

Memorandum

To: State Agency IT Directors and Purchasing Agents

From: Craig P. Orgeron, Ph.D

Date: May 16, 2012 (*date extension*)
January 11, 2011 (*revised evaluation methodology, date extension and new letterhead*)
October 29, 2010 (*updated Vendor contact information and list in Item 7.*)
June 2, 2010 (*updated to include ARRA contract information*)
March 2, 2010 (*original date of publication*)

Re: Security and Risk Assessment Services RFP No. 3606 Instructions for Use

CC: ITS Project File Number 38421

1. Scope

RFP No. 3606 was created to establish a vendor pool for the acquisition of security risk and assessment services for the wide area, local area and other network based systems used by the agencies and institutions of the State of Mississippi. The Vendors on this list were qualified by the Mississippi Department of Information Technology Services based upon their proposal responses to Request for Proposal (RFP) No. 3606 to provide the necessary services.

This procurement does not include the remediation work required to satisfy/resolve any findings. If remediation services are required, procurement of those services should follow state law and established policy for procurement of IT services. Remediation services may be purchased using the EPL resulting from Security Consulting Services RFP No. 3610. This EPL is available on the ITS Web Site (www.its.ms.gov).

If security-related hardware and software products are required for remediation, procurement of those products should follow state law and established policy for procurement of IT products. Security hardware and software products may be purchased using the EPL resulting from Security Hardware and Software RFP No. 3612. This EPL is available on the ITS Web Site (www.its.ms.gov). For more information on using either the Security Consulting Services EPL or the Security Hardware and Software EPL, refer to the ITS Web Site or call the ITS Procurement Help Desk at (601) 432-8166.

The ITS Information Security Division has created and maintains the State's Enterprise Security Policy and Enterprise Security Plan. Both of these documents can be found at http://www.its.ms.gov/services_security.shtml (ACE Login Required).

2. **Who May Use**

This list of Vendors may be used by Mississippi agencies and institutions required to perform security risk assessments. This is a multi-vendor award that meets all Mississippi requirements for legal purchases.

State agencies are required by ITS to perform a security risk assessment every three years (see item 4.1.9 of the Enterprise Security Policy - PSG 100-09). For more details, please visit ITS' Information Security Division webpage (http://www.its.ms.gov/services_security.shtml) or contact Jay White, ITS Information Security Division, (601) 432-8180, Jay.White@its.ms.gov. State agencies are not required to use the Vendors on this list to perform the assessment. Agencies desiring to procure security risk assessment services from Vendors other than those on this list should follow state law and established policy for procurement of IT services.

3. **Dollar Limitations of Use**

There are no maximum dollar limitations for agencies and institutions using this list of Vendors.

4. **Effective Dates**

The list of approved Vendors for RFP No. 3606 is valid through February 23, 2014, or until revised or replaced.

5. **Using RFP No. 3606 for Security Risk Assessment Services**

ITS has already evaluated the Vendors using both cost and non-cost factors, including technical requirements and vendor qualifications, and selected a small award of five security risk assessment services Vendors.

Each State agency or institution must work with two or more of the awarded Vendors from RFP No. 3606 to formulate the scope of the security assessment engagement and its fixed cost. The agency or institution will be required to obtain Statements of Work (SOW) from at least two awarded Vendors, send a procurement request to ITS with the Statements of Work, and receive a CP-1 approval document before beginning the security risk assessment. Agencies or institutions must select the lowest and best Vendor based on the Statements of Work received. The selection must follow the scoring methodology outlined below.

Although cost in most cases will be the main consideration, there may be other factors to consider and that deserve merit. If non-cost factors are used in the evaluation of the SOWs,

the Request for SOWs must include specifications for those factors. The customer must document each vendor's score for each of the evaluative factors as part of customer's purchase file and include this information in the packet submitted to ITS.

- History with Vendor – Agencies may prefer to work with a Vendor who has performed previous security risk assessments on their networks. The previous knowledge of the agency's network will reduce the learning curve that would exist with a Vendor who has never performed an assessment on the network. Alternatively, agencies may prefer to work with a Vendor who has no previous assessment experience with their networks to involve multiple perspectives in accessing security risks. **Regardless, Vendors who have previously performed installation, maintenance, and/or support services are precluded from providing security risk assessment services for that agency.**
- Quality and Responsiveness of the Statement of Work - Customers should always give the Vendor a reasonable response time of at least 1 week to provide a Statement of Work. The Statements of Work should reflect an understanding of the project and a clear explanation of the services to be provided.
- Functional/Technical Requirements – Rather than simply providing a list of devices to be scanned and/or quantities of other tasks to be performed, customers may wish to outline specific assessment requirements and require vendors to respond to those requirements in the SOW.

For assistance with SOWs, please contact Jay White, ITS Information Security Division, (601) 432-8180, Jay.White@its.ms.gov.

ITS requires that cost be 90 to 100% of the score. No more than 10 points may be awarded for non-cost points.

When cost is less than 100% of the score, customers must compute the cost score as a ratio of the difference between a given proposal's cost and the cost of the lowest valid proposal. The following cost scoring formula should be used for every cost evaluation:

Points awarded for cost = $(1 - [(B-A)/A]) * n$

Where:

A = Total lifecycle cost of lowest valid SOW

B = Total lifecycle cost of SOW being scored

n = number of points allocated to cost for this procurement

In simpler terms, lowest price gets a perfect cost score. A SOW that is 20% more expensive than the lowest priced SOW gets 20% fewer cost points.

Scoring Matrix Example

Scoring Factor	Max Points	Low Cost	Vendor 1	Vendor 2
Cost of Security Risk Assessment	n= 90	\$1,470,888 "A"	\$1,470,888 "B"	\$1,472,841 "B"
"the math"			$(1 - [(1,470,888 - 1,470,888) / 1,470,888]) * 90$	$(1 - [(1,472,841 - 1,470,888) / 1,470,888]) * 90$
Points for Cost	90		90.00	89.88
Non-Cost Factors				
History with Vendor	2	NA	0	2
Quality and Responsiveness of the Statement of Work	3	NA	2	3
Functional/ Technical Requirements	5	NA	4	3
Total Score	100		96	97.88

In this scenario, Vendor 1 would have been awarded if cost had been 100% of the evaluation. When considering other evaluation factors, Vendor 2 would have been awarded.

Note that it is VERY important for the customer in their solicitation of SOWs and quotations to inform the responding Vendors as to whether cost is to be 100% of the score. If not 100%, customer should state the other evaluative factors that will be considered in the quote request to the Vendors, including detailed specifications for the Vendors to respond to and for the customer to evaluate.

Variations on the above example might include:

- Cost is between 90 and 100 points, for instance, 97 points, and only 3 points are awarded for some or all of the additional factors. For this example, the customer would let "n=97" in the table above.
- In the example in the table, the ten non-cost points could split between "Quality and Responsiveness of SOW" and "Functional/Technical Requirements." Cost would be 90 points (n=90), Quality and Responsiveness of SOW = 5, and Functional/ Technical Requirements = 5 (or other allocation of the 10 points between these two selected factors).

6. **Budgeting and Planning for RFP No. 3606 Purchases**

ITS performed a cost evaluation for the Vendors awarded under RFP No. 3606. In order to help agencies and institutions budget for the cost of a security risk assessment, the following information is provided based on the Vendors' responses to RFP No. 3606.

SMALL AGENCY MODEL		
	Element Description	Qty
1.	Windows External Server Vulnerability Scan	5
2.	Windows Internal Server Vulnerability Scan	10
3.	Workstation Internal Vulnerability Scan	4
4.	Firewall Vulnerability Scan	1
5.	External Router Analysis	1
6.	Switch Analysis	1
7.	VPN Assessment	1
8.	Penetration Services	20 hours
9.	Additional Security Consulting Services	8 hours
10.	Security Policy Review	1
11.	Assessment Report	1
Range in Cost for Small Agency Model = \$7,807.50 - \$13,540.00		

MEDIUM AGENCY MODEL		
	Element Description	Qty
1.	Windows External Server Vulnerability Scan	10
2.	Windows Internal Server Vulnerability Scan	25
3.	Workstation Internal Vulnerability Scan	300
4.	Firewall Vulnerability Scan	1
5.	Firewall Analysis/Review	1
6.	External Router Analysis	1
7.	Switch Analysis	5
8.	Wireless Access Point Analysis	1
9.	VPN Assessment	1
10.	Penetration Services	40 hours
11.	Additional Security Consulting Services	16 hours
12.	Security Policy Review	1
13.	Assessment Report	1
Range in Cost for Medium Agency Model = \$17,320.25 - \$29,060.00		

LARGE AGENCY MODEL		
	Element Description	Qty
1.	Windows External Server Vulnerability Scan	30
2.	Windows Internal Server Vulnerability Scan	60
3.	Workstation Internal Vulnerability Scan	1,000
4.	Firewall Vulnerability Scan	1
5.	Firewall Analysis	1
6.	External Router Analysis	1
7.	Switch Analysis	20
8.	Wireless Access Point Analysis	1
9.	VPN Assessment	1
10.	Penetration Services	80 hours
11.	Additional Security Consulting Services	40 hours
12.	Security Policy Review	1
13.	Assessment Report	1
Range in Cost for Large Agency Model = \$33,604.00 - \$67,550.00		

ITS will verify that the costs in the Statements of Work are at or below the costs proposed by the Vendors in response to RFP No. 3606.

Note that the security risk assessment rates provided by the Vendors are fully loaded. Travel or per diem line items will not be accepted.

7. What Goes in Your Purchase/Audit File for Submission to ITS

At a minimum include:

- i. A copy of this Instructions for Use memo (for your files only).
- ii. A copy of the document sent to Vendors to request the Statements of Work/quotes.
- iii. Copies of the Vendors' Statements of Work/quotes.
- iv. A copy of the evaluation methodology and Vendors' scores.
- v. A copy of the CP-1 approval document (received from ITS).
- vi. A copy of the purchase order (for your files only).
- vii. Any additional project-related documentation or justification.
- viii. Signed Confidentiality Agreement (for your files only). [See Item 11 below.]

8. **RFP No. 3606 Vendor Information**

See the attached Vendor Information for the list of Vendors approved under RFP No. 3606 and each Vendor's contact information. Please contact the Vendors directly to discuss any questions regarding their services or pricing, and to request Statements of Work.

9. **Contract**

ITS has executed a Master Security and Risk Assessment Services Agreement with each awarded Vendor, and purchases made from this RFP will use those Terms and Conditions. If you would like a copy of a Vendor's executed agreement, please contact the ITS Procurement Help Desk at (601) 432-8166.

10. **American Recovery and Reinvestment Act (ARRA) of 2009**

While ARRA requirements are still evolving and some current EPLs were established prior to the establishment of federal rules concerning the use of ARRA funds, to the best of our knowledge and current assessment, ITS believes the EPLs are valid purchase instrument for the use of ARRA funds.

The Master Security and Risk Assessment Services Agreements executed with each valid Vendor for this RFP include ARRA-related terms and conditions. These terms and conditions have been created in conjunction with the Mississippi Office of the State Auditor and the Mississippi Department of Finance and Administration.

ITS recommends that customers using these instruments for purchases using ARRA funds obtain written quotations from multiple Vendors approved under RFP No. 3606, that the request for quotations state that ARRA funds will be used for the purchase, and that all quotations be maintained in the purchase file.

11. **Confidentiality Agreements**

Before beginning a security risk assessment, the Vendor and agency must sign a Confidentiality Agreement. A sample Confidentiality Agreement is attached to these instructions.

12. **Object Codes**

ITS, in conjunction with the Office of the State Auditor and the Department of Finance and Administration, requests that all Customers carefully code purchases with the correct Minor Object Codes. State agencies that utilize the Statewide Automated Accounting System (SAAS) should use the following object codes on purchase order documents for purchases from this list:

Object Code:	Category:	Use For:
61902	IS Professional Fees – Outside Vendor	Payments to an outside vendor for IT consulting and personnel services such as consulting studies, project management, staff management, IT staff augmentation; analysis, design, and development of software; installation of hardware or cabling. (Including Telecommunication)

13. **To Report a Problem or Request Assistance**

If you have questions about using the list or if you have any problems with the delivery of services, please contact Jay White of ITS at (601) 432-8180, the ITS Procurement Help Desk at (601) 432-8166, or contact the Vendor directly from the contact information provided.

14. **Copies of this document are available on the Internet at**

http://www.its.ms.gov/services_security.shtml

Attachments: RFP No. 3606 Vendor Information
Confidentiality Agreement

RFP No. 3606 Vendor Information

Business Communications, Inc.			
Contact Name:	Blake Webber	Phone Number:	(601) 914-2461
E-mail Address:	government@bcianswers.com bwebber@bcianswers.com	Fax Number:	(601) 427-4561
Place Order To: 442 Highland Colony Parkway Ridgeland, MS 39157		Remit Payment To: P.O. Box 11407 Birmingham, AL 35246-1261	

Integrated Computer Solutions, Inc.			
Contact Name:	Kyle Glave	Phone Number:	(770) 206-5262 or (404) 229-4524
E-mail Address:	kyle.glave@icsinc.com	Fax Number:	(334) 270-2896
Place Order To: 60 Commerce Street, Suite 1100 Montgomery, AL 36104-3530		Remit Payment To: Attention: Accounts Payable P.O. Box 241527 Montgomery, AL 36124-1527	

Next Step Innovation			
Contact Name:	Trent Townsend	Phone Number:	(601) 957-7588
E-mail Address:	trent_townsend@nextstepinnovation.com	Fax Number:	(866) 412-4090
Place Order To: C/o Trent Townsend 3040 Indiana Avenue Vicksburg, MS 39180		Remit Payment To: 3040 Indiana Avenue Vicksburg, MS 39180	

Pileum Corporation			
Contact Name:	Elizabeth Frazier	Phone Number:	(601) 863-0275
E-mail Address:	elizabethfrazier@pileum.com	Fax Number:	(601) 352-2191
Place Order To: 190 East Capitol Street Suite 175 Jackson, MS 39206		Remit Payment To: 190 East Capitol Street Suite 175 Jackson, MS 39206	

Software Engineering Services			
Contact Name:	Doug Ashbaugh	Phone Number:	(515) 226-9295
E-mail Address:	dashbaugh@sessolutions.com	Fax Number:	(515) 226-9292
Place Order To: 1200 Valley West Drive Suite 204 West Des Moines, Iowa 50315		Remit Payment To: 1311 Fort Crook Road South Suite 100 Bellevue, Nebraska 68005	

CONFIDENTIALITY AGREEMENT

This Confidentiality Agreement (hereinafter referred to as “Agreement”) is entered into by and between **INSERT NAME OF VENDOR** a **INSERT STATE OF INCORPORATION** corporation (hereinafter referred to as “Contractor”) having an office at **INSERT STREET ADDRESS FOR VENDOR**, and **{INSERT NAME OF CUSTOMER AGENCY}**, having its principal place of business at **{INSERT STREET ADDRESS FOR CUSTOMER AGENCY}** (hereinafter referred to as “Customer Agency”). Contractor and the Customer Agency are collectively referred to herein as “the Parties”.

WHEREAS, confidential information (hereinafter referred to as “Information” and “Confidential Information”) may be used for evaluating transactions between the Parties; and

WHEREAS, the Parties desire to protect any such confidential information, and each of us agrees that the following terms apply when one of us (Discloser) discloses Information to the other (Recipient);

NOW THEREFORE, in consideration of the mutual understandings, promises and agreements set forth, the parties hereto agree as follows:

ARTICLE 1 DISCLOSURE OF INFORMATION

Information will be disclosed either:

- 1) in writing;
- 2) by delivery of items;
- 3) by initiation of access to Information, such as may be in a data base; or
- 4) by oral or visual presentation.

Information should be marked with a restrictive legend of the Discloser. Excluding Information obtained via electronic access, if Information is not marked with such legend or is disclosed orally, the Information will be identified as confidential at the time of disclosure.

ARTICLE 2 USES AND OWNERSHIP OF CONFIDENTIAL INFORMATION

Confidential Information will be used for evaluating transactions between the Parties and/or their employees. Until the Parties have completed all such transactions pursuant to definitive agreements, or unless one of the Parties obtains prior written authorization from the other, such Confidential Information will be kept strictly confidential by the Parties and their respective employees. Duplication, distribution or disclosure of any Confidential Information to any persons other than the Parties’ employees who (a) are actively and directly participating in the evaluation of the transaction or (b) those who otherwise need to know such information for the

purpose of evaluating each transaction, and who agree to keep such information confidential and be bound by this Agreement as if they were signatories is strictly prohibited. Before disclosure to any of the above mentioned employees, the Recipient will have a written agreement with the party sufficient to require that party to treat Information in accordance with this Agreement. Both Parties agree to the determination of the other regarding the classification of Confidential Information and to take appropriate steps to safeguard it from disclosure. Each of the Parties is liable for any breach by it or its employees. Modification, alteration, breakdown, disassembly or reverse engineering of any Confidential Information is prohibited without prior written consent. Confidential Information is the property of the original disseminator. Derivatives and improvements are property of the disseminator of the Confidential Information from which the derivative improvement arises.

ARTICLE 3 CONFIDENTIALITY PERIOD

The Parties understand and agree that their obligations under this Confidentiality Agreement shall continue in effect in perpetuity or until such time as the Information becomes general public knowledge through no fault of their own.

ARTICLE 4 EXCEPTIONS TO CONFIDENTIAL INFORMATION

Confidential Information does not include information that is: (a) already in the Recipient's possession without obligation of confidentiality; (b) developed independently, or (c) publicly available when received, or subsequently becomes publicly available through no fault of the Recipient.

ARTICLE 5 REQUEST FOR DISCLOSURE OF INFORMATION

If either of the Parties is requested or required (by oral questions, interrogatories, requests for information or documents, subpoena, civil investigative demand, other process, or an order issued by a court or by a local, state or federal regulatory or administrative body) to disclose Confidential Information, each agrees to immediately notify the other of the existence, terms and circumstances surrounding such request or order; consult with the other on the advisability of the owner of the Confidential Information taking steps to resist or narrow such request or order, and refrain from opposing any action by the owner of the Confidential Information to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded the Confidential Information.

ARTICLE 6 RETURN/DESTRUCTION OF CONFIDENTIAL INFORMATION

If either party determines that it does not wish to proceed with any transaction, that party will promptly advise the other. If all transactions contemplated by the Parties are not consummated, or at any time and upon request, the Parties will promptly deliver to each other all of the Confidential Information in any form whatsoever and destroy all copies, reproductions, summaries, analyses or extracts thereof based thereon in the Parties' possession or in the possession of any of their employees. Upon the request, such destruction will be certified in writing under penalty of perjury by an authorized employee who supervised the destruction thereof. Notwithstanding the return or destruction of the Confidential Information, the Parties and their employees shall continue to be bound by the obligations hereunder. The Parties agree to limit and control the copies, extracts or reproductions made of the Confidential Information and to keep a record of the Confidential Information furnished to them and the location of such

Confidential Information. The Parties will also maintain a list to whom Confidential Information has been disclosed and shall deliver to the other, upon written request, a copy of such list, specifying the Confidential Information disclosed or provided and the date on which such Confidential Information was first disclosed.

ARTICLE 7 GOVERNING LAW

This Agreement shall be construed and governed in accordance with the laws of the State of Mississippi and venue for the resolution of any dispute shall be Jackson, Hinds County, Mississippi.

For the faithful performance of the terms of this Agreement, the parties hereto have caused this Agreement to be executed by their undersigned authorized representatives.

INSERT NAME OF CUSTOMER AGENCY

INSERT NAME OF CONTRACTOR

By: _____
Authorized Signature

By: _____
Authorized Signature

Printed Name: _____

Printed Name: _____

Title: _____

Title: _____