cutting through complexity

Commonwealth of Pennsylvania

Consulting Services for an Enterprise Security Assessment

IT ITQ #4400004480

Solicitation Number: 3192013001

PROPOSAL COVER SHEET

COMMONWEALTH OF PENNSYLVANIA

Office of Administration/Enterprise Information Security Office

RFQ# 3192013001

Enclosed in three separately sealed submittals is the proposal of the Contractor identified below for the above-referenced RFQ:

Contractor Information	
Contractor Name	**KPMG LLP**
Contractor Mailing Address	30 North Third Street, Suite 1000 Harrisburg, PA 17101
Contractor Website	www.us.kpmg.com
Contractor Contact Person	Thomas Skoog
Contact Person’s Phone Number	[redacted]
Contact Person’s Facsimile Number	614-886-9279
Contact Person’s Email Address	[redacted]
Contractor Federal ID Number	[redacted]
Submittals Enclosed and Separately Sealed	
☒	Technical Submittal
☐	Disadvantaged Business Submittal
☒	Cost Submittal
Signature	
[redacted]	
Signature of an official authorized to bind the Contractor to the provisions contained in the Contractor’s proposal:	
Printed Name	Thomas Skoog
Title	Principal

KPMG LLP
Suite 1000
30 North Third Street
PO Box 1190
Harrisburg, PA 17108-1190

Telephone [redacted]
Fax +1 717 233 1101
Internet www.us.kpmg.com

April 10, 2013

Dan Paese
Enterprise Information Security Office
Commonwealth of Pennsylvania Office of Information Technology
1 Technology Park
Harrisburg, PA 17110

Dear Mr. Paese,

On behalf of KPMG LLP (KPMG or firm), I am pleased to submit our response to the Commonwealth of Pennsylvania Office of Administration / Office of Information Technology ("OA/OIT") Request for Proposals (RFP) dated March 19, 2013. KPMG has assembled an exceptional team of technical information security professionals to provide assistance with the enterprise security assessment. Our objective in undertaking this engagement is to help you understand any gaps within key areas of your network perimeter by conducting an enhanced approach to network intrusion and penetration testing, in which greater awareness is gained over the adequacy of security controls in place to defend the perimeter.

To achieve this objective KPMG will bring to you:

- **An exceptionally qualified team** – Aaron Hipp, who will serve as your engagement manager, leads KPMG's Technical Security Services Center of Enablement and has extensive experience in delivering technical security assessments within a number of organizations. Bill Varhol, identified to serve as the subject matter professional, will ensure that your requirements are addressed through execution. Our team's experience will translate directly into benefits for the OA/OIT.
- **A fresh perspective** – In addition to our data-centric, risk-based approach, the OA/OIT will benefit from a new set of eyes that KPMG's professionals will bring. We offer you objective insight to business operations, risk management, and optimization without any preconceived impressions.
- **Cyber security innovation** – There is a strong linkage between preventative measures within enterprise security as well as detective measures, including logging, incident response, and investigation. KPMG's recommendations will assist you in understanding the impact of findings identified and provide actionable recommendations in suitable timeframes agreed by the OA/OIT.

In closing, our team is excited to continue our relationship with the OA/OIT. We believe you will see the value in our proposal and select us to assist you with this important engagement.

Should you have any questions, please do not hesitate to contact me at [redacted] or [redacted]

Sincerely,

KPMG LLP

[redacted]

Tom Skoog
Principal

Contents

This proposal includes data that shall not be disclosed outside of the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this proposal or quotation. If, however, a contract is awarded to this offeror or quoter as a result of—or in connection with—the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from other sources without restriction. The data subject to this restriction is contained on every page of this proposal.

1. Understanding the problem

RFQ Reference
Understanding the Problem: Provide a brief narrative (one paragraph) that accurately assesses the problem to be solved based on your understanding of the project requirements stated in the SOW.

KPMG highly values this opportunity to work with the OA/OIT, and we understand that the OA/OIT is seeking qualified contractors to provide consulting services to perform a detailed security assessment of the OA/OIT enterprise level information technology assets. We are confident that we are aligned to support you in achieving your objectives in the following areas:

- Assessment of security controls and procedures at the OA/OIT Technology center to include, but not limited to, enterprise directory services, firewalls, intrusion detection systems, and physical security controls.
- Detailed security assessment, based on leading practices, to analyze the external footprint of the OA/OIT by performing vulnerability scans against all OA/OIT identified assets and further to perform targeted penetration testing against OA/OIT determined high-risk assets identified during the scans.
- Email-based social engineering to determine the likelihood of obtaining user credentials with the possibility of additional social engineering tests and further penetration testing using obtained information.

2. Contractor prior experience

RFQ Reference
Contractor Prior Experience: Detail three (3) projects your company performed that are similar in nature and scope to the requirements stated in the SOW. Include reference company name and address, contact person with phone number, email address and best time to call, project name, project start and end dates and a brief description of the project.

KPMG's Information Protection and Business Resilience (IPBR) practice assists organizations, both nationally and globally, transforming their security, privacy, and continuity controls into business-enabling platforms while maintaining the confidentiality, integrity, and availability of critical business functions. Outlined in the tables below, you will see that KPMG has successfully delivered security assessment services in a similar capacity to the OA/OIT's request.

**** Note: Due to the sensitive and confidential nature of these types of assessments we are unable to provide certain details. If you wish to contact our references, we only ask that you please work through us to coordinate a time to speak to our clients.***

Project reference #1

Name of Client & Project Title	Technology Company - Information Security Assessment
Contract Value	** See note above.*
Nature and Scope of Project:	KPMG was engaged to conduct a security assessment for the following areas: Internet Services and External Network, Network Assessment, Database Assessment, and a review of the security due diligence process as it relates to information security involvement. The key objective of the internet services assessment was to conduct external vulnerability scanning and host discovery against the public-facing network systems to identify vulnerabilities within the environment. This included a scope of approximately 1.5M IP addresses. The assessment was intended to focus on identifying and reporting vulnerabilities that an attacker may be able to leverage in order to gain unauthorized access into the target systems or data. The network assessment focused on the identification of network device vulnerabilities, architecture issues related to subnet configurations, and inter-zonal access from the Internet and untrusted zones to secure, internal network zones. This assessment also included the development of recommendations for remediation of identified issues. A total of 2,283 devices, 23,674 subnets, and 6 key datacenters were included. The key objective of the database assessment was to identify databases containing sensitive information, through the performance of scans to gauge the

	effectiveness of patch management, user management, and database configuration. Approximately 600 Oracle databases and 14,000 MySQL databases were within scope. Lastly, security due diligence processes as related to information security were reviewed along with a review and documentation of the information security processes.	
Project Duration:	**Start Date Year** 09/2012	**End Date Year** 03/2013
Nature of the Client:	A multinational Internet corporation providing web portal, search engine, directory, mail, news, and other related services.	
Nature of Client Audience:	The audience of the final deliverables and assessment activity included both technical professionals responsible for implementing detailed recommendations and upper management responsible for setting the remediation strategy.	
Number of Users:	Approximately 14,000 employees and millions of users	
#& Composition of Vendor Employee & Consultants Assigned:	The KPMG team consisted of the following roles: ▪ KPMG Principal and overall project authority ▪ KPMG Managing Director and project manager ▪ Three KPMG Manager and project manager ▪ Two KPMG Sr. Associates and SMP ▪ Three KPMG Associates and SMP Aaron Hipp was a designated Manager on this engagement for the Internet services and external network assessment. Bill Varhol was a designated Sr. Associate and SMP on this engagement for the Internet services and external network assessment.	
Client Contact Information:	** See note above.*	

Project reference #2

Name of Client & Project Title	Financial Services organization – Enterprise Wide Security Assessments	
Contract Value	** See note above.*	
Nature and Scope of Project:	KPMG has been engaged over the last three years to perform a variety of information security assessments. Throughout the last three years, KPMG has provided the following services: external penetration testing, vulnerability management program review, review of intrusion detection and prevention capabilities, internal penetration testing and vulnerability assessment, mobile banking authentication review, web application security testing, security review of third-party connections, and review of development environment.	
Project Duration:	**Start Date Year** 05/2010	**End Date Year** 05/2013 (expected completion)
Nature of the Client:	One of the biggest credit unions in the country with approximately 1.7 million members. This engagement was performed in cooperation with the client's internal audit department.	
Nature of Client Audience:	The audience for all provided deliverables during this engagement included members of the internal audit department. All project deliverables were reviewed with internal audit and presented by KPMG to the client's Board of Directors.	
Number of Users:	Approximately 4,300	
#& Composition of Vendor Employee & Consultants Assigned:	The KPMG team consisted of the following: ▪ KPMG Principal and overall project authority ▪ KPMG Managing Director for quality assurance ▪ KPMG Manager and project manager ▪ KPMG subject matter professionals	
Client Contact Information:	** See note above.*	

Project reference #3

Name of Client & Project Title	Financial Services organization – Network Security Audit	
Contract Value	** See note above.*	
Nature and Scope of Project:	KPMG was engaged to complete several different components of work. The first was to provide independent assurance that the controls in place to mitigate technical security risks over the client's network environment are designed and operating effectively. Specific controls included network device configuration review (firewalls, routers, switches, VPN equipment, etc.), third-party security assessment, and intrusion detection and prevention monitoring processes. Second was to assess the adequacy of access and authentication controls over a specific web application, and security controls in place for integration between the application and a third-party application. And lastly to assess the adequacy of access and authentication controls over a specific web application and security controls in place for the integration between the application and IVR system.	
Project Duration:	**Start Date Year** 02/2012	**End Date Year** 05/2012
Nature of the Client:	A leading provider of insurance, investments, and retirement products and services. This engagement was performed in cooperation with the client's internal audit department.	
Nature of Client Audience:	The audience for all provided deliverables during this engagement included members of the internal audit department. Deliverables were compiled within the client standard of internal audit formats and turned over to internal audit at assessment completion.	
Number of Users:	5,000-10,000	
#& Composition of Vendor Employee & Consultants Assigned:	The KPMG team consisted of the following: ▪ KPMG Principal and overall project authority ▪ KPMG Manager and project manager ▪ KPMG Sr. Associate and SMP Bill Varhol was the designated Sr. Associate and SMP on this engagement.	
Client Contact Information:	** See note above.*	

3. Contractor personnel and qualifications

RFQ Reference

Contractor Personnel and Qualifications: Provide resumes with names of individuals that show the qualifications and skills required to successfully develop and implement the project as defined in the SOW. It is very important that the proposed individuals meet the minimum levels of experience and have all proper certifications, if requested. The proposed project manager must have demonstrated project management skills and technical background and experience to appropriately manage the project. Ensure resumes contain no personal information as these may become public documents.

KPMG staffs each engagement team with professionals who possess the knowledge, skills, time, and experience to perform the engagement effectively. Our ability to deliver a quality assessment relies on our team’s strong understanding of relevant policies, technology, and systems as well as the associated process risks and controls. That is why our engagement teams include experienced professionals and subject matter professionals (SMPs) who can actively participate in areas requiring special knowledge, skills, and tools.

For this important project, we have assembled a team with very specific and relevant experience suited to your needs. Our team is committed to providing you with a priority level of service, attention, and relevant experience you deserve. We will work hard to anticipate your business needs, as well as IT security issues. We will provide ample personal contact with management and communicate on a regular basis to help ascertain that all your issues are addressed in a proactive and timely fashion. Our experienced IT security assessment team will adapt to the specific needs of the OA/OIT.

Engagement Team

Tom Skoog, your Lead Engagement Principal, will provide oversight and supervision of the program manager. He is the overall authority over project work and will be available regularly to communicate with OA/OIT leadership. He has provided oversight to numerous information protection teams performing vulnerability assessments and penetration testing engagements. He has more than 25 years of providing business and technology advisory services to a wide array of companies and government entities in the U.S., Canada, Argentina, and throughout Europe and Asia.

Aaron Hipp, your Engagement Manager, will be the primary liaison between the OA/OIT and KPMG. He will identify, schedule, and supervise the professionals performing the day-to-day work for their respective portions of the engagement and will participate in and review work. Aaron leads KPMG’s Technical Security Services Center of Enablement and has extensive experience in delivering technical security assessments within a number of organizations. He has more than 12 years of IT experience in the information systems field and has a varied background in information security, security management, and regulatory compliance. His technical security experience includes a wide range of platforms, networks, and engineering concepts.

Bill Varhol, Engagement Staff, will serve as a member of the engagement team as a SMP responsible for conducting the external network security testing and social engineering exercises. His experience ranges across technical security assessments including full-scope penetration testing vulnerability assessments.

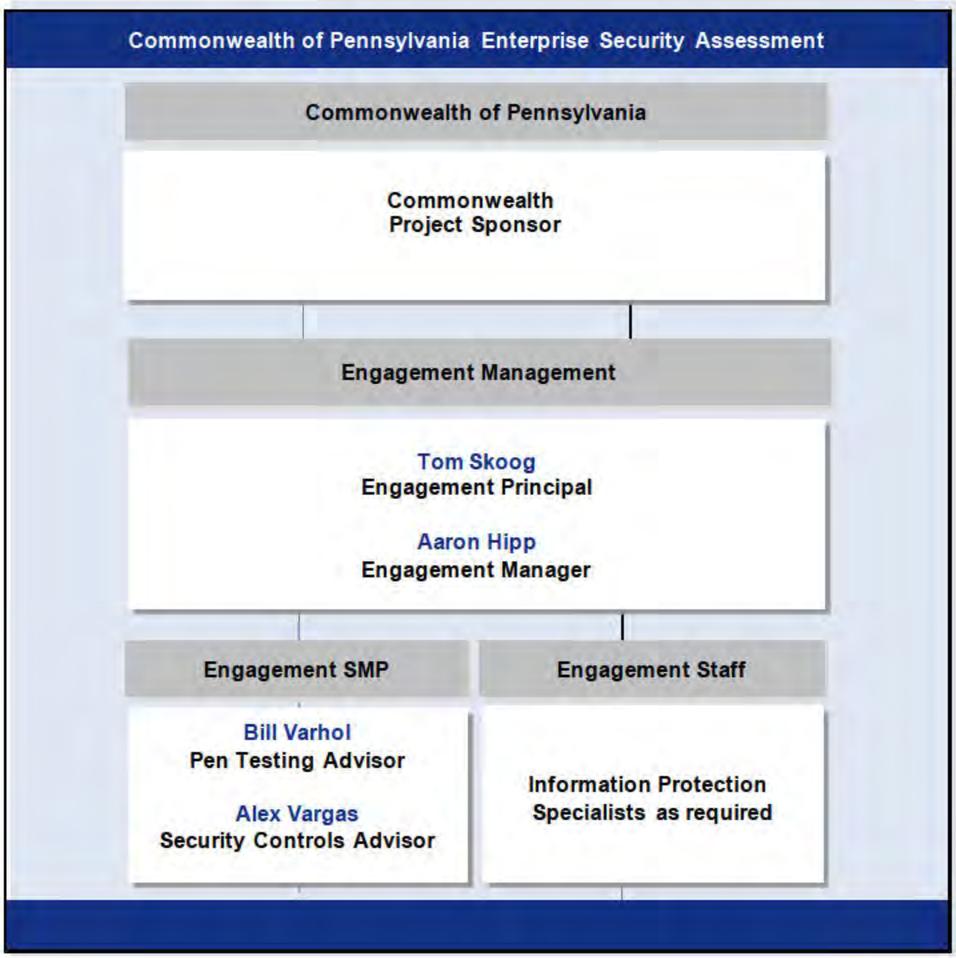
Included amongst his credentials is the required Certified Ethical Hacker (CEH) certification for which he is a SMP and Vice-Chair of the EC-Council Scheme Committee (the governing organization of the CEH certification).

Alex Vargas, Engagement Staff, will serve as a member of the engagement team as a SMP responsible for conducting the security controls and procedures review. He has over ten years experience in development and over two years experience in network security. Alex specializes in a variety of different areas including network forensics, security training and education, and secure coding practices.

KPMG will assign additional resources and SMPs with the necessary skills and experience to assist with fieldwork and reporting as appropriate for the successful completion of this project.

For the staff resumes of the individual team members proposed for this engagement please refer to Appendix A.

Engagement Team Org Chart

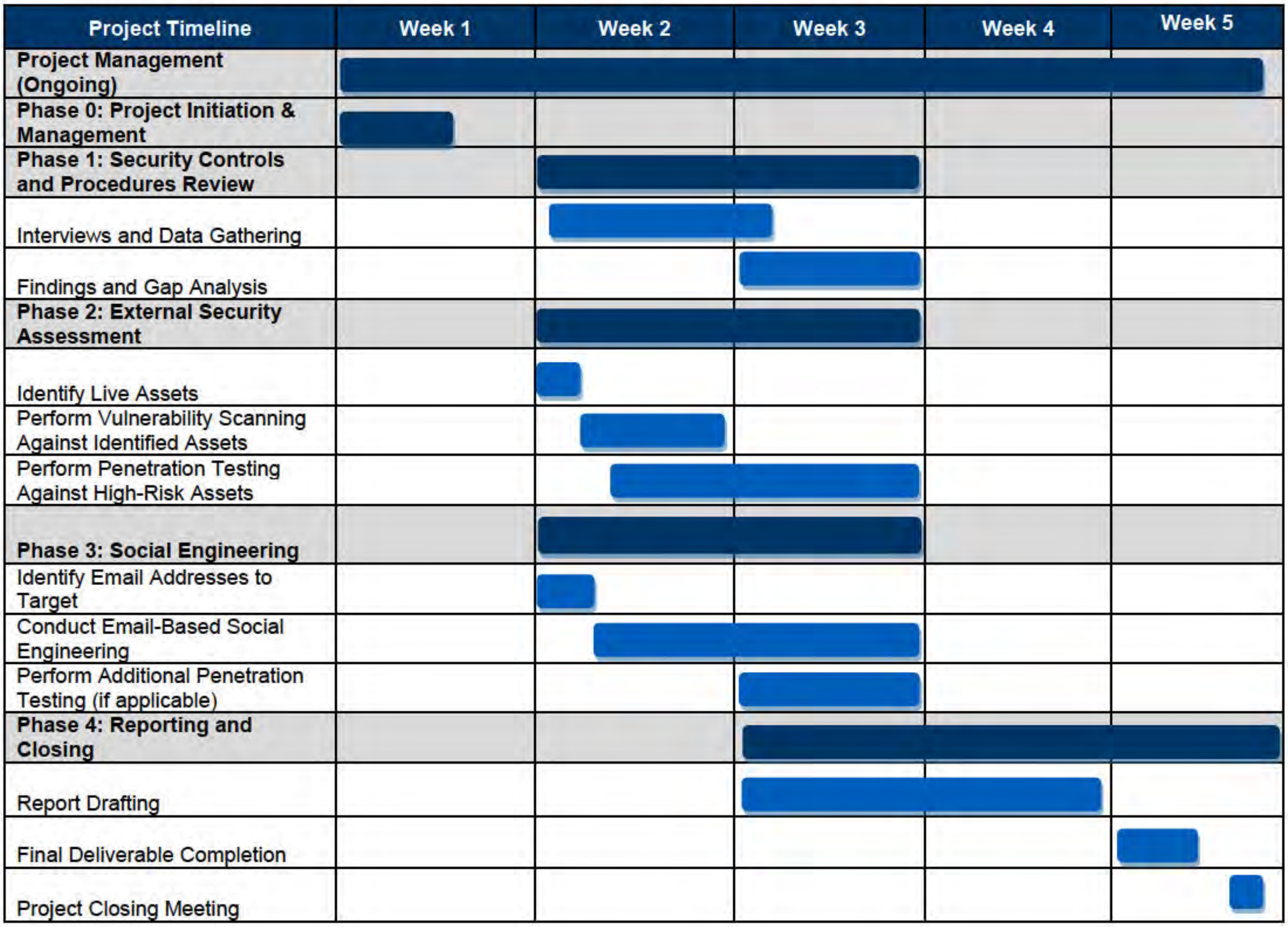

Commonwealth of Pennsylvania Enterprise Security Assessment
Commonwealth of Pennsylvania
Commonwealth Project Sponsor
Engagement Management
Tom Skoog
Engagement Principal
Aaron Hipp
Engagement Manager
Engagement SMP
Engagement Staff
Bill Varhol
Pen Testing Advisor
Alex Vargas
Security Controls Advisor
Information Protection Specialists as required

4. Project work plan

RFQ Reference

Project Work Plan: Utilizing a GANTT or PERT chart, include a high-level summary that shows all the tasks and deliverables to complete the project. Explain your approach to deliverables. Explanation must be limited to one page.

Based on information provided by the OA/OIT, we are prepared to start the enterprise information security assessment at a mutually agreeable date no later than May 1, 2013. Depending on the schedules of the OA/OIT, we expect the project to last approximately five weeks, as depicted in the timeline below.



Project Timeline	Week 1	Week 2	Week 3	Week 4	Week 5
Project Management (Ongoing)	■	■	■	■	■
Phase 0: Project Initiation & Management	■				
Phase 1: Security Controls and Procedures Review		■	■		
Interviews and Data Gathering		■	■		
Findings and Gap Analysis			■		
Phase 2: External Security Assessment		■	■		
Identify Live Assets		■			
Perform Vulnerability Scanning Against Identified Assets		■			
Perform Penetration Testing Against High-Risk Assets		■	■		
Phase 3: Social Engineering		■	■		
Identify Email Addresses to Target		■			
Conduct Email-Based Social Engineering		■	■		
Perform Additional Penetration Testing (if applicable)			■		
Phase 4: Reporting and Closing			■	■	■
Report Drafting			■	■	
Final Deliverable Completion					■
Project Closing Meeting					■

Throughout the engagement, KPMG will provide draft deliverables to the OA/OIT Program Manager for review and comment. This will provide opportunities to review the deliverables and obtain the OA/OIT's feedback on their content and quality. KPMG understands the final report deliverable to consist of:

- Executive Summary Report
- Detailed Findings Report
- Recommended Remediation Report

Executive Summary Report

The target audience for this report is the OA/OIT's executive management. This report will comprise of the assessment scope, objectives, and approach of each of the assessments. The report will also summarize the urgent and high-risk security vulnerabilities identified by the scanning tool in clear terms, as well as provide potential remediation strategies.

Detailed Findings Report

The target audience for this report is the OA/OIT's security management, operations teams, and application development teams. This report will outline the scope of the assessment activity, procedures used to perform the activity, and summary of identified vulnerabilities. This data will be structured to include a severity rating for Vulnerability Risk Classification based on industry standards. Items that are deemed a critical risk will be escalated to you at the time of discovery, and will also be reported in this document.

Recommended Remediation Report

The target audience for this report is security management, operations, and application development teams. This report will outline the scope of the assessment activity and summarize the identified vulnerabilities. In addition, the report will include leading industry system hardening methods, application coding mitigation strategy, application architecture mitigation strategies, and governance remediation details. Other industry vulnerability comparisons, where possible, will also be included.

At the conclusion of the engagement, deliverable reports, supporting evidence, related documentation, raw output from tools and assessments, and other beneficial data will be presented to the OA/OIT Program Manager on CD for distribution to the appropriate OA/OIT teams. In addition, six printed copies of the final report will also be delivered. The advice, recommendations, work product, and deliverables provided as part of this engagement will be developed for OA/OIT management, and are not intended for use by any other party or for any other purpose, and may only be relied upon by OA/OIT management and will be so marked. We disclaim any intention or obligation to update or revise the observations whether as a result of new information, future events or otherwise. Should additional documentation or other information become available which impacts upon the observations reached in our deliverables, we reserve the right to amend our observations and summary documents, including deliverables, accord.

5. Cost

RFQ Reference
Cost: Complete the attached Cost Matrix SA2013001 Enterprise Security Statement Cost Matrix to submit the cost portion of your bid.

Our fixed price professional fees will be $72,800 required to complete the engagement. The completed cost matrix attached below presents the resources required.

[redacted]

6. Domestic workforce utilization

RFQ Reference

Domestic Workforce Utilization: Complete and sign the Attachment C Domestic Workforce Utilization Form in Appendix B of the Statement of Work.

The signed and completed Domestic Workforce Utilization Form has been attached as requested.

[redacted]

7. Small diverse business participation

RFQ Reference

Disadvantaged Business Participation: To maximize DGS-certified Small Diverse Business participation in the project, the greatest consideration will be given to a Small Diverse Business bidding as a prime contractor. For all other prime contractors subcontracting to a Small Diverse Business, briefly explain what your company's approach will be to maximize Small Diverse Business participation in the project if you are selected for award. This should include detail on which portions of the contract will be performed by the Small Diverse Business. Include specific percentage commitments to be paid to Small Diverse Businesses based upon the total contract value. The more definitive the commitment and the greater the percentage commitment, the greater consideration that your company will receive for this best value selection factor.

KPMG is a strong supporter of the OA/OIT's Small Diverse Business Program and we often team with DBE/MBE/WBE firms to deliver our services. However, this RFQ requires specialized skills and involves aggressive timelines. KPMG is proposing to perform all of the services with KPMG resources rather than rely on subcontractors.

8. Other

RFQ Reference
Other: Any other factor not included in the above criteria determined especially relevant for this project.

Assumptions

The following assumptions were used to determine our cost for this engagement. If it is later determined that any of these assumptions were not valid, KPMG reserves the right to submit a change request to reflect updated assumptions, and resulting changes to the project.

- The OA/OIT will provide the actual IP ranges to be tested and include any specific systems or applications that should not be tested.
- The OA/OIT will be responsible for all necessary change control activities.
- Evasion techniques are available but currently understood to be out of scope.

Responsibilities of the OA/OIT

The overall leadership and guidance of the OA/OIT is required for an engagement such as this to be successful, particularly as it relates to management's decisions based on the information, results, and recommendations provided by KPMG to the OA/OIT. In preparing our response, we have made the following assumptions regarding the OA/OIT's involvement:

- The OA/OIT will designate a qualified individual to coordinate the project with KPMG and other stakeholders;
- While KPMG project team provides findings and options, the OA/OIT is responsible to make all management decisions;
- The OA/OIT will provide reasonable access to its technical staff and systems throughout the project;
- The OA/OIT will provide qualified resource to evaluate the adequacy of services performed by KPMG project team;
- The OA/OIT will review and approve interim-deliverables in a timely manner;
- The OA/OIT will accept the risks inherent to penetration testing either via a signed Letter of Authorization (sample in Appendix B), or provide a point of contact that has the authority to approve individual groups of tests on a per instance basis;

- For any work performed onsite at the OA/OIT, KPMG personnel will require adequate workspace, equipment, appropriate network access, and building access to be provided to the KPMG team members; and
- The OA/OIT will be responsible for coordinating logistical matters related to scheduling meetings, identifying key resources within the OA/OIT at large to participate in the project, and coordinating communications within the OA/OIT personnel.

Communication

We believe effective communication between the OA/OIT and KPMG is a critical success factor for this project. KPMG will maintain an open line of communication with the OA/OIT Program Management. Our communication plan will include: reporting structures, issue reporting, escalation and resolution methodology, regular meetings, and status reports.

Engagement Terms and Conditions

Our engagement is subject to completion of KPMG’s normal engagement acceptance process and execution of an Engagement Letter, which will reference the terms and conditions of the Master Services Agreement (MSA) in place between KPMG and the OA/OIT.

Performance of active security testing is contingent upon the OA/OIT’s completion of a signed Authorization Letter, referenced in **Appendix B,** which sanctions use of vulnerability analysis tools and penetration techniques against the OA/OIT’s information systems.

Clarification of SOW Requirements

KPMG is enthusiastic about the opportunity to strengthen our relationship with the OA/OIT. During our thorough review of the RFQ and related SOW, we identified a few items for which we would like to clarify.

SOW Section IV-3 under “Requirements”

Your statement is as follows:

d) All raw data from any test will be the property of the OA/OIT. All data, deliverables, and records residing with the Contractor will be returned to the OA/OIT no later than June 30th 2013. Contractor copies of all data, deliverables and records shall be destroyed in the manner and on the timeline directed by the OA/OIT, and a certification shall be made in writing as to their destruction.

KPMG would like to add the following paragraph to the end of above section:

“Notwithstanding the foregoing, Contractor may retain a copy of information received, developed, or otherwise relating to this contract to the extent necessary to comply with its contractual obligations and applicable professional standards. Information stored on routine back-up media for the purpose of disaster recovery will be subject to destruction in due course. Latent data such as deleted files and other non-logical data types, such as memory dumps, swap files, temporary files, printer spool files and metadata that can customarily only be retrieved by computer forensics experts and are generally considered inaccessible without the use of specialized tools and techniques will not be within the requirement for the return of records as contemplated by this paragraph.”

SOW Section IV-3 under “Information Handling”

Your statement is as follows:

a) This project will require handling of sensitive information. The selected Contractor shall prevent access to, copying of and/or distribution of such information except as necessary and permitted for work on this project. The selected Contractor is responsible for proper disposal (i.e. shred, surrender) of both hard and electronic working copies of such sensitive information during work on this project, as well as any remaining information upon the completion of the project. The Contractor must certify in writing to the disposal of sensitive information. The requirements of this provision will survive the termination of the Purchase Order and the contract.

KPMG would like to add the following paragraph to the end of above section:

"Use of Third Party Service Providers –The OA/OIT acknowledges that in connection with the performance of services under the Contract, Contractor uses third party service providers within and without the United States to provide at Contractor's direction administrative and clerical services to Contractor. These third party service providers may in the performance of such services have limited access to information, including but not limited to confidential information, received by Contractor from or at the request or direction of the Contractor. Contractor represents to the OA/OIT that each such third party service provider has agreed to conditions of confidentiality with respect to the OA/OIT's information to the same or similar extent as Contractor has agreed to pursuant this Contract. Contractor has full responsibility to cause these third party service providers to comply with such conditions of confidentiality and Contractor shall be responsible for any consequences of their failure to comply. Accordingly, the OA/OIT consents to Contractor disclosure to a third party service provider and the use by such third party service provider of data and information, including but not limited to confidential information, received from or at the request or direction of the OA/OIT for the purposes set forth herein."

SOW Section IV-3 (c). Information Technology Bulletins

Your statement is as follows:

c) The Contractor shall comply with the Information Technology Bulletins (ITB's) issued by the Office of Administration, Office for Information Technology (OA-OIT). ITB's may be found at http://www.portal.state.pa.us/portal/server.pt?open=512&objID=416&PageID=210791&mode=2 . All proposals must be submitted on the basis that all ITBs are applicable to this procurement. It is the responsibility of the Contractor to read and be familiar with the ITBs. Notwithstanding the foregoing, if the Contractor believes that any ITB is not applicable to this procurement, it must list all such ITBs in its technical submittal, and explain why it believes the ITB is not applicable. The Issuing Office may, in its sole discretion, accept or reject any request that an ITB not be considered to be applicable to the procurement. The Contractor's failure to list an ITB will result in its waiving its right to do so later, unless the Issuing Office, in its sole discretion, determines that it would be in the best interest of the OA/OIT to waive the pertinent ITB.

KPMG has reviewed OA/OIT's ITB's and identified ITB's that are not applicable to this procurement. Please refer to the following attachment:

PA ITB Analysis Final
04102013.xlsx

Other Matters

Your ITQ statement 28.b is as follows:

b) The Contractor certifies that it is not currently under suspension or debarment by the Commonwealth, any other state, or the federal government, and if the Contractor cannot so certify, then it agrees to submit along with the bid/Proposal a written explanation on why such certification cannot be made.

With respect to the Federal Government, KPMG has no concerns with the certification. KPMG is a nationwide accounting firm and works on thousands of engagements each year across the country. We do not formally track state or local contract terminations, debarments, or suspensions. As is the case with other major accounting firms, from time to time KPMG may receive a question or complaint from a client about the conduct of a particular engagement. KPMG attempts to promptly address and resolve issues with clients, so that clients do not invoke contractual termination or default clauses. KPMG is not aware of any significant issues, relating to contracts with other clients in the last 5 years, or any terminations, suspensions, or debarments of those contacts, which would present any concerns with respect to KPMG's ability to successfully perform the services contemplated by this proposal.

KPMG’s services as outlined in this proposal constitute an advisory engagement conducted under the American Institute of Certified Public Accountants (“AICPA”) Standards for Consulting Services. Such services are not intended to be an audit, examination, attestation, special report or agreed-upon procedures engagements as those services are defined in AICPA literature applicable to such engagements conducted by independent auditors. Accordingly, these services shall not result in the issuance of a written communication to third parties by KPMG directly reporting on financial data or internal control or expressing a conclusion or any other form of assurance.

The OA/OIT agrees that KPMG may list it as a customer in its marketing materials. In addition, the OA/OIT gives KPMG the right to use the OA/OIT’s logo on documents prepared for the OA/OIT internally (e.g., internal presentations, etc.).

Appendices

Appendix A: Résumés

[redacted]

THOMAS SKOOG

Principal

KPMG LLP
191 W. Nationwide Blvd, Suite 500
Columbus, OH 43215

[redacted]
Fax 614-388-5624

[redacted]

Function and Specialization

Tom is a member of the IT Advisory practice focusing on Information Protection Services, IT Performance Improvement and IT Risk Management. Tom leads the IT Advisory practice in the Ohio Valley.

Professional Associations

- Information Systems Audit and Control Association (ISACA)

Education, Licenses & Certifications

- BS, Northern Michigan University
- Certified Information System Security Professional (CISSP)
- ITIL Foundation Certified

Background

Tom is a Principal in KPMG's Advisory Services practice focusing on Information Protection, IT Performance Improvement, IT Project Management and IT Risk Management initiatives. He has over 25 years of providing business and technology advisory services to a wide array of companies and government entities in the U.S., Canada, Argentina, and throughout Europe and Asia.

Professional and Industry Experience

Tom serves as the retail sector leader for our Advisory Services practice in the Midwest. He has over 25 years of retail experience in both industry and professional service roles. He has worked with retailers on improving regulatory compliance, IT operations, inventory management, enabling e-Business initiatives, and security and continuity maturity for a variety of retailers in the U.S.

Information Protection & Business Continuity

- Led a team of professionals assisting one of the world's largest retailers develop business continuity, disaster recovery and business resilience plans. Has interacted with virtually every facet of the business in understanding critical processes and designing recovery/high availability strategies.
- Led a team responsible for the development of an Identity and Access Management strategy for a large Midwest healthcare provider. His strategy and subsequent implementation resulted in various awards being bestowed on this entity from certain Information Security professional organizations.
- Worked with one of the largest department store retailers on the development of business continuity plans and the creation of a BCP governance structure to manage the program on a going-forward basis.
- Worked with a Midwest financial services company in the assessment of current compliance with PCI requirements and developed a roadmap to assist in moving towards a compliant state within the next 12 months. Continues to work with this firm on assessing remediation efforts.
- Led a large business impact analysis for every state agency of a large, Midwestern state and developed recovery recommendations for the processes and technologies supporting the processes. Ability to interact with a variety of Executive branch officials and state legislators in discussing the results of the work and recommendations to move forward.
- Provided oversight to multiple security vulnerability and attack & penetration assessments for companies in a variety of industries.

[redacted]

AARON HIPP

Manager

KPMG LLP
191 West Nationwide Blvd
Columbus OH, 43215

[redacted]
Fax 614-283-5325

[redacted]

Function and Specialization

Aaron is a member of the IT Advisory practice and is the National Lead for Technical Security Services Center of Enablement.

Professional Associations

- Information Systems Security Association (ISSA)
- Information Systems Audit and Control Association (ISACA)

Education, Licenses & Certifications

- BS, Computer Engineering Technology from the University of Dayton, Ohio
- Certified Information System Auditor (CISA)
- Pursuing Certified Information System Security Professional (CISSP)
- Pursuing Certified Ethical Hacker (CEH)

Background

Aaron is KPMG’s National Lead for the Technical Security Services Center of Enablement and a Manager in the IT Advisory practice in Columbus, OH. He has over 12 years of IT experience in the information systems field and has a varied background in information security, security management and regulatory compliance. His technical security expertise includes a wide range of platforms, networks, and engineering concepts. He has experience in using existing and emerging technologies to resolve complex technical and business problems. Aaron’s current and past clients include some of the leading entities in the financial services, healthcare and banking industries.

He has completed the Certified Ethical Hacker course and is working towards his CISSP.

Professional and Industry Experience

Aaron has substantial experience leading and coordinating IT advisory engagements across several industries, with a focus on the financial services, healthcare, and banking sectors. He has served as the project lead with responsibility for planning, budgeting, and execution, of projects including: Attestation and External Audit engagements, Vulnerability and Compliance assessments, RF/Wireless, Data Loss Prevention (DLP), and External Internet exposure analysis as well as designing new solutions using current and emerging technologies. He has also provided subject matter knowledge and guidance to a leading global financial institution on controls testing for systems with respect to application and database security, change management, and segregation of duties.

Information Protection & Business Continuity

- Responsible for coordinating and executing a Global Vulnerability Assessment and Penetration Test for a Fortune 5 retail company. The scope of this project include in-country and remote based testing performed concurrently in over 15 countries for the wired and wireless networks.
- Led KPMG’s National Security Testing Lab renovation effort from development through “go live” to create a security testing facility capable of supporting all US based security testing activities.
- Currently Act as KPMG’s Center of Enablement lead for all US based Security testing and global strategic alignment.
- Designed and implemented a vulnerability and compliance management solution to be used globally for a large bank holding company as well as the day to day Project Management responsibilities.
- Performed a vulnerability assessment of a major healthcare client’s wireless network infrastructure as well as performing configuration compliance analysis and rouge access point identification for the entire infrastructure including 18 remote sites.
- Participated in KPMG’s Security Vulnerability Assessment for an automotive industry IT infrastructure and company websites.

[redacted]

WILLIAM J. VARHOL

Senior Associate

KPMG LLP
150 West Jefferson, Suite 1900
Detroit, MI 48226

[redacted] [redacted]
Fax 313-447-2069

[redacted]

Function and Specialization

William is a member of the IT Advisory practice specializing in IT Security including vulnerability assessments and full-scope penetration testing.

Professional Associations

- InfraGard National Members Alliance
- Vice Chair, EC-Council Scheme Committee

Education, Licenses & Certifications

- Microsoft Certified Systems Engineer + Security Specialization (MCSE + S)
- GIAC Penetration Tester (GPEN) (exp.)
- Offensive Security Certified Professional (OSCP)
- Offensive Security Wireless Professional (OSWP)
- Certified Ethical Hacker (CEH)
- EC-Council Certified Security Analyst (ECSA)
- Licensed Penetration Tester (LPT)
- CompTIA Security+

Background

Mr. Varhol is currently serving as a senior associate in KPMG's IT Advisory practice. He has a strong IT security background with a handful of industry recognized certifications and over 10 years in the information technology field. He has held a variety of previous positions including helpdesk technician, systems administrator, network administrator, and information assurance officer.

Professional and Industry Experience

Mr. Varhol joins KPMG bringing with him IT experience from both the private and public sectors. Just prior to joining KPMG, he served as a contractor within the US Department of Defense as a systems administrator and information assurance officer. His experience there provided him with insight into practices such as DIACAP and other defense regulations. Mr. Varhol has also worked for a non-profit organization and in the payment card industry for one of the world's largest credit card processors.

Since joining KPMG, he has participated in many technical engagements primarily focusing on vulnerability assessments and penetration testing. He has also provided security policy review services to clients as well as general information security guidance.

In addition to his professional affiliations, Mr. Varhol is actively involved within the information security community and volunteers much of his time to assist different groups with a variety of projects.

Information Protection

- Provided internal and external network, website, database, and wireless vulnerability assessments and penetration testing to some of the nation's top retailers, universities, e-commerce companies, manufacturing companies, banks, insurance companies, nuclear energy companies, and others.
- Participated in multiple social engineering engagements for security awareness testing including telephone calls and email phishing. Created custom scripts and a web-based application that helped streamline the phishing process and increase the rate of success for email phishing tests.
- Conducted security policy reviews including antivirus management, patch management, third-party connections, configuration management, and intrusion detection practices as well as general information security controls.

Other Activities

- Certified Ethical Hacker (CEH) SME
- Volunteer, Cyber Security Forum Initiative
- Volunteer, Hackers For Charity
- Community Board of Advisors, The Ethical Hacker Network
- Member, Citizen Corps Community CERT (Novi, MI)

[redacted]

ALEX VARGAS

Senior Associate, Advisory

KPMG LLP
1601 Market Street
Philadelphia, PA - 19103

[redacted] [redacted]
Fax 313-447-2069

[redacted]

Function and Specialization

Alex is a member of the Advisory practice specializing in information protection and risk management.

Professional Associations

- OWASP
- ISACA

Languages

- English

Education, Licenses & Certifications

- B.S. in Economics
- M.S. in Information Security
- SANS GIAC Certified Intrusion Analyst

Background

Alex is a Senior Associate in KPMG's Philadelphia Advisory Practice, specializing in Information Protection and Business Resilience. He attended Purdue University where he was involved with Center for Education and Research in Information Assurance and Security (CERIAS) and Purdue Homeland Security, Measured Response. He has over ten years of experience in development and over two years of experience in network security. Alex's areas of expertise include: training and educating individuals in information security, designing secure web applications, performing network forensics, and assessing risk and compliance from a technical and business perspective.

Professional and Industry Experience

Alex has led and assisted in projects across a variety of industries including: healthcare, education, and technology. He has always had a keen focus on security and for more than ten years. His expertise lies in: network traffic forensic analysis, vulnerability assessments, web application security, and code audit.

- Evaluated real-time security events for multiple clients across all industries. Provided in-depth analysis to the clients about how to react and best next steps to contain the issue.
- Performed HIPAA training for new hires in best security practices.
- Created coding standards to improve coordination and productivity between developers.
- Maintained and audited coding standards; Implemented new controls.
- Performed network vulnerability assessments; implemented and created technical controls for private practices to exceed HIPAA recommendations.

Technical Skills

Mac OS X, UNIX, Linux, Microsoft Windows, Novell, C/C++, PHP, MUMPS ,lasso, Visual Python, SQL, Java, XSL/XSLT, JavaScript, XML, CSS, XHTML, backtrack, metasploit, nessus, mod_security, impervia, snort

Other Activities

- CERIAS Researcher, 2003-2006
- Member, Chicago Security Group (ChiSec), 2008-2012
- Golden Key International Honour Society, 2009
- Volunteer (Security), THOTCON, 2010, 2011

Appendix B: KPMG Authorization Letter Template

KPMG Authorization Letter Template

[MONTH], [DAY], 2013

Tom Skoog, Principal
KPMG LLP
191 W. Nationwide Blvd Ste. 500
Columbus, OH 43215

Dear Mr. Skoog:

Pursuant to our agreed upon engagement letter dated [DATE of Letter], [YEAR of Letter], this letter sets forth the terms for permission and authorization to conduct security testing at the Commonwealth of Pennsylvania Office of Administration / Office of Information Technology (“OA/OIT”).

The OA/OIT is aware of the risks associated with security testing and has taken the necessary pre-testing steps (e.g., data backup, internal communications) to help minimize these risks.

This letter of authorization is intended to enable KPMG LLP (“KPMG”) to perform these tests without concern for being subject to action by the OA/OIT for trespassing on OA/OIT property, unintended network or system interruptions or unauthorized access to the OA/OIT computer networks.

I acknowledge that KPMG may need to install security testing software on OA/OIT systems as part of the testing process and that all installed software will be removed at the end of the engagement. Subsequently, I acknowledge that KPMG LLP may access and store data, sensitive to the organization as part of the regular testing procedures with the expectation that all data will be treated as confidential and destroyed at the end of the engagement unless required to be retained as part of the KPMG work papers to support the work performed. In these cases, the data will be sanitized to the extent possible.

I, [COMPANY AUTHORITY NAME, TITLE], authorize KPMG LLP to perform security testing activities against the following:

1. External data network and web application access to the following network segments and hosts:
    a. XX.XX.XX.XX – XX.XX.XX.XX
    b. XX.XX.XX.XX – XX.XX.XX.XX
2. DMZ data network access to the following network segments and hosts:
    a. XX.XX.XX.XX
    b. http://www.domain.com
    c. https://www.domain.com/application
3. Internal data network access to the following network segments:
    a. XX.XX.XX.XX – XX.XX.XX.XX
    b. XX.XX.XX.XX – XX.XX.XX.XX

The security testing is authorized to occur between [TIME, TIME ZONE, MONTH, DAY, YEAR] and [TIME, TIME ZONE, MONTH, DAY, YEAR].

Signed on behalf of the Commonwealth of Pennsylvania,

[Client AUTHORITY NAME]

[TITLE]

Commonwealth of Pennsylvania OA/OIT

*Client Office Number*________________

*Client Mobile Number*_______________

*Client Alternative Number*___________

Contact us

Tom Skoog
Principal Advisory

[redacted]

Aaron Hipp
Manager, Advisory

[redacted]

kpmg.com