/confidential data include: mandatory training for handling sensitive data, data encryption, and agreement to

allow physical inspections, and sanctions for loss of data in conjunction with their support of the State of Alabama.

**VII.1.2 The Cyber Security Specialists must provide the capability to achieve the following deliverables:**

**VII.1.2.1. An automated enterprise vulnerability management program including the following:**

- **Vulnerability Management**
  - Generate/maintain inventory of all assets (hardware/software) using an Information Assurance Vulnerability Assessment (IAVA) Scan Product
  - Automate scan results recorded from IAVA Scan Product Patch agents to the mid-level server(s)
  - Execute manual scans from mid-level server(s) to end user
  - Manage the flow of vulnerability information to top-level Security Management Console
  - Conduct prioritization of vulnerabilities based on risk exposure and IAVA criticality
  - Ensure scheduled reporting of vulnerability status to System Administrators
  
- **Patch Management**
  - Provide daily evaluation of assets for security patch/IAVA compliance from mid-level server(s)
  - Ensure end user update agents check daily with the mid-level server for security patches
  - Provide successful push of Microsoft and all other application vendor security patches from mid-level server to end user update agents
  - Automate weekly reporting of patch compliance from end user to the mid-level server(s)
  - Automate weekly reporting of patch compliance of all mid-level server(s) to the top-level IAVA Patch Product Security Management Console
  - Provide notification of IAVA compliance to the System Administrators
  
- **Application Software Updates**
  - Provide notification that newer software releases are available for download
  - Push application software updates from top-level server(s) to mid-level server(s)
  - Push application software updates from mid-level server to end user devices

- **Policy Compliance**
  - Check end user devices against secure baseline archived on mid-level server
  - Generate weekly reports of policy compliance
- **General Considerations**
  - Perform multiple roles on the IAVA Patch Product server to support Role Based Access Control
  - Implement Configuration Management process to ensure that only tested and approved updates are pushed to clients

**VII.1.2.2. An Enterprise Risk Management Program including the following:**

- Establish the quantifiable value and importance assigned to IT resources
- Identify vulnerabilities and potential threats to each resource identified
- Provide comprehensive view of network risk (including vulnerability, application, configuration and policy risk) enabling organizations to make better decisions about how to effectively manage and reduce it
- Implement appropriate controls for reducing or eliminating risk (risk mitigation) identified
- Ensure that highest priority risks are quickly mitigated effectively reducing overall network risk
- Verify that assessment tools locate, examine, report, and fix security flaws and misconfigurations so organizations can proactively harden their applications and improve and simplify routine audits
- Automate assessment tools to complete assessments better, faster, and at lower cost.

**VII.1.2.3. An Enhanced Endpoint Security Control Capability including the following:**

- Share/transport data using portable storage devices safely and securely
- Reduce risk of sensitive data disclosure in event of data or device loss
- Determine if unauthorized files are being copied off of State PCs, and prevent it
- Remotely overwrite file systems or destroy them altogether when someone tries to turn on a lost or stolen device
- Ensure that data management practices adapt to changing information environment

**VII.2. General Security Levels & Qualifications:** The CRO's of Information Services Division may have additional requirements such as criminal background checks, and drug screenings as is the case. Technical knowledge required for these positions will vary depending on the security project. The qualifications shown are the minimum acceptable, individual SOW may place higher and/or more specific requirements:

**–Program Manager – ISD-09-001**

Masters Degree (preferred) or Bachelor's Degree in Information Systems or a closely related field. This must include a minimum of at least 5 years experience as a manager/project manager performing responsible work in IT security systems. Requires a detailed understanding of NIST Special Publication 800-series documents and State of Alabama information security policies, standards, plans, and procedures.

Project Management Institute (PMI) Certified Project Management Professional (PMP) Certified Information Systems Security Professional (CISSP).

**–Project Manager – ISD-09-002**

Masters Degree (preferred) or Bachelor's Degree in Information Systems or a closely related field. This must include a minimum of at least 3 years experience as a manager/project manager performing responsible work in IT security systems including experience in configuration and change management. Requires a detailed understanding of NIST Special Publication 800-series documents and State of Alabama information security policies, standards, plans, and procedures. Must have a strong understanding of the State of Alabama cyber infrastructure. Project Management Institute (PMI) Certified Project Management Professional (PMP). Certified Information Systems Security Professional (CISSP).

**–Sr. Systems Analyst – ISD-09-003**

Masters Degree (preferred) or Bachelor's Degree in Information Systems or a closely related field. This must include a minimum of at least 5 years responsible work in IT security systems. Requires a detailed understanding of NIST Special Publication 800-series documents and State of Alabama information security policies, standards, plans, and procedures. Project Management Institute (PMI) Certified Project Management Professional (PMP). Certified Information Systems Security Professional (CISSP). Cisco Certified Design Associate (CCDA) and/or Cisco Certified Network Associate (CCNA). Cisco Field Engineer Wireless Specialist and/or Cisco System Engineer Wireless Specialist. Must possess an excellent understanding of Cisco and Nortel Networks; Adtran, Allied Telesyn, and Cabletron equipment; TCP/IP, Novell, XNS, Ethernet, Token Ring, and FDDI; PPP, MPLS, Frame Relay, and ISDN WAN; CLIX, UNIX, and Windows operating systems. Prefer experience with IA scan tools such as eEye Retina, HP Webinspect, or AppDetective.

**–Systems Analyst - ISD-09-004**

Masters Degree (preferred) or Bachelor's Degree in Information Systems or a closely related field. This must include a minimum of at least 3 years responsible work in IT security systems. Requires a detailed understanding of NIST Special Publication 800-series documents and State of Alabama information security policies, standards, plans, and procedures. Certified Information Systems Security Professional (CISSP). Certified Information Systems Auditor (CISA). Must possess an excellent understanding of network infrastructures, information assurance, vulnerability management, and risk assessment/analysis.

**–Sr. Systems Engineer - ISD-09-005**

Masters Degree (preferred) or Bachelor's Degree in Information Systems or a closely related field. This must include a minimum of at least 3 years responsible work in IT security systems with 3 years responsible work in IT security systems. Requires a detailed understanding of NIST Special Publication 800-series documents and State of Alabama information security policies, standards, plans, and procedures. Microsoft Certified Professional (MCP), Certified Information Systems Security

Professional (CISSP) or Microsoft Certified Systems Engineer (MCSE). Requires strong background in Active Directory (AD), Windows server, Windows XP, Exchange Server, and firewall software; should include advanced knowledge of TCP/IP, DHCP, WINS, DNS, IIS, NT Cluster and Load Balancing, CITRIX MetaFrame and Terminal Server, Packeteer PacketShaper, network monitoring, and System Management Server. Must possess an excellent understanding of network infrastructures including routing and switching equipment, firewalls, DNS servers, web servers, web filtering and caching servers, file servers, VPN server, and backup servers, and control panel based web and email hosting servers.

**–Technical Writer - ISD-09-006**

Bachelor's Degree (preferred) in Communication, Information Systems or a closely related field. This must include a minimum of at least two college level courses in Information Systems. Minimum of 2 years responsible experience working with texts of a technical nature and with revisions so that they would be understood by a general audience. If the person(s) being proposed have any professional certifications for IT related fields such as Certified Information Systems Security Professional (CISSP) please provide this information.

# ATTACHMENT - A

## Candidate Data Sheet GUIDE

ISD Information Technology Professional Services

**Privacy** – all information provided in the Candidate Data Sheet (CDS) will be used for candidate evaluation and selection for the specific Statement of Work to which the candidate is responding **only**. The information will not be disclosed for any other purpose.

**SOW #** - the number corresponding to the Statement of Work to which the candidate is responding. This will be in the form: ABC-yr-nnnn. ABC is a three character representation of the hiring agency. Yr is a 2-digit representation of the fiscal year under which the work is expected to begin. Nnn is a unique number assigned by the hiring agency.

**Job Classification#** - the number of the Job Classification that corresponds to the SOW to which the candidate is responding

**Title**—the title of the Job Classification that corresponds to the SOW to which the candidate is responding

**Contract Rate(s)**—the amount per hour to be charged to ISD for this candidate if hired, for each fiscal year (October 1 – September 30) in which work will be performed under the specified work order. If the work order ends prior to a fiscal year, mark N/A.

**Candidate’s status**—if the candidate is an official employee of the firm (i.e., receives fringe benefits and a W-2 tax form), mark “Employee.” If the candidate is an independent contractor of the firm (i.e., receives no fringe benefits and submits a 1099 tax form), mark “Self-Employed (1099)”

**Subcontracting Vendor Name (if applicable)**—the name of the subcontractor for which the candidate works. If the candidate works directly for the primary vendor, mark N/A

**Governmental Reporting Section**—this information is requested for the purpose of vendor diversity score carding.

### EDUCATION Section

- Please mark the highest level of education completed. If the candidate is currently enrolled in a degree program, that degree does not constitute a “level completed.”
- Placing the most recently attended institution first, list all secondary and post-secondary educational institutions attended. Do not include transcripts.

**PROFESSIONAL LICENSE/CERTIFICATE Section** - List any professional licenses or certifications in the fields associated with the SOW. You may attach additional forms as required.

**SPECIALIZED QUALIFICATIONS SECTION**

- **SOW Specialized Skill Requirement**—list each Specialized Skill Requirement listed on the corresponding Statement of Work. Include only those specialized skill requirements listed on the SOW to which the candidate is responding.
- **Total Yrs. Exp.**—list the total number of full time equivalent years the candidate has experience with the corresponding Specialized Skill
- **Most Recent Yr (YY)**—list the most recent year in which the candidate has used the corresponding Specialized Skill
- **Related Work Exp. Entry(s)**—list the corresponding Work Experience number where the candidate gained this experience. For example, if the candidate gained this experience from a position listed in slots 1 and 2 in the **WORK EXPERIENCE** section, then the candidate would enter 1,2 in the space provided

**WORK EXPERIENCE Section**

- **Salary/Hourly Rate**—this information is optional
- **Describe your duties and responsibilities as they relate to the Statement of Work**—describe only those job responsibilities that apply directly to the corresponding Statement of Work. Job duties listed that are outside the scope of the SOW **will not** be considered

**REFERENCES Section**

- Include only professional references. **Do not list personal references**
- **List only three references**

**APPLICANT and CONTRACTING FIRM CERTIFICATION Section**

**Read this section carefully. By submitting the Candidate Data Sheet, the candidate AND the firm bidding agree to the terms and conditions outlined in this section**

STATE OF ALABAMA
ISD INFORMATION TECHNOLOGY PROFESSIONAL SERVICES
CANDIDATE DATA SHEET

This form must be used to respond to a State of Alabama Statement of Work.
Résumés submitted in other formats may be rejected without qualification review.

SOW # \_\_\_\_\_ Job Classification: # \_\_\_\_\_ Title \_\_\_\_\_

Prime Vendor \_\_\_\_\_ Contract Hourly Rate: \$ \_\_\_\_\_ .00

Candidate's status (1099) [ ] Employee [ ] Self Employed Subcontracting Vendor Name (if applicable) [ ] N/A or \_\_\_\_\_

Full Name Last First MI \_\_\_\_\_

Address \_\_\_\_\_ City \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_

Daytime Phone ( ) - Evening Phone ( ) - Email Address \_\_\_\_\_

[ ] U.S. Citizen [ ] Non-U.S. Citizen Visa Status

I have been involuntarily terminated, discharged, forced or asked to resign from any job. If yes, expand the space below and provide an explanation. Note any mitigating or extenuating circumstances. [ ] Yes [ ] No

I have been convicted of a misdemeanor or felony crime. If yes, expand the space below and provide an explanation. Note any mitigating or extenuating circumstances. [ ] Yes [ ] No

The following information is requested for governmental reporting:
Date of Birth - \_\_\_/\_\_\_/\_\_\_ (Day) (Month) (Year)
Gender (check one) [ ] Male [ ] Female
Race (Check all that apply) [ ] White, Non-Hispanic [ ] Asian [ ] Black [ ] Pacific Islander [ ] Hispanic [ ] Other [ ] Native American or Alaskan Native

\_\_\_\_\_ ISD APPROVAL

**EDUCATION**

<i>Mark highest completed.</i>	Some HS <input type="checkbox"/>	HS/GED <input type="checkbox"/>	Associate <input type="checkbox"/>	Bachelor <input type="checkbox"/>	Master <input type="checkbox"/>	Doctoral <input type="checkbox"/>
--------------------------------	----------------------------------	---------------------------------	------------------------------------	-----------------------------------	---------------------------------	-----------------------------------

List most recent first, all secondary and post-secondary education (high school, GED, colleges, and universities) attended. Do not include copies of transcripts unless requested.

School Name	Address	Major	Degree Earned (Y/N)	Year Received	Total Credits Earned

**PROFESSIONAL LICENSE OR CERTIFICATE**

License/Certificate Name	Issued By	License/Certificate No.	Issue Date mm/dd/yyyy	Expiration Date
			/   /	/   /
			/   /	/   /

**SPECIALIZED QUALIFICATIONS**

For each specialized skill or knowledge requirement specific to the SOW, give the total number of years of experience and the Work Experience entry number(s)—(1, 2, etc.) providing the required skill or knowledge. Do not list any skill not specified in the SOW to which you are responding.

SOW Specialized Skill Requirement					
	Total Years Exp.		Most Recent Yr (YY)		Related Work Exp. Entry(ies)
	Total Years Exp.		Most Recent Yr (YY)		Related Work Exp. Entry(ies)
	Total Years Exp.		Most Recent Yr (YY)		Related Work Exp. Entry(ies)
	Total Years Exp.		Most Recent Yr (YY)		Related Work Exp. Entry(ies)
	Total Years Exp.		Most Recent Yr (YY)		Related Work Exp. Entry(ies)
	Total Years Exp.		Most Recent Yr (YY)		Related Work Exp. Entry(ies)
	Total Years Exp.		Most Recent Yr (YY)		Related Work Exp. Entry(ies)
	Total Years Exp.		Most Recent Yr (YY)		Related Work Exp. Entry(ies)
	Total Years Exp.		Most Recent Yr (YY)		Related Work Exp. Entry(ies)

**WORK EXPERIENCE**

To add work experience, place the insertion point directly below the last row and click the “Add Work Experience” button on the toolbar to the top right. Your Word “Security Setting” must be set to “Medium” in order to add additional information.

Describe your work experience related specifically to the Statement of Work to which you are responding. <b>Do not attach job descriptions.</b> Please list most recent job first				
<b>Work Experience 1</b>				
<i>Job Title</i> _____				
FROM (mm/yy) /	TO (mm/yy) /	Reason for Leaving	Salary/Hourly Rate \$ (optional)	Hours per Wk
Company Name		Supervisor’s Name		Supervisor’s Phone No. ( ) - Ext.
Company Address Address Line 1 Address Line 2			Supervisor’s Email Address	
Describe your duties and responsibilities as they relate to the Statement of Work.				

<b>Work Experience 2</b>				
<i>Job Title</i> _____				
FROM (mm/yy) /	TO (mm/yy) /	Reason for Leaving	Salary/Hourly Rate \$ (optional)	Hours per week
Company Name		Supervisor’s Name		Supervisor’s Phone No. ( ) - Ext.
Company Address Address Line 1 Address Line 2			Supervisor’s Email Address	

Describe your duties and responsibilities as they relate to the Statement of Work.

References (list 3)

1) Name	Title	Organization
Address	Phone ( ) - Ext.	Email Address
2) Name	Title	Organization
Address	Phone ( ) - Ext.	Email Address
3) Name	Title	Organization
Address	Phone ( ) - Ext.	Email Address

**APPLICANT and BIDDING FIRM CERTIFICATION**

By submitting this data sheet to the State of Alabama, the applicant AND contractor firm **certify** that, to the best of their knowledge and belief, all of the information on and attached to this application is true, correct, complete, and made in good faith. The candidate further authorizes the release of all relevant prior employment, military service, academic/school, and criminal records. False or fraudulent information on or attached to this application may be grounds for not hiring a candidate or firing a candidate once work has begun and may be punishable by fine or imprisonment. Any information provided to the State of Alabama may be investigated.

Candidate(signature)\_\_\_\_\_ Contractor Firm(signature)\_\_\_\_\_

Name \_\_\_\_\_ Contractor Firm Name \_\_\_\_\_

## **ATTACHMENT – B**

### **Alabama Computer Access Security, Privacy, and Code of Conduct agreements**

#### **1. 9.17 ALABAMA COMPUTER ACCESS SECURITY, PRIVACY, AND CODE OF CONDUCT**

Completion of the Computer Access Security Agreement and Code of Ethics Forms, immediately following this page, will be mandatory for each vendor candidate completing work for the state under the contract resulting from this ITB. Submission of a proposal in response to this ITB indicates agreement with these terms.

**ALABAMA COMPUTER CRIME ACT AWARENESS  
VERIFICATION FORM**

I, \_\_\_\_\_ have read, or had read to me the Alabama Computer Crime Act and hereby acknowledge that I understand my rights and responsibilities regarding intellectual property, that is computer software, hardware, and computer information. I agree to conduct myself accordingly in adhering to the Alabama Computer Crime Act, departmental policy and relevant law.

Signed \_\_\_\_\_ Date \_\_\_\_\_

Witnessed by \_\_\_\_\_ Date \_\_\_\_\_

State of Alabama, Department of Finance, Information Services Division

**CONFIDENTIALITY AND COMPLIANCE COMMITMENT**

**I understand that:**

There may be State, local, federal, department, , board, commission, Division or other applicable confidentiality requirements in regard to data, algorithms, policies, procedures or other issues that I may be privileged to as a result of my association with the Information Services Division.

The permissions, profiles, privileges, accesses and other entrustments granted to me as a result of my association with the Information Services Division are to accomplish my assigned responsibilities and authority.

I may be required to execute additional confidentiality and compliance agreements unique to other State or related entities if assigned responsibilities associated with the information services support of such entities.

Accordingly, I **agree** to:

Ascertain applicable confidentiality requirements before revealing any material.

Comply with applicable confidentiality requirements.

I acknowledge these understandings and agreements by my signature below.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Witness: \_\_\_\_\_

Date: \_\_\_\_\_