REQUEST FOR PROPOSALS FOR

SAP ERP SYSTEM AND INFORMATION SECURITY PROGRAM ASSESSMENTS

ISSUING OFFICE

Pennsylvania Turnpike Commission

Information Technology Department

RFP NUMBER

13-10340-3950

DATE OF ISSUANCE

January 7, 2013

REQUEST FOR PROPOSALS FOR

RFP 13-10340-3950

TABLE OF CONTENTS

PART I – GENERAL INFORMATION FOR PROPOSERS

I-1 Purpose.

This request for proposals (RFP) provides interested Proposers with sufficient information to enable them to prepare and submit proposals for consideration by the Pennsylvania Turnpike Commission (Commission) to address the technology consulting service requirements of the Commission's Information Technology (I.T.) department.

The Commission seeks to retain the services of an I.T. consulting firm(s) experienced in performing SAP Enterprise Resource Management (ERP) system assessments and Information Security Program Assessments.

I-2 Issuing Office.

This RFP is issued for the Commission by the Information Technology Department**.** All questions regarding this RFP must be directed to the Commission pursuant to the process identified in Part I-9 below. No questions will be addressed except through such process.

I-3 Problem Statement.

The Commission is soliciting proposals from qualified I.T. consulting firm(s) for the purpose of conducting an assessment(s) of the Commission's SAP ERP System and the Commission's Information Security Program.

I-4 Scope.

This RFP contains instructions governing the proposals to be submitted and the material to be included therein; a description of the service to be provided; requirements which must be met to be eligible for consideration; general evaluation criteria; and other requirements to be met by each proposal.

The scope of work for this RFP will be divided into two lots. Lot 1 is an SAP ERP System Assessment. Lot 2 is an Information Security Program Assessment. Proposers may submit proposals for each lot and/or both lots for a maximum of three proposals. The Commission anticipates that efficiencies may be likely with an award of both lots to the same Proposer and anticipates to see pricing from Proposers submitting for both lots to reflect these potential efficiencies.

I-5 Type of Contract.

It is proposed that, if contract(s) are entered into as a result of this RFP, they will be fixed-price, deliverable-based contract(s).

The Commission may in its sole discretion undertake negotiations with multiple Proposers whose proposals as to price and other factors show them to be qualified, responsible, and capable of performing the work.

Also, the Commission does not intend for the selected Proposer (Contractor), who is awarded a contract as a result of this RFP, to provide specifications or recommendations to the Commission concerning the need for additional services or to otherwise recommend to the Commission the making of a contract or a course of action of which the making of a contract is an express or implied part. Instead the Commission expects that the selected Proposer (Contractor) would identify options or alternatives available to the Commission; in these circumstances the selected Proposer (Contractor) would not be precluded from any future procurements or follow-on work related to any options or alternatives so identified in the assessments.

I-6 Rejection of Proposals.

The Commission reserves the right to reject any and all proposals received as a result of this request, or to negotiate separately with competing Proposers.

I-7 Subcontracting.

Any use of subcontractors by a Proposer must be identified in the proposal. During the contract period use of any subcontractors by the selected Proposer, which were not previously identified in the proposal, must be approved in advance in writing by the Commission.

A firm that responds to this solicitation as a prime may not be included as a designated subcontractor to another firm that responds to the same solicitation. **Multiple responses under any of the foregoing situations may cause the rejection of all responses of the firm or firms involved.** This does not preclude a firm from being set forth as a designated subcontractor to more than one prime contractor responding to the project advertisement.

The existence of any subcontract shall not change the obligations of the selected Proposer to the Commission. Upon request of the Commission, the selected Proposer must provide the Commission with a copy of the subcontract agreement between the selected Proposer and the subcontractor. The Commission reserves the right, for good cause, to require that the selected Proposer remove a subcontractor from the project. The Commission will not be responsible for any costs incurred by the selected Proposer in replacing the subcontractor if good cause exists.

I-8 Incurring Costs.

The Commission is not liable for any costs the Proposer incurs in preparation and submission of its proposal, in participating in the RFP process or in anticipation of award of contract.

I-9 Questions and Answers.

Written questions may be submitted to clarify any points in the RFP which may not have been clearly understood. Written questions should be submitted by email to RFP-Q@paturnpike.com with **RFP# 12-10340-3950** in the Subject Line to be received no later than **2:00 PM local time on Thursday, January 17, 2013**. All questions and written answers will be posted to the website as an addendum to and become part of this RFP.

I-10 Addenda to the RFP.

If it becomes necessary to revise any part of this RFP before the proposal response date, addenda will be posted to the Commission's website under the original RFP document. It is

the responsibility of the Proposer to periodically check the website for any new information or addenda to the RFP.

The Commission may revise a published advertisement. If the Commission revises a published advertisement less than ten days before the RFP due date, the due date will be extended to maintain the minimum ten-day advertisement duration if the revision alters the project scope or selection criteria. Firms are responsible to monitor advertisements/addenda to ensure the submitted proposal complies with any changes in the published advertisement.

I-11 Response.

To be considered, proposals must be delivered to the Pennsylvania Turnpike Commission's Contracts Administration Department, Attention: Wanda Metzger, on or before **12:00 PM local time on Tuesday, February 5, 2013.** The Pennsylvania Turnpike Commission is located at 700 South Eisenhower Boulevard, Middletown, PA 17057 (Street address). Our mailing Address is P. O. Box 67676, Harrisburg, PA 17106.

Please note that use of U.S. Mail, FedEx, UPS, or other delivery method, does not guarantee delivery to the Contracts Administration Department by the above-listed time for submission. Proposers mailing proposals should allow sufficient delivery time to ensure timely receipt of their proposals. If the Commission office location to which proposals are to be delivered is closed on the proposal response date, due to inclement weather, natural disaster, or any other cause, the deadline for submission shall be automatically extended until the next Commission business day on which the office is open. Unless the Proposers are otherwise notified by the Commission, the time for submission of proposals shall remain the same.

I-12 Proposals.

To be considered, Proposers should submit a complete response to this RFP, using the format provided in PART II. Each proposal should be submitted in **five (5)** hard copies of the Technical Submittal and **five (5)** hard copies of the Cost Submittal. In addition to the hard copies of the proposal, **one complete and exact copy of the entire proposal (Technical and Cost, along with all requested documents) on CD-ROM or Flash Drive in Microsoft Office or Microsoft Office-compatible format.** Proposer should ensure that there is no costing information in the technical submittal. The CD or Flash drive should clearly identify the Proposer and include the name and version number of the virus scanning software that was used to scan the CD or Flash drive before it was submitted. The Proposer shall present the proposal to the Contracts Administration Department only. No other distribution of proposals will be made by the Proposer. Each proposal page should be numbered for ease of reference. An official authorized to bind the Proposer to its provisions must sign the proposal. If the official signs the Proposal Cover Sheet (Appendix C to this RFP) and the Proposal Cover Sheet is attached to the proposal, the requirement will be met. For this RFP, the proposal must remain valid for at least **120** days. Moreover, the contents of the proposal of the selected Proposer will become contractual obligations if a contract is entered into.

Each and every Proposer submitting a proposal specifically waives any right to withdraw or modify it, except as hereinafter provided. Proposals may be withdrawn by written or fax notice (fax number (717) 986-8714) received at the Commission's address for proposal delivery prior to the exact hour and date specified for proposal receipt.

Overnight Delivery Address:
Contracts Administration Department
Attn: Donald Klingensmith
Director of Contracts Administration
PA Turnpike Commission
700 South Eisenhower Blvd.
Middletown, PA 17057

US Mail Delivery Address:
Contracts Administration Department
Attn: Donald Klingensmith
Director of Contracts Administration
PA Turnpike Commission
P.O. Box 67676
Harrisburg, PA 17106

However, if the Proposer chooses to attempt to provide such written notice by fax transmission, the Commission shall not be responsible or liable for errors in fax transmission. A proposal may also be withdrawn in person by a Proposer or its authorized representative, provided his/her identity is made known and he/she signs a receipt for the proposal, but only if the withdrawal is made prior to the exact hour and date set for proposal receipt. A proposal may only be modified by the submission of a new sealed proposal or submission of a sealed modification which complies with the requirements of this solicitation.

I-13 Economy of Preparation.
Proposals should be prepared simply and economically, providing a straightforward, concise description of the Proposer's ability to meet the requirements of the RFP.

I-14 Discussions for Clarification.
Proposers who submit proposals may be required to make an oral or written clarification of their proposals to the Issuing Office through the Contracts Administration Department to ensure thorough mutual understanding and Proposer responsiveness to the solicitation requirements. The Issuing Office through the Contracts Administration Department will initiate requests for clarification.

I-15 Best and Final Offers.
The Issuing Office will not conduct discussions with Proposers for the purpose of obtaining "best and final offers." Each Proposer should submit its best offer in its proposal.

I-16 Prime Proposer Responsibilities.
The selected Proposer will be required to assume responsibility for all services offered in its proposal whether or not it produces them. Further, the Commission will consider the selected Proposer to be the sole point of contact with regard to contractual matters.

I-17 Proposal Contents.
Proposals will be held in confidence and will not be revealed or discussed with competitors, unless disclosure is required to be made (i) under the provisions of any Commonwealth or United States statute or regulation; or (ii) by rule or order of any court of competent jurisdiction. All material submitted with the proposal becomes the property of the

Pennsylvania Turnpike Commission and may be returned only at the Commission's option. Proposals submitted to the Commission may be reviewed and evaluated by any person other than competing Proposers at the discretion of the Commission. The Commission has the right to use any or all ideas presented in any proposal. Selection or rejection of the proposal does not affect this right.

In accordance with the Pennsylvania Right-to-Know Law (RTKL), 65 P.S. § 67.707 (Production of Certain Records), Proposers shall identify any and all portions of their Proposal that contains confidential proprietary information or is protected by a trade secret. Proposals shall include a written statement signed by a representative of the company/firm identifying the specific portion(s) of the Proposal that contains the trade secret or confidential proprietary information.

Proposers should note that "trade secrets" and "confidential proprietary information" are exempt from access under Section 708(b)(11) of the RTKL. Section 102 defines both "trade secrets" and "confidential proprietary information" as follows:

Confidential proprietary information: Commercial or financial information received by an agency: (1) which is privileged or confidential; **and** (2) the disclosure of which would cause substantial harm to the competitive position of the person that submitted the information.

Trade secret: Information, including a formula, drawing, pattern, compilation, including a customer list, program, device, method, technique or process that: (1) derives independent economic value, actual or potential, from not being generally known to and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use; **and** (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. The term includes data processing software by an agency under a licensing agreement prohibiting disclosure.

65 P.S. §67.102 (emphasis added).

The Office of Open Records has determined that a third party must establish a trade secret based upon factors established by the appellate courts, which include the following:

the extent to which the information is known outside of his business;
the extent to which the information is known by employees and others in the business;
the extent of measures taken to guard the secrecy of the information;
the value of the information to his business and to competitors;
the amount of effort or money expended in developing the information; and
the ease of difficulty with which the information could be properly acquired or duplicated by others.

See *Crum v. Bridgestone/Firestone North Amer. Tire*, 907 A.2d 578, 585 (Pa. Super. 2006).

The Office of Open Records also notes that with regard to "confidential proprietary information the standard is equally high and may only be established when the party asserting

protection shows that the information at issue is either 'commercial' or 'financial' and is privileged or confidential, and the disclosure ***would*** cause substantial competitive harm." (emphasis in original).

For more information regarding the RTKL, visit the Office of Open Records' website at www.openrecords.state.pa.us.

I-18 Debriefing Conferences.
Proposers whose proposals are not selected will be notified of the name of the selected Proposer and given the opportunity to be debriefed, at the Proposer's request. The Issuing Office will schedule the time and location of the debriefing. The Proposer will not be compared with other Proposers.

I-19 News Releases.
News releases pertaining to this project will not be made without prior Commission approval, and then only in coordination with the Issuing Office.

I-20 Commission Participation.
Unless specifically noted in this section, Proposers must provide all services to complete the identified work.

I-21 Cost Submittal.
The cost submittal shall be placed in a separately sealed envelope within the sealed proposal and kept separate from the technical submittal. **Failure to meet this requirement will result in disqualification of the proposal.**

I-22 Term of Contract.
The Commission intends that the term of the contract will commence on the Effective Date (as defined below) and will remain in effect for a period of one year. The Commission shall fix the Effective Date after the contract has been fully executed by the Contractor and by the Commission and all approvals required by Commission contracting procedures have been obtained.

I-23 Proposer's Representations and Authorizations.
Each Proposer by submitting its proposal understands, represents, and acknowledges that:

a. All information provided by, and representations made by, the Proposer in the proposal are material and important and will be relied upon by the Issuing Office in awarding the contract(s). Any misstatement, omission or misrepresentation shall be treated as fraudulent concealment from the Issuing Office of the true facts relating to the submission of this proposal. A misrepresentation shall be punishable under 18 Pa. C.S. 4904.

b. The price(s) and amount of this proposal have been arrived at independently and without consultation, communication or agreement with any other Proposer or potential Proposer.

c. Neither the price(s) nor the amount of the proposal, and neither the approximate price(s) nor the approximate amount of this proposal, have been disclosed to any other firm or person who is a Proposer or potential Proposer, and they will not be disclosed on or before the proposal submission deadline specified in the cover letter to this RFP.

d. No attempt has been made or will be made to induce any firm or person to refrain from submitting a proposal on the Contract, or to submit a proposal higher than this proposal, or to submit any intentionally high or noncompetitive proposal or other form of complementary proposal.

e. The proposal is made in good faith and not pursuant to any agreement or discussion with, or inducement from, any firm or person to submit a complementary or other noncompetitive proposal.

f. To the best knowledge of the person signing the proposal for the Proposer, the Proposer, its affiliates, subsidiaries, officers, directors, and employees are not currently under investigation by any governmental agency and have not in the last four (4) years been convicted or found liable for any act prohibited by State or Federal law in any jurisdiction, involving conspiracy or collusion with respect to bidding or proposing on any public contract, except as disclosed by the Proposer in its proposal.

g. To the best of the knowledge of the person signing the proposal for the Proposer and except as otherwise disclosed by the Proposer in its proposal, the Proposer has no outstanding, delinquent obligations to the Commonwealth including, but not limited to, any state tax liability not being contested on appeal or other obligation of the Proposer that is owed to the Commonwealth.

h. The Proposer is not currently under suspension or debarment by the Commonwealth, or any other state, or the federal government, and if the Proposer cannot certify, then it shall submit along with the proposal a written explanation of why such certification cannot be made.

i. The Proposer has not, under separate contract with the Issuing Office, made any recommendations to the Issuing Office concerning the need for the services described in the proposal or the specifications for the services described in the proposal.

j. Each Proposer, by submitting its proposal, authorizes all Commonwealth agencies to release to the Commission information related to liabilities to the Commonwealth including, but not limited to, taxes, unemployment compensation, and workers' compensation liabilities.

I-24 Insurance.

A. General Insurance Requirements

1. The Professional Services shall not commence until the Professional Service Contractor has obtained, at their own expense, all of the insurance as required hereunder and such insurance has been approved by the Commission; nor shall the Professional Service Contractor allow any Subcontractor to commence work on any Commission projects until all insurance required of the Subcontractor has been so obtained and approved by the Contractor. Approval of insurance required of the Professional Service Contractor will be granted only after submission to the Commission, original certificates of insurance signed by the representatives of the insurers or, at the Commission's request, certified copies of the required insurance policies.
2. The Professional Service Contractor shall require all Subcontractors to maintain during the term of the Contract Commercial General Liability Insurance, Business Auto Liability Insurance, Professional Liability Insurance (if applicable), Pollution Liability Insurance (if applicable), and Workers' Compensation and Employers Liability Insurance at the same limits required of Professional Service Contractor.
3. All insurance required herein, with the exception of the Professional / Errors and Omissions Liability Insurance shall be written on an "occurrence" basis and not a "claims-made" basis. For Professional Liability "claims-made" coverage:
    a. The retroactive date must be on or prior to the start of work under this contract; and
    b. The Subcontractor must purchase "tail coverage/an extended reporting period" or maintain coverage for a period of three years – the required completed operations period.
4. The Commission, its commissioners, agents, servants, employees and representatives shall be named as additional insured on the Contractor's liability (General Liability, Automobile Liability and Umbrella Liability insurance) insurance program with respect to the liability arising out of the Contractor's work (including products and completed operations as well as ongoing operations) and the certificate of insurance, or the certified policy, if required, must also state this. This coverage should be provided, along with evidence of such coverage, for a period of two years after completion of the project.
5. All insurance policies required hereunder shall be endorsed to provide that the policy is not subject to cancellation, non-renewal, or material reduction in coverage until thirty (30) days prior written notice has been given to the Owner.
6. Insurance provided to the Commission as specified herein shall be primary and non-contributory.
7. No acceptance and/or approval of any insurance by the Commission shall be construed as relieving or excusing the Professional Service Contractor or the Professional Service Contractor's Surety (if applicable) from any liability or obligation imposed upon either or both of them by provisions of this Contract.
8. Any deductibles or self-insured retention's of ($10,000) or greater shall be disclosed by the Professional Service Contractor, and are subject to Commissions written

approval. Any deductible or retention amounts elected by the Professional Service Contractor or imposed by the Professional Service Contractor's insurer(s) shall be the sole responsibility of the Professional Service Contractor.

9. All insurance companies shall have an AM Best's rating of A- or better and be licensed to do business in the State of Pennsylvania.
10. There shall be no liability upon the Commission, public officials, their employees, their authorized representatives, or agents either personally or as officials of the Commission in carrying out any of the provisions of the Contract nor in exercising any power or authority granted to them by or within the scope of the Contract, it being understood that in all such matters they act solely as agents and representatives of the Commission.
11. Waiver of Rights of Recovery and Waiver of Rights of Subrogation:
    a. The Contractor and subcontractors waive all rights of recovery against the Owner and all the additional insured's for loss or damage covered by any of the insurance maintained by the contractor or subcontractor.
    b. If any of the policies of insurance required under this contract require an endorsement to provide for the waiver of subrogation, then the named insured of such policies will cause them to be so endorsed.
12. Any type of insurance or any increase in limits of liability not described above which the contractor requires for its own protection or on account of statute shall be its own responsibility and at its own expense.

B. Professional Service Contractor Liability Insurance Requirements

- The Professional Service Contractor shall purchase the following insurance coverage's for the minimum limits specified below or required by law.

    - **Commercial General Liability** insurance for bodily injury, personal injury, and property damage including loss of use, etc. with minimum limits of:

$1,000,000	each occurrence;
$1,000,000	personal and advertising injury;
$2,000,000	general aggregate; and
$2,000,000	products/completed operation aggregate.

This insurance shall include coverage for all of the following

- Coverage is to be provided by the standard Commercial General Liability insurance policy ("Occurrence Form");
- General aggregate limit applying on a per project/ location basis;
- Liability arising from premises and operations;
- Liability arising from the actions of independent contractors;
- Contractual liability including protection for the Professional Service Contractor from bodily injury and property damage claims arising out of liability assumed under this Contract;

- Liability arising from the explosion, collapse or underground (XCU) hazards (If Applicable)
- Products/Completed Operations Coverage must be maintained for a period of at least two (2) years after final payment (including coverage for the Additional Insureds as set forth in these Insurance Requirements).

- **Business Auto Liability** insurance with a minimum limit of $1,000,000 per accident and including, but not limited to, coverage for all of the following:

  - Liability arising out of the ownership, maintenance or use of any auto;
  - Auto non-ownership and hired car coverage
  - Contractual Liability Coverage (including Liability for Employee Injury assumed under a Contract as provided in the standard ISO policy form)

- **Workers' Compensation** insurance with statutory benefits as required by any state or federal law, including standard "other states" coverage; employer's liability insurance with minimum limits of:

$1,000,000	each accident for bodily injury by accident;
$1,000,000	each employee for bodily injury by disease; and
$1,000,000	policy limit for bodily injury by disease.

  1. Including Waiver of Right to Recover from Others Endorsement (WC 00 0313) where permitted by state law.
  2. United States Longshore & Harbor Workers Act Coverage, where applicable; and
  3. Maritime Coverage under the Jones Act, where applicable.

- **Professional Liability:** Service Contractors (such as, but not limited to Architects, Engineers, Attorneys, Financial Advisors, Marketing Professionals, Physicians and Risk Management Consultants) shall provide professional liability and/or malpractice insurance with minimum limits of $1,000,000.

- **Umbrella Liability or Excess Liability** insurance with minimum limits of:

$1,000,000	per occurrence;
$1,000,000	aggregate for other than products/completed operations and auto liability; and
$1,000,000	products/completed operations aggregate.

Policy to apply excess of the Commercial General Liability (following form, Per Project / location), Commercial Automobile Liability and Employers Liability Coverage.

- **Crime Coverage:**

Contractor shall provide evidence of Comprehensive Crime Coverage in the amount of not less than $5,000,000 to include coverage for theft from The Pennsylvania Turnpike Commission by Service Provider's employees, agents or subcontractors. If on a loss discovered basis, this coverage will remain in place for at least 3 years following the completion of work

- **Pollution Liability (If Applicabl**e) Insurance

  - Occurrence/Claims Made Limit: $1,000,000 per project
  - Insurance to be maintained for the duration of the work for a period of two years thereafter
  - No Exclusions for Silica, Asbestos or Lead.
  - Include Mold Coverage for full policy limit of liability.
  -

- **Watercraft and Aircraft Liability (If Applicable):** If contractor utilizes any owned, used, leased, hired or borrowed watercraft or aircraft to complete their work in accordance with this Contract, the coverage shall be maintained.

Minimum Limits of Liability:

$2,000,000 Per Occurrence
$2,000,000 Aggregate

C. Indemnification

The Contractor shall protect, defend, indemnify and hold harmless the Commission, and their agents and employees from and against all liability (including liability for violation of any law or any common law duty), claims, damages, losses, and expenses including attorneys' fees arising in connection with, out of, or resulting from the performance of the work, provided that any such liability, claim, damage, loss or expense (i) is attributable to bodily injury, sickness, disease, or death, or to any statutory or regulatory rule designed to protect against such conditions, or to injury to or destruction of tangible property (other than the work itself), and including the loss of the use resulting there from, and (ii) is caused by or results from, in whole or in part, any act or omission of the Contractor, any Subcontractor, Sub-subcontractor(s), anyone direct or indirectly employed by any of them or anyone for whose acts any of them may be liable, regardless of whether or not it is also caused by or results from any act or omission of any party indemnified hereunder.

In any and all claims against the Commission or any of their agents or employees, by an employee of the Contractor, Subcontractor, or any Sub-subcontractor, or anyone directly or indirectly employed by any of them, or anyone for whose acts any of them may be liable, the indemnification obligation shall not be limited in any way by any limitation on the amount or type of damages, compensation or benefits payable by or for any Contractor, Subcontractor or any Sub-subcontractor under Workmen's Compensation Acts, Disability Benefits Acts, or other Employee.

I-25 Independent Capacity of Contractor

The parties to the Contract agree that the services performed by the Contractor under the terms of the Contract are performed as an independent Contractor. The Services performed by the Contractor are performed neither as an employee of the Commission nor as a partnership or joint venture between the Commission and the Contractor.

I-26 Compliance with Laws

The Contractor shall comply with all federal, state, and local laws applicable to its Services, including, but not limited to, all statutes, regulations and rules that are in effect as of the Effective Date of the Contract and shall procure at its expense all licenses and all permits necessary for the fulfillment of its obligation.

I-27 Inspection and Acceptance

Acceptance of Developed Materials will occur in accordance with a Deliverable Approval Plan submitted by the selected Proposer and approved by the Commission. Upon approval of the plan by the Commission, the Deliverable Approval Plan becomes part of the Contract.

For the purposes of this RFP and resulting contract(s), Developed Works or Developed Materials shall mean all documents, sketches, drawings, designs, works, papers, files, reports, computer programs, computer documentation, data, records, software, samples or any other literary works, works of authorship, or tangible material authored or prepared by selected Proposer in carrying out the obligations and services under the Contract, without limitation. The terms are used herein interchangeably.

I-28 Notice of Delays

Whenever the selected Proposer encounters any difficulty that delays or threatens to delay the timely performance of the Contract (including actual or potential labor disputes), the selected Proposer shall promptly give notice thereof in writing to the Commission stating all relevant information with respect thereto. Such notice shall not in any way constitute a basis for an extension of the delivery schedule or be construed as a waiver by the Commission of any rights or remedies to which it is entitled by law or pursuant to provisions of the Contract. Failure to give such notice, however, may be grounds for denial of any request for an extension of the delivery schedule because of such delay. If an extension of the delivery schedule is granted, it will be done consistent with Section I-29 (Changes).

I-29 Changes

At any time during the performance of the Contract, the Commission or the selected Proposer may request a change to the Contract. Contractor will make reasonable efforts to investigate the impact of the change request on the price, timetable, specifications, and other terms and conditions of the Contract. If the Commission and the selected Proposer agree on the results of the investigation and any necessary amendments to the Contract, the parties must complete and execute a change notice to modify the Contract and implement the change. The change request will be evidenced by an Agreement Amendment or Supplemental Agreement and a Notice to Proceed. No work may begin on the change request until the selected Proposer has received the Notice to Proceed. If the parties cannot agree upon the results of the investigation or the necessary amendments to the Contract, the change request will not be implemented.

Changes outside the scope of the Contract shall be accomplished through the Commission's normal procurement procedures, and may result in an amended Contract or a new contract. No payment will be made for services outside of the scope of the Contract for which no amendment has been executed, prior to the provision of the services.

I-30 Background Checks

The selected Proposer must, at its expense, arrange for a background check for each of its employees, as well as the employees of any of its subcontractors, who will have access to Commission I.T. facilities, either through on-site access or through remote access. Background checks are to be conducted via the Pennsylvania State Police Request for Criminal Record Check form and procedure found at http://www.portal.state.pa.us/portal/server.pt?open=512&objID=4451&PageID=458621&mode=2. The background check must be conducted prior to initial access and on an annual basis thereafter.

Before the Commission will permit access to the selected Proposer, the selected Proposer must provide written confirmation that the background checks have been conducted. If, at any time, it is discovered that an employee of the selected Proposer or an employee of a subcontractor of the selected Proposer has a criminal record that includes a felony or misdemeanor involving terroristic behavior, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility or which raises concerns about building, system or personal security or is otherwise job-related, the selected Proposer shall not assign that employee to any Commission facilities, shall remove any access privileges already given to the employee and shall not permit that employee remote access unless the Commission consents to the access, in writing, prior to the access. The Commission may withhold its consent in its sole discretion. Failure of the selected Proposer to comply with the terms of this Section on more than one occasion or the selected Proposer's failure to cure any single failure to the satisfaction of the Commission may result in the Contractor being deemed in default of its Contract.

The Commission specifically reserves the right of the Commission to conduct or require background checks over and above that described herein.

I-31 Confidentiality

The selected proposer agrees to protect the confidentiality of the Commission's Confidential Information. The Commission agrees to protect the confidentiality of selected Contractor's Confidential Information. In order for information to be deemed confidential, the party claiming confidentiality must designate the information as "confidential" in such a way as to give notice to the other party (notice may be communicated by describing the information, and the specifications around its use or disclosure, in the Statement of Work). Neither party may assert that information owned by the other party is such party's confidential information. The parties agree that such confidential information shall not be copied, in whole or in part, or used or disclosed except when essential for authorized activities under the Contract and, in the case of disclosure, where the recipient of the Confidential Information has agreed to be bound by confidentiality requirements no less restrictive than those set forth herein. Each copy of such Confidential Information shall be marked by the party making the copy with any notices appearing in the original. Upon termination or cancellation of the Contract or any license

granted hereunder, the receiving party will return to the disclosing party all copies of the Confidential Information in the receiving party's possession, other than one copy, which may be maintained for archival purposes only, and which will remain subject to the Contract's security, privacy, data retention/destruction and confidentiality provisions (all of which shall survive the expiration of the Contract). Both parties agree that a material breach of these requirements may, and at the discretion of the non-breaching party, result in termination for default, in addition to other remedies available to the non-breaching party.

Insofar as information is not otherwise protected by law or regulation, the obligations stated in this Section do not apply to information:

1. already known to the recipient at the time of disclosure other than through the contractual relationship;
2. independently generated by the recipient and not derived from the information supplied by the disclosing party;
3. known or available to the public, except where such knowledge or availability is the result of unauthorized disclosure by the recipient of the proprietary information;
4. disclosed to the recipient without a similar restriction by a third party who has the right to make such disclosure; or
5. required to be disclosed by the recipient by law, regulation, court order, or other legal process.

There shall be no restriction with respect to the use or disclosure of any ideas, concepts, know-how, or data processing techniques developed alone or jointly with the Commission in connection with services provided to the Commission under the Contract.

The Contractor shall use the following process when submitting information to the Commission it believes to be confidential and/or proprietary information or trade secrets:

1. Prepare an un-redacted version of the appropriate document, and
2. Prepare a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret, and
3. Prepare a signed written statement that states: (i) the attached document contains confidential or proprietary information or trade secrets; (ii) the Contractor is submitting the document in both redacted and un-redacted format in accordance with 65 P.S. § 67.707(b); and (iii) the Contractor is requesting that the document be considered exempt under 65 P.S. § 67.708(b)(11) from public records requests.
4. Submit the two documents along with the signed written statement to the Commission.

I-32 Software Installation.

The selected Provider shall not install any software or monitoring tools on the Commission's equipment without the Commission's written consent to do so and then, shall only install such software or monitoring tools in coordination with the Commission.

I-33 Virus, Malicious, Mischievous or Destructive Programming.

Notwithstanding any other provision in the Contract to the contrary, if the Contractor or any of its employees, subcontractors or consultants introduces a virus or malicious, mischievous or destructive programming into the Commission's software or computer networks and provided further that the Commission can demonstrate that the virus or malicious, mischievous or destructive programming was introduced by the Contractor or any of its employees, subcontractors or consultants, the Contractor shall be liable for any damage to any data and/or software owned or licensed by the Commission. The Contractor shall be liable for any damages incurred by the Commission including, but not limited to, the expenditure of Commission funds to eliminate or remove a computer virus or malicious, mischievous or destructive programming that result from the Contractor's failure to take proactive measures to keep virus or malicious, mischievous or destructive programming from originating from the Contractor, its servants, agents or employees through appropriate firewalls and maintenance of anti-virus software and software security updates (such as operating systems security patches, etc.). In the event of destruction or modification of software, the selected Proposer shall eliminate the virus, malicious, mischievous or destructive programming, restore the Commission's software, and be liable to the Commission for any resulting damages.

The Contractor shall perform a security scan on any software or computer program developed by the Contractor or its subcontractors that may come in contact with the Commission's software or computer networks. The Contractor shall perform such security scan prior to introducing any such software or computer program into any of the Commission's computing environments. The results of these security scans will be provided to the Commission prior to installation. The Commission may perform, at its discretion, additional security scans on any software or computer program prior to installing in a Commission environment as listed above.

The Commission may, at any time, audit, by a means deemed appropriate by the Commission, any computing devices being used by representatives of the Contractor to provide services to the Commission that will be connected to a Commission's network for the sole purpose of determining whether those devices have anti-virus software with current virus signature files and the current minimum operating system patches or workarounds have been installed. Devices found to be out of compliance will immediately be disconnected and will not be permitted to connect or reconnect to the Commission's network until the proper installations have been made. The Commission shall not install any software or monitoring tools on the Contractor's equipment without the Contractor's written consent to do so.

I-34 Contract Construction

The provisions of the Contract shall be construed in accordance with the provisions of all applicable laws and regulations of the Commonwealth of Pennsylvania. However, by executing the Contract, the selected Proposer agrees that it has and will continue to abide by the intellectual property laws of the United States of America.

I-35 Ownership Rights

A. Ownership of Properties

All “Developed Works” shall be owned by the Commission. All software owned by the Commission or its licensors (“Commission Software”) as of the Effective Date, shall be and shall remain the exclusive property of the Commission or its licensors, and the Contractor shall acquire no rights or interests in the Commission Software or Tools or that of its licensors by virtue of the Contract except as described in this Section or in another provision set forth in the Contract. The Contractor shall not use any Commission Software, Commission Tools or software or tools of its licensors for any purpose other than for completion of work to be performed under the Contract. In the use of Commission Software, Commission Tools or software or tools of its licensors, the selected Proposer will be bound by the confidentiality provisions of the Contract.

B. Use of Contractor-Owned Software

All software owned by the Contractor (Contractor Software) and tools owned by the Contractor (Contractor Tools, as defined below) prior to the Effective Date of the Contract shall be and shall remain the exclusive property of the Contractor. The Commission shall acquire no rights or interests in the Contractor Software or the Contractor Tools by virtue of the Contract except as set forth in this Section.

C. Definition of Contractor Tools

Contractor Tools is defined as any tools, both in object code and source code form, which the Contractor has previously developed, or which Contractor independently develops or licenses from a third party, excluding any tools that Contractor creates pursuant to the Contract. Contractor Tools includes but is not limited to, methodologies, information, concepts, toolbars for maneuvering between pages, search engines, JAVA applets, and ActiveX controls.

D. Required Reports, Records and Inventory of Contractor Tools and Contractor Software

The Contractor must provide a list of all Contractor Tools and Contractor Software to be delivered in connection with the deliverables or Developed Materials prior to commencing any work under the Contract. Contractor must also provide a list of all other Contractor Tools and Contractor Software intended to be used by Contractor to provide the services under the Contract but will not become part of or necessary for the use of the Developed Materials. All Contractor Tools and Contractor Software necessary to use deliverables or Developed Materials shall be delivered to the Commission along with the license set forth below. Contractor may amend these lists from time to time while the Contract is being carried out or upon its completion. In the event that the Contractor fails to list a Contractor Tool, but can demonstrate that such tool was independently developed by Contractor prior to the Contract on which it was used, The Contractor shall nevertheless retain complete ownership of such Contractor Tool that is necessary to use the deliverables or Developed Materials, provided that notice is given to the Commission prior to its use on the Contract. Any Contractor Tools or Contractor Software not included on the lists will be deemed to have been created under the Contract.

As part of its response to a RFP, the Contractor will provide a list of all software and tools that are commercially available and which are required to support the deliverables or Developed Materials.

E. Expiration or Termination Non Exclusive License Grant—Non-Commercial Contractor Tools and Software

Upon the expiration or termination for any reason of the Contractor's obligation to provide the Services under the Contract, and at the request of Commission, the Contractor shall (i) grant to Commission a paid-up, nonexclusive, nontransferable license to use, modify, prepare derivative works and unless the Commission terminates the Contract without cause, grant to third parties engaged by the Commision the right to use, modify, and prepare derivative works based upon all or any portion of the non-commercially available Contractor Software and the non-commercially available Contractor Tools owned by Contractor and used by Contractor in connection with the Services, the foregoing rights being granted to the extent reasonably necessary to facilitate the Commission's or such third party's completion of and maintenance of the Services to be provided by the Contractor under the Contract immediately prior to such expiration or termination and (ii) deliver to the Commission the object code version of such non-commercially available Contractor Software and such non-commercially available Contractor Tools in the form used by Contractor in connection with the Services immediately prior to such expiration or termination to allow the Commission to complete and maintain such work. If Commission enters into a contract that allows for the use of the Contractor Software or Contractor Tools for which a license is granted in this section, the Commission will include a provision in that contract that limits the use of the Contractor Software or Contractor Tools as delineated in this Section.

F. Rules of Usage for Developed Works

If Developed Works modify, improve, or enhance application software programs or other materials generally licensed by the Contractor, then such Developed Works shall be the property of the Contractor, and the Contractor hereby grants Commission an irrevocable, nonexclusive, worldwide, fully paid-up license (to include source code and relevant documentation) in perpetuity to use, modify, execute, reproduce, display, perform, prepare derivative works from and distribute, within the Commission, of such Developed Works.

When the Developed Work is a report provided by a research company that was provided under the Contract, but which was not developed specifically for the Commission under the Contract, the ownership of the Developed Work will remain with the Contractor, provided, however, that the Commission has the right to copy and distribute the Developed Work within the Commission.

G. Copyright Ownership

Developed Works developed as part of the Scope of Work for the Project, including Developed Works developed by Subcontractors, are the sole and exclusive property of the Commission and shall be considered "works made for hire" under the United States Copyright Act of 1976, as amended, 17 United States Code. In the event that the Developed Works do not fall within the specifically enumerated works that constitute works made for hire under the

United States copyright laws, Contractor agrees to assign and, upon their authorship or creation, expressly and automatically assigns all copyright interests, proprietary rights, trade secrets, and other right, title, and interest in and to such Developed Works to the Commission. Contractor further agrees that it will have its Subcontractors assign, and upon their authorship or creation, expressly and automatically assign all copyright interest, proprietary rights, trade secrets, and other right, title, and interest in and to the Developed Works to the Commission. The Commission shall have all rights accorded an owner of copyright under the United States copyright laws including, but not limited to, the exclusive right to reproduce the Developed Works in multiple copies, the right to distribute, copies by sales or other transfers, the right to register all copyrights in its own name as author in the United States and in foreign countries, the right to prepare derivative works based upon the Developed Works and the right to display the Developed Works. The Contractor further agrees that it will include this requirement in any subcontractor or other agreement with third parties who in any way participate in the creation or development of Developed Works. Upon completion or termination of the Contract, Developed Works shall immediately be delivered by Contractor to the Commission. Contractor warrants that the Developed Works are original and do not infringe any copyright, patent, trademark, or other intellectual property right of any third party and are in conformance with the intellectual property laws of the United States.

The Contractor shall not use any computer program, code, or any works developed by or for Contractor independently of the Contract ("Pre-Existing Materials") in the performance of the Services under the Contract, without the express written consent of the Commission. Any Pre-Existing Materials used by Contractor for performance of Services under the Contract without Commission consent shall be deemed to be Developed Works as that term is used in this Section. In the event that Commission provides such consent, Contractor shall retain any and all rights in such Pre-Existing Materials.

H. Usage Rights for Know-How and Technical Information

Either Party, in the ordinary course of conducting business, may use any ideas, concepts, know-how, methodologies, processes, components, technologies, algorithms, designs, modules or techniques not otherwise covered by this Section relating to the Services which Contractor or Commission (alone or jointly with the Commission) develops or learns in connection with Contractor's provision of Services to the Commission under the Contract.

I. Commission Intellectual Property Protection

The Contractor acknowledges the Commission's exclusive right, title and interest, including without limitation copyright and trademark rights, in and to Commission Software, Commission Tools and the Developed Works developed under the provisions of this Section, shall not in any way, at any time, directly or indirectly, do or cause to be done any act or thing contesting or in any way impairing or tending to impair any part of said right, title, and interest, and shall not use or disclose the Commission Software, Commission Tools, or the Developed Works without Commission's written consent, which consent may be withheld by the Commission for any reason. Further, the Contractor shall not in any manner represent that the Contractor has any ownership interest in the Commission Software, Commission Tools, or the Developed Works. This provision is a material part of this Section.

J. Contractor Intellectual Property Protection

The Commission acknowledges that it has no ownership rights in the Contractor Software or Contractor Tools other than those set forth in the Contract, or as may be otherwise granted in writing.

K. Source Code and Escrow Items Obligations

Simultaneously with delivery of the Developed Works to Commission, the Contractor shall deliver a true, accurate and complete copy of all source codes relating to the Developed Works. To the extent that the Developed Works include application software or other materials generally licensed by the Contractor, then the source code shall be placed in escrow, subject to the terms and conditions of an Escrow Agreement to be executed by the Parties and an Escrow Agent that is acceptable to the Commission.

L. Contractor's Copyright Notice Obligations

Contractor will affix the following Copyright Notice to the Developed Works developed under this Section and all accompanying documentation: "Copyright © [year] by the Pennsylvania Turnpike Commission. All Rights Reserved." This notice shall appear on all tangible versions of the Developed Works delivered under the Contract and any associated documentation. It shall also be programmed into any and all Developed Works delivered hereunder so that it appears at the beginning of all visual displays of such Developed Works.

M. Commercial Software

If a product or deliverable under the Contract is commercially available software or requires commercially available software for use and the Contractor is the licensor of the software, Contractor shall enter into a license agreement with the Commission. If a product or deliverable under the Contract is commercially available software or requires commercially available software for use and the Contractor is not the licensor of the software, the Contractor hereby agrees that, before it incorporates such software into a deliverable, Contractor will inform the licensor of the software that it will be required to enter into a software license agreement with the Commission.

I-36 Publication Rights and/or Copyrights

Except as otherwise provided in Part I-35 (Ownership Rights), the Contractor shall not publish any of the results of the work without the written permission of the Commission. The publication shall include the following statement: "The opinions, findings, and conclusions expressed in this publication are those of the author and not necessarily those of the Pennsylvania Turnpike Commission." The Contractor shall not include in the documentation any copyrighted matter, unless the Contractor provides the Commission with written permission of the copyright owner.

Except as otherwise provided in Part I-35(Ownership Rights) and the confidentiality provisions of Part I-31 (Confidentiality), the Commission shall have unrestricted authority to reproduce, distribute, and use any submitted report or data designed or developed and delivered to the Commission as part of the performance of the Contract.

Rights and obligations of the parties under this Section survive the termination of the Contract.

I-37 Liquidated Damages

By accepting the Contract, the Contractor agrees to the delivery and acceptance requirements of the Contract. If a Contract schedule is not met, the delay will interfere with the Commission's program. In the event of any such delay, it would be impractical and extremely difficult to establish the actual damage for which the Contractor is the material cause. The Commission and the Contractor therefore agree that, in the event of any such delay the amount of damage shall be the amount set forth in this Section and agree that the Contractor shall pay such amount as liquidated damages, not as a penalty. Such liquidated damages are in lieu of all other damages arising from such delay.

The Commission and Contractor agree that the Deliverables identified in the Payment Schedule set forth in the Contract as "Major Deliverables" (the "Major Deliverables") shall be those for which liquidated damages shall be applicable in the event of delay of their completion beyond the delivery date specified in the Contract. If Major Deliverables are not identified in the Contract, liquidated damages shall apply to the total value of the Contract.

The amount of liquidated damages for any such Major Deliverable not completed by the deliverable schedule set out in the Contract shall be three-tenths of a percent (0.3%) of the price of the specifically identified Major Deliverable for each calendar day following the scheduled completion date of such Major Deliverable. Liquidated damages shall be assessed each calendar day until the date on which the Contractor completes such Major Deliverable, up to a maximum of thirty (30) calendar days. Contractor may recoup the total amount of liquidated damages assessed against previous Major Deliverables if the Contractor accelerates progress towards future Major Deliverables and meets the final project completion date set out in the Contract.

If, at the end of the thirty (30) day period specified above, the Contractor has not met the schedule for completion of the Major Deliverable, then the Commission, at no additional expense and at its option, may either (i) immediately terminate the Contract and all software, documentation, reports, Developed Materials and any other materials provided for or created for the Commission as a result of the Contract shall be given to the Commission, and the Commission shall be entitled to such other remedies afforded in the Contract or (ii) order the Contractor to continue with no decrease in effort until the work is completed in accordance with the Contract and accepted by the Commission or until the Commission terminates the Contract. If the Contract is continued, any liquidated damages will also continue until the work is completed.

At the end of the Contract term, or at such other time(s) as identified in the Contract, liquidated damages shall be paid by the Contractor and collected by the Commission by deducting them from the invoices submitted under the Contract or any other contract Contractor has with the Commission, by collecting them through the performance security, if any, or by billing the Contractor as a separate item.

To the extent that the delay is caused by the Commission, no liquidated damages will be applied.

If the delays are caused by the default of a Subcontractor, and if such default arises out of causes beyond the control of both the Contractor and Subcontractor, and without their fault or negligence, the Contractor shall not be liable for liquidated damages for delays, unless the supplies or services to be furnished by the Subcontractor were obtainable from other sources in sufficient time to permit the Contractor to meet the required performance schedule.

I-38 Force Majeure

Neither party will incur any liability to the other if its performance of any obligation under the Contract is prevented or delayed by causes beyond its control and without the fault or negligence of either party. Causes beyond a party's control may include, but aren't limited to, acts of God or war, changes in controlling law, regulations, orders or the requirements of any governmental entity, civil disorders, fire, epidemics and quarantines, general strikes throughout the trade, and freight embargoes.

The Contractor shall notify the Commission orally within five (5) days and in writing within ten (10) days of the date on which the Contractor becomes aware, or should have reasonably become aware, that such cause would prevent or delay its performance. Such notification shall (i) describe fully such cause(s) and its effect on performance, (ii) state whether performance under the contract is prevented or delayed and (iii) if performance is delayed, state a reasonable estimate of the duration of the delay. The Contractor shall have the burden of proving that such cause(s) delayed or prevented its performance despite its diligent efforts to perform and shall produce such supporting documentation as the Commission may reasonably request. After receipt of such notification, the Commission may elect to cancel the Contract or to extend the time for performance as reasonably necessary to compensate for the Contractor's delay.

In the event of a declared emergency by competent governmental authorities, the Commission by notice to the Contractor, may suspend all or a portion of the Contract.

PART II—INFORMATION REQUIRED FROM PROPOSERS

Proposals must be submitted in the format, including heading descriptions, outlined below. To be considered, the proposal must respond to all requirements in this part of the RFP. Any other information thought to be relevant, but not applicable to the enumerated categories, should be provided as an appendix to the proposal. Each proposal shall consist of two (2) separately sealed submittals. The submittals are as follows: (i) Technical Submittal, in response to Part II-1 hereof; (ii) Cost Submittal, in response to Part II-2 hereof.

The Commission reserves the right to request additional information which, in the Commission's opinion, is necessary to assure that the Proposer's competence, number of qualified employees, business organization, and financial resources are adequate to perform according to the RFP.

The Commission may make such investigations as deemed necessary to determine the ability of the Proposer to perform the work, and the Proposer shall furnish to the Issuing Office all such information and data for this purpose as requested by the Commission. The Commission reserves the right to reject any proposal if the evidence submitted by, or investigation of, such Proposer fails to satisfy the Commission that such Proposer is properly qualified to carry out the obligations of the agreement and to complete the work specified.

For Proposers responding with a combined Lot 1 & 2 proposal, sections II-1 A, B, C, and D below should be described once while sections II-1, E, F, G and H should be clearly grouped and described by Lot.

II-1 Technical Submittal.

A. Title Page

Show the name of your firm, Federal I.D. number, address, name of contact person, contact person's email and telephone number date and the subject: REQUEST FOR SAP ERP ASSESSMENT LOT 1, REQUEST FOR INFORMATION SECURITY PROGRAM ASSESSMENT LOT 2 or REQUEST FOR SAP ERP AND INFORMATION SECURITY PROGRAM ASSESSMENTS LOTS 1 & 2 as appropriate.

B. Table of Contents

Include a clear identification of the material by section and by page number.

C. Cover Letter and Executive Summary

This letter must be signed by an individual who is authorized to negotiate terms, render binding decisions and commit your firm's resources.

Summarize your understanding of our organization, your understanding of the work to be done and make a positive commitment to perform the work necessary. This section should summarize the key points of your submittal. (Limit to two pages.)

D. Firm Overview

Provide a brief history and description of your firm's business organization and its I.T. consulting services expertise and experience as it relates to the requirements discussed in Part IV of this RFP. Include the location of offices and the number and types of I.T. consultants or other relevant professional staff in each office. Discuss your firm's presence in and commitment to the Commonwealth of Pennsylvania. Include a discussion of the specific expertise and services that distinguish your firm.

E. Personnel

described in Section IV of this RFP. Specifically identify the primary person(s) who will be responsible for managing the relationship with the Commission during this endeavor. Proposer must submit a current resume for all proposed staff listing relevant experience and applicable professional affiliations.

F. Relevant Experience and Expertise

Provide a narrative statement regarding your consulting services expertise and experience as it relates to Part IV of this RFP. Additionally include a statement regarding your understanding of the requirements as outlined in this RFP and your ability to provide consulting services in accordance with the same.

Describe your firm's experience in providing similar assessment consulting services to other clients, especially other governmental entities and/or similar public/private sector transportation organizations. Describe the business practices that enable you to complete these tasks in an efficient, timely and, at times, expeditious manner.

Provide a list of three references of clients for which your firm has performed similar work, as described in this RFP, within the past three years.

Include a statement regarding any other specialized I.T. consulting services your firm may offer.

G. Approach

Provide a description of the proposed approach/methodology that you will follow in the assessment along with a project plan and realistic timeline that identifies the phases and tasks required to complete the assessment. Include in this section the deliverables and reports the will be provided, the project controls that will be used, and the tasks that will be performed.

Note: The Commission is interested in conducting the assessment as expeditiously as possible and would favor an approach that moves aggressively to complete the assessment

while still providing a thorough assessment that fully meets all of the requirements of the RFP.

Provide a description of all of the deliverables that you will provide as an output of the assessment, including samples and, at a minimum, a table of contents for each deliverable.

Provide relevant samples of deliverables from similar assessment projects that your firm was primarily responsible for producing.

H. Commitment to Diversity and Inclusion

The Turnpike Commission is committed to the inclusion of disadvantaged, minority, and woman firms in contracting opportunities. Responding firms shall clearly identify DBE/MBE/WBE firms, expected to participate in the Contract, in their Proposal. Proposed DBE/MBE/WBE firms must be certified by the Pennsylvania Unified Certification Program (www.paucp.com) at the time of the submission of the proposal. The utilization of disadvantaged, minority and women-owned businesses are encouraged and will be considered a factor in the evaluation determination.

II-2 Cost Submittal.

The information requested in this section shall constitute your cost submittal. **THE COST SUBMITTAL SHALL BE PLACED IN A SEPARATE SEALED ENVELOPE WITHIN THE SEALED PROPOSAL AND ON A CD-ROM, SEPARATE FROM THE TECHNICAL SUBMITTAL.**

Proposers should **not** include any assumptions in their cost submittals. If the proposer includes assumptions in its cost submittal, the Issuing Office may reject the proposal. Proposers should direct in writing to the Issuing Office pursuant to Part I-9 (Questions and Answers.) of this RFP any questions about whether a cost or other component is included or applies. All Proposers will then have the benefit of the Issuing Office's written answer so that all proposals are submitted on the same basis.

1. Title Page

Show the name of your firm, Federal I.D. number, address, telephone number, name of contact person, date and the subject: REQUEST FOR SAP ERP ASSESSMENT LOT 1, REQUEST FOR INFORMATION SECURITY PROGRAM ASSESSMENT LOT 2 or REQUEST FOR SAP ERP AND INFORMATION SECURITY PROGRAM ASSESSMENTS LOTS 1 & 2 as appropriate.

Cost Letter

This letter should summarize the Respondent's understanding of the work to be done and the Proposer's total fixed-price cost for performing the work necessary to successfully meet the requirements of the RFP. The Respondent should also identify the percentage of total cost that is associated with work to be performed by D/M/WBE firms.

The Proposer must attach to the Cost letter a table that identifies the Resources (by position) that will be devoted to the effort, the average loaded rate for those resources and the number of hours each will devote to the effort. The table must also identify any other direct costs that went into calculating the Proposer's cost. The sum of the loaded rates times the number of hours for each position, plus the other direct costs must equal the total fixed price cost identified in the Cost letter. Proposers should use Appendix B (Cost Breakdown) to provide this information.

Any costs not provided in the cost proposal will be assumed as no charge to the Commission.

The Contractor shall only perform work on the Contract after the Effective Date is affixed and the fully-executed contract sent to the selected Proposer. The Commission shall issue a written Notice to Proceed to the selected Proposer authorizing the work to begin on a date which is on or after the Effective Date. The Contractor shall not start the performance of any work prior to the date set forth in the Notice of Proceed and the Commission shall not be liable to pay the Contractor for any service or work performed or expenses incurred before the date set forth in the Notice to Proceed. No Commission employee has the authority to verbally direct the commencement of any work under the Contract.

PART III—CRITERIA FOR SELECTION

III-1 Mandatory Responsiveness Requirements.

To be eligible for selection, a proposal shall be (a) timely received from a Proposer; (b) properly signed by the Proposer; and (c) formatted such that all cost data is kept separate from and not included in the Technical Submittal.

III-2 Proposal Evaluation.

Proposals will be reviewed, evaluated, and rated by a Technical Evaluation Team (TET) of qualified personnel based on the evaluation criteria listed below. The TET will present the evaluations to the Professional Services Procurement Committee (PSPC). The PSPC will review the TET's evaluation and provide the Commission with the firm(s) determined to be highly recommended for this assignment.

The Commission will select the most highly qualified firm for the assignment or the firm whose proposal is determined to be most advantageous to the Commission by considering the TET's evaluation and the PSPC's determination as to each firm's rating. In making the PSPC's determination and the Commission's decision, additional selection factors may be considered taking into account the estimated value, scope, complexity and professional nature of the services to be rendered and any other relevant circumstances. Additional selection factors may include, when applicable, the following: geographic location and proximity of the firm, firm's Pennsylvania presence or utilization of Pennsylvania employees for the assignment; equitable distribution of work; diversity inclusion; and any other relevant factors as determined as appropriate by the Commission.

Award will only be made to a Proposer determined to be responsive and responsible in accordance with Commonwealth Management Directive 215.9, Contractor Responsibility Program.

III-3 Evaluation Criteria.

The following criteria will be used, in order of relative importance from the highest to the lowest, in evaluating each proposal. Respondents should explicitly address each of these evaluation criteria in its response.

1. Proposer and Personnel Qualifications and Experience
    a. Proposer's relevant experience and expertise in conducting I.T. assessments as it relates to the requirements discussed in Part IV of this RFP.
    b. Qualifications, experience and competency of professional personnel who will be assigned to the contract by the Proposer including tenure with firm, length of time in the industry and type of experience.
    c. Financial ability of the Proposer to undertake a project of this size.
    d. Response of references.

2. Approach

a. Understanding of the Commission's needs and scope of work.
b. Soundness of proposed approach, methodology, and deliverables for conducting I.T. assessments as it relates to the requirements discussed in Part IV of this RFP.
c. Responsiveness to the Commissions desire for expeditious timeline for completion.
d. Quality, completeness and applicability of sample deliverables provided.
e. Responsiveness, organization, and clarity of Proposal.

3. Cost.

   While this area may be weighted heavily, it will not normally be the deciding factor in the selection process. The Commission reserves the right to select a proposal based upon all the factors listed above, and will not necessarily choose the firm offering the best price. The Commission will select the firm with the proposal that best meets its needs, at the sole discretion of the Commission.

4. Disadvantaged, Minority and Women Business Enterprise (D/M/WBE)

   This refers to the inclusion of D/M/WBE firms, as described in Part II-1 H, and the extent to which they are expected to participate in the Contract. Participation will be measured in terms of total dollars committed or percentage of total contract amount to certified D/M/WBE firms.

PART IV—WORK STATEMENT

IV-1 General Objectives.

To meet the I.T. consulting services needs of the Commission as they relate to specific Commission programs, projects, initiatives and issues.

IV-2 Nature and Scope of the Project.

A. SAP ERP ASSESSMENT LOT 1

In May of 2006, the Commission selected SAP as its Enterprise Resource Planning (ERP) system to address the challenge of replacing its existing disparate and obsolete business systems. The Commission's SAP ERP system was implemented in two major phases over a 21-month period and has been in full production operation since March of 2008.

The Commission is soliciting proposals from qualified I.T. consulting firms for the purpose of conducting an overall assessment of the Commission's SAP Enterprise Resource Management (ERP) system and system environment. For detailed current and historical statistical information about the Commission's SAP system and system environment, please see Appendix A: SAP System Summary.

B. INFORMATION SECURITY PROGRAM ASSESSMENT LOT 2

The Commission is soliciting proposals from qualified I.T. consulting firms for the purpose of conducting an overall assessment of the Commission's Information Security Program.

The Commission's computing environment primarily uses Microsoft and Cisco products, with VMWare for virtualization, HP Servers, and NetApp Storage. There are approximately 200 routers, 500 switches, 500 subnets, 1100 desktop/laptop computers, and approximately 9100 IP addresses in use.

The PTC interacts with between 30 and 40 business partners through site-to-site tunneling, co-located equipment, or by performing regular file transfers. In addition to the PATurnpike.com Internet site, the Commission has various public facing applications that are hosted in our De-Militarized Zone (DMZ) or by third party vendors, including, Outlook Web Access, Activesync, Virtual Desktop Interface, Secure File Transfer Protocol (SFTP), and EZPass TagTeller.

Various security related tools are in use to protect the network including, vulnerability scanning tools, Security Information and Event Management (SIEM) tools, web filtering tools, video management tools, and anti-malware tools.

IV-3 Requirements.

A. SAP ERP ASSESSMENT LOT 1

The Commission would like to have an assessment performed on its SAP ERP system and system environment that addresses at least the following areas:

1. An assessment of the original baseline implementation of the system that includes, at a minimum, the following:
   a. Assess whether or not the Commission's original SAP ERP implementation goals were achieved and, if not, what the gaps or shortcomings are.
   b. Compare and contrast the Commission's SAP system implementation to other SAP ERP system implementations of similar size, scope and complexity. Provide an overall assessment of how the Commission's SAP system implementation compares with other similar SAP ERP projects including a comparison of system implementation costs and system support and maintenance costs. The Proposer must identify the organizations used for comparisons by name or with sufficient descriptive information to assure the Commission that the organizations and implementations are of similar size, scope and complexity.
2. An assessment of the current status and health of the system that includes, at a minimum, the following:
   a. Assess the current status and health of the functional and technical components of the Commission's SAP ERP environment and identify any issues, gaps or shortcomings. Identify options to remedy any issues, gaps or shortcomings found including benefits and disadvantages to each option.
   b. Assess how the Commission uses the SAP ERP system to support key business processes and compare the Commission's use of the system with industry best practices. Identify any gaps, issues or shortcomings.
   c. Assess whether or not the Commission is utilizing the system to its fullest potential and identify options for enhancements or improvements including benefits and disadvantages to each option.
   d. An assessment of the policies, practices and procedures of the SAP support organization, including project management, change management, incident response, new feature implementation methodologies, and maintenance and upgrade processes and procedures. Identify any gaps, issues or shortcomings.
   e. An assessment of the SAP system environment including hardware and database infrastructure and performance. Identify any gaps, issues or shortcomings.
3. An assessment of the current organizational support structure for the system that includes, at a minimum, the following:
   a. Assess the current organizational support structure that is in place, contrasting it against the size, scope and complexity of the system, with specific consideration to structure, complement and compensation. Identify any issues, gaps or shortcomings and identify options to remedy including benefits and disadvantages to each option.
   b. Assess the current skills and competencies of the existing support staff for the SAP system. Identify any issues, gaps or shortcomings and options to address them.

B. INFORMATION SECURITY PROGRAM ASSESSMENT LOT 2

The Commission would like to have an assessment performed on its Information Security Program, using industry best practices and guidelines such as NIST Security related Special Publications and ISO 27000, which addresses at least the following areas:

- Current information security policies, practices and procedures;
- Current information security technologies and tools;
- Information security staff skills and competencies and the information security organization staffing model.

Emphasis should be placed on, but not limited to:

1. The Commission's boundary defenses, including:
    a. Internal/external network penetration testing. Scans must be coordinated with the Commission's staff and must not impact production capabilities of systems and networks,
    b. Business Partner Connectivity,
    c. Firewall rule set review,
    d. DMZ;
2. The Commission's data loss prevention program;
3. The Commission's Security Information Event Management (SIEM) program including monitoring/log review effectiveness and Incident Response (SIRT) processes and procedures;
4. PTC's access control program, including:
    a. Password management,
    b. Segregation of duties,
    c. Privileged users,
    d. Remote access,
    e. Wireless access; and
5. The Commission's web application security.

Because of the nature of Information Security Program Assessments, the selected Proposer will have access to Commission Confidential Information associated with hardware and system configurations and settings, network topologies, hardware and software specifications, and identified vulnerabilities and may gain access to Confidential or Sensitive Information in Commission files and databases, which it shall keep confidential.

APPENDIX A—SAP SYSTEM SUMMARY

See attached Appendix A (Adobe Acrobat PDF file format)

APPENDIX B—COST BREAKDOWN

See attached Appendix B (Excel Spreadsheet).

APPENDIX C—PROPOSAL COVER SHEET

See attached Appendix C (Word Document).

Addendum No. 1

RFP # 13-10340-3950

SAP ERP SYSTEM AND INFORMATION SECURITY PROGRAM ASSESSMENTS

Prospective Respondents: You are hereby notified of the following information in regard to the referenced RFP:

REVISIONS

1. On Page 23, Part II of the RFP, Section II-1, E, the language has been revised to read as follows:

E. Personnel
Provide the names, proposed roles, background and experience, current professional licenses, office location and availability of the consulting personnel that would perform the assessment consulting services as described in Section IV of this RFP. Specifically identify the primary person(s) who will be responsible for managing the relationship with the Commission during this endeavor. Proposer must submit a current resume for all proposed staff listing relevant experience and applicable professional affiliations.

2. On Page 3, Part I of the RFP, Section I-12, the language has been revised to read as follows:

I-12 Proposals.
To be considered, Proposers should submit a complete response to this RFP, using the format provided in PART II. Each proposal should be submitted in ~~five (5)~~ six (6) hard copies of the Technical Submittal and ~~five (5)~~ six (6) hard copies of the Cost Submittal.

3. The response date referenced in Part I-11 of the RFP has been extended and revised as follows:

I-11 Response.
To be considered, proposals must be delivered to the Pennsylvania Turnpike Commission's Contracts Administration Department, Attention: Wanda Metzger, **on or before 12:00 PM local time on ~~Tuesday, February 5, 2013~~ Thursday, February 28, 2013.**

QUESTIONS & ANSWERS

The questions submitted in response to the above referenced RFP up to January 17, 2013, will be answered in another addendum to be posted at a later date.

All other terms, conditions and requirements of the original RFP dated January 7, 2013 remain unchanged unless modified by this Addendum.

Addendum No. 2

RFP # 13-10340-3950

SAP ERP SYSTEM AND INFORMATION SECURITY PROGRAM ASSESSMENTS

Prospective Respondents: You are hereby notified of the following information in regard to the referenced RFP:

REVISIONS

1. On Page 4, Part I of the RFP, Section I-12, the language has been revised to read as follows:

Overnight Delivery Address:
Contracts Administration Department
Attn: Wanda Metzger
PA Turnpike Commission
700 South Eisenhower Blvd.
Middletown, PA 17057

US Mail Delivery Address:
Contracts Administration Department
Attn: Wanda Metzger
PA Turnpike Commission
P.O. Box 67676
Harrisburg, PA 17106

QUESTIONS AND ANSWERS

Following are the answers to questions submitted in response to the above referenced RFP as of January 17, 2013. All of the questions have been listed verbatim, as received by the Pennsylvania Turnpike Commission (PTC).

1) Who are the decision makers that will evaluate proposals and can we talk to them?

As stated in RFP Section III-2, Proposal Evaluation, Proposals will be reviewed, evaluated and rated by the Technical Evaluation Team (TET) of qualified personnel based on the evaluation criteria listed below. The PTC will not provide the names of the proposal evaluators. All communications concerning this procurement should be made through the contracting office (see RFP Section I-9).

2) Because SAP implementations vary so widely, would the Turnpike Commission provide a specific example of what they would consider an equivalent system for comparison as part of Lot 1?

See Appendix A.

3) For Lot 1, how many stakeholders does the Turnpike Commission expect the successful bidder(s) will need to interview?

As many as needed to accomplish the objectives of the project.

4) Are the current business processes supported by SAP documented? If so, will successful bidder(s) have access to that documentation?

Yes. The successful bidder will have access.

5) For Lot 2, how many stakeholders does the Turnpike Commission expect the successful bidder(s) will need to interview?

See the answer to question 3.

6) Do Lot 1 and Lot 2 need to complete at the same time?

No. While PTC anticipates that both activities can occur in parallel and we would like to complete both tasks as quickly as possible, there is no requirement that they end at the same time.

7) Is there a "drop-dead" date by which assessments must be completed?

No.

8) What is the process for formal acceptance of the deliverable(s) so invoicing can commence?

See RFP Section I-27 Inspection and Acceptance.

9) Does the Commission expect the offeror to perform a vulnerability assessment on the web applications and provide mitigation steps? Can you list the number of web-accessible applications and technologies involved?

Yes and the Commission's business partner hosts 8 in scope web apps, plus 3 mobile applications for smartphones.

10) Does the Commission have software licenses of the vulnerability assessment tools that the offeror can use for the infrastructure and application vulnerability assessment?

Refer to Section I-32 in RFP. The offeror will be expected to use their own software/tools to address this item.

11) Does the Commission expect the offeror to perform a security configuration review of the infrastructure, web applications and boundary defense devices using leading industry standards such as NIST special publication SP800-53?

See RFP Section IV-3, B, Information Security Program Assessment Lot 2.

12) The RFP requests the offeror to assess the commission's Security Information Event Management (SIEM) and data loss prevention programs. Can the Commission provide the product names used for the SIEM and the data loss prevention solutions that are currently being used? This is to help the offeror propose practitioners with relevant experience to perform the assessment?

The current SIEM in use at the Commission is QRadar, and there is no DLP product in use at this time.

13) Is the Commission required to meet Payment Card Industry (PCI) and other regulations? If yes, could the commission provide the list of regulations and standards the commission's information systems have to meet?

PCI related functions are performed by a 3rd party and PCI compliance is out of scope for this assessment.

14) Can the Commission mention the time of the last PCI audit and the vendor who performed this audit?

N/A

15) To estimate the effort for a review of the Commission's logical access control program, can the commission mention the solution and technology used for

a) Password management?

Active Directory Password Policy

b) Segregation of duties?

SAP Roles, sub-roles, Active Directory access privileges

c) Privileged users management?

IT Standards and procedures

d) Remote access?

Various virtual, VPN, and remote control tools

e) Wireless access?

Cisco

16) Does the Commission expect the offeror to develop any security policies and standards as part of this assessment?

The offeror is not expected to develop policy, however they are expected to point out deficiencies and recommend remediation.

17) The Commission states that there is a need for an overall assessment of their current SAP ERP system and Information Security Program. Please specify the format of deliverables expected as a result of these assessments: is the assessment expected to be in the form of a written report? Does the Commission expect multiple reports (i.e. one for the assessment of the original baseline implementation of the system, one for the current status and health of the system, and one for an assessment of the current organizational support structure for the system) or is one comprehensive report expected? Should we plan for a presentation to accompany the report? Are there expected dues dates for these deliverables (e.g. 6 months from start date)?

See RFP Section II-1, G. Approach.

18) Based on the SAP ERP and Information Security Program assessments, does the Commission expect that recommendations for action will accompany these assessments and, if so, what recommendations are expected? Would one of the possible recommendations be that the ERP system would be replaced?

See RFP Section I-5, Type of Contract and Section IV-3, Requirements. We anticipate options not recommendation and no option is off the table.

19) What are the anticipated contract dates for this project?

PTC would like to begin as quickly after RFP award as possible.

20) Is there a budget set for this project? If so, can it be shared with bidders?

The budget will not be shared with bidders

21) (p. 14, RFP Section: Part 2 – SAP Support Organization, RFP Text: The ESSG also works to effectively promote enterprise business process standardization….software.) Can you describe the ESSG process documentation available for the enterprise business processes?

Business Process Transactions Maps, BPPs and swim-lane diagrams.

22) (p 29, RFP Section IV-3 A. 2.d., RFP Text: An assessment of the policies, practices and procedures of the SAP support organization…procedures.) Can you describe the type of documentation of existing policies, practices and procedures?

We have various types of documentation that are in various forms such as MS Word, MS Visio and PDF documents.

23) (p. 29, RFP Section IV-3 A. 2.b., RFP Text: Assess how the Commission uses the SAP ERP system to support key business processes…) Can you describe the key business processes implemented in SAP?

In addition to the information provided in Appendix A there are approximately eighteen (18) enterprise-wide key business processes that we will provide details on to the successful bidder. An example business process would be Procure-to-Pay.

24) (p. 29, RFP Section IV-3 A. 2. a., RFP Text: Assess the current status and health of the functional and technical components of the Commission's SAP ERP environment and identify any issues, gaps or shortcomings. Identify options to remedy any issues, gaps or shortcomings found including benefits and disadvantages to each option.) Is SAP - BW configuration and performance to be included in the assessment?

Yes.

25) Will you provide offsite (remote) access to the awarded vendor?

No.

26) For the engagement being requested, is a thorough Information Security controls assessment (using a standard such as ISO or NIST as the framework) sufficient, or is a formal ISO 2700x Gap Analysis the preferred approach?

a) An IS controls assessment will review your security program and report on its overall status against best practice methodologies while paying particular attention to the areas you've highlighted, whereby a formal gap analysis will be a tabular report of whether you do or do not meet the specific ISO 2700x requirements for pre-defined security program components.

See RFP Section II-1, G. Approach. Also, refer to question 11 above.

27) For the Penetration Testing, how many of the 9100 total IPs do you want tested? How many of those would you like tested externally (via the Internet, as an outside attacker would see them) vs. internally (where we come onsite and test from within the network)?

See RFP Section II-1, G. Approach

28) Also, for the Penetration Testing, how intrusive do you want the testing to be? We offer 3 levels of testing – please select one for all the IPs or a different level for subsets of the IPs:

a) Vulnerability Assessment: "What are our weaknesses and how can we address them?"
i) Automated Scanning with manual validation/false positive reduction
ii) DELIVERABLE: List of vulnerabilities sorted by risk and host

b) Basic Pen Test: "Can someone break in to these systems?"
i) Automated Scanning with manual validation/false positive reduction
ii) Host penetration (local exploitation of discovered vulnerabilities)
iii) DELIVERABLE: List of vulnerabilities sorted by risk and host AND proof-of-concept information for penetrated hosts

c) Full Pen Test: "Can someone break in and if so, what damage could they inflict?"
i) Target validation
ii) Host penetration (local exploitation of discovered vulnerabilities)
iii) Privilege escalation on exploited hosts and attempted secondary penetration of other resources on customer's network
iv) DELIVERABLE: List of only those vulnerabilities that were successfully exploited to penetrate or bypass controls AND a narrative of successful penetration with step-by-step proof

See RFP Section II-1, G. Approach.

29) For the firewall rule set review, please provide us with the make and model of the firewalls, the count of the logical and physical firewalls (and how many are pairs vs. standalones), and the approximate number of rules per firewall to review.

The Commission has 3 pairs of firewalls: 1 pair has approximately 80 rules, 1 pair has approximately 10 rules, and 1 pair has approximately 5 rules.

30) For the web application security component, are you looking for actual web applications assessments? If so, how many web applications do you want assessed of each type (Static, Basic, Portal, Advanced or Custom) based on the following table:

Web App Assessment Scoping					
Application Includes one or more of	**Static**	**Basic**	**Portal**	**Advanced**	**Custom**
Static Content	√	√	√	√	√
Dynamic pages	√	√	√	√	√
Database backend		√	√	√	√
Login/accounts		√	√	√	√
Search function		√	√	√	√
HTML forms		√	√	√	√
File access			√	√	√
File upload			√	√	√
Instant messaging			√	√	√
Social networking			√	√	√
Stores PII				√	√
Financial data				√	√
Shopping cart				√	√
Flash or AJAX					√

See RFP Section II-1, G. Approach

31) Are you requesting wireless network penetration testing? If so, how many sites will we need to test? How many wireless access points at each site are there?

Yes, 2 sites (Central Administration Building (CAB), Highspire, PA and Turnpike Industrial Park Building (TIP), Middletown, PA), 80 total (22 in TIP, 58 in CAB)

32) Pages 6 through 21 - The RFP mentions several terms and conditions throughout these pages. However, there are missing terms (e.g. Limit of Liability, Warranties, etc.) that would make up a complete contract.

i) Is there an underlying full contract that vendors can review prior to the proposal submission date? Are the terms negotiable?

No. Some of the terms are negotiable while others are not [an example of a non-negotiable term is the application of Pennsylvania law but non-negotiable terms are not limited to this example].

33) Page 24, Section II-1, item H - how will PA Turnpike evaluate the Diversity portion of a vendors bid? Should vendors break out the Diversity cost in the Cost submittal? Likewise, should vendors state the diversity % in the Technical submittal?

See RFP Section III-3, item 4 for Criteria for Selection.
See RFP Section II-2, Cost Submittal, Cost Letter.

34) For Lot 1, How detailed is the documentation of the SAP system configuration and will this be accessible to the Contractor's assessment team?

It's documented at a high level and yes it will be accessible.

35) What is the make up of the current organizational support structure?

See ESSG Team Organization Chart on page 15 of the RFP Appendix A.

36) Page 29, Section IV-3, #3 – Does the current organization include contracted services provided by non-Turnpike employees? If so, is it an RFP requirement to review and assess the capabilities of contract resources?

Yes, we utilize staff augmentation resources but assessment of their capabilities is not a requirement of this RFP.

37) What government or industry regulations must PTC adhere to for data security?

PTC maintains certain personnel related data that falls under HIPPA. PTC contracted services are required to follow PCI requirements (which is out of scope).

38) Please clarify the expected information collection modes. Please clarify non-tool-based, through interview, observations, walk-thrus, and document reviews, versus tool-based?

See RFP Section II-1, G, Approach

39) For any tool-based testing, is PTC's preference to use vendor provided tools or to use PTC's tools?

See the answer to question 10

40) Please provide details of:
a) volume of available documentation (security policies, practices and procedures)
b) inventory of current security tools / technologies
c) numbers / roles of security staff organization / number in IT

Details related to the above will be provided to the successful proposer.

41) Please indicate if this work will take place at the PTC HQ location, or if travel will be needed to visit other remote sites.

We anticipate all work will take place either at the PTC's Central Administration Building in Highspire, PA or at the PTC's Turnpike Industrial Park facility in Middletown, Pa, which is in close proximity.

42) For the technical portions of the information security review, please describe the following:
a) Approximate # of interviews (IT Managers, administrators, network engineering, operations) to review security architecture
b) Firewalls: # and type of firewalls
i) Will we review PTC's firewall reviews or are you seeking our review of your firewall rule set?
ii) # of rules per firewall

c) IDS/IPS devices - Number and types of IDS/IPS – do you want the vendors to conduct config/signature enablement reviews?
d) 200 routers/500 switches; do you want the vendor to conduct configuration reviews?
e) VPN devices – do you want the vendor to review and test configurations?
f) Internal/External network vulnerability scans and/or penetration testing:
i) External – please describe # of externally visible IP addresses.
ii) Internal – please describe # of internal servers and # of IPs to be scanned.
g) Please provide number and type of database instances (distributed systems only) to be tested for configuration and vulnerabilities.
h) If social engineering assessment is to be included; how many and types of modes are to be tested? (i.e., phone, phishing, removable media).
i) If war dialing is to be included, please provide the number of phone numbers
j) If wireless penetration testing is to be included, please provide the number of access points, floors and building / locations.
i) Is the goal of the wireless testing to determine penetration testing or to assess the security posture of the access points?
k) Web application security – does the PTC intend for the vendor to review the security development lifecycle or perform actual testing of the various public facing applications?
i) If testing is in-scope, is PTC seeking application scans (determining vulnerabilities, or more thorough application penetration testing)?
ii) If penetration testing of the application is in-scope, please provide the following for each application:

(a) What does the application do – please provide a high level description of the application and describe how a typical user would interact with the application.
(b) How many dynamic pages (or forms) might a given user access in the course of interacting with the application? What percentage of the total number of pages includes fields that require user input, as opposed to content presentation only?
(c) How many user roles are there (regular user, organization admin, site admin, etc)? Can all users within a given role see/access the same data, or is data segregated by user or organization?
(d) Can users write data or do they have read-only permissions?
(e) Does dynamic content come from a database? If so, what kind of database is used and how does the server connect to the database?
(f) How are authentication and authorization performed? Authentication could be Basic auth, HTML forms, NTLM auth, LDAP server, certificates, etc.
(g) Is encryption used (SSL or something unique)?
(h) Which technologies and programming languages are in use (.NET, ASP, XML, IIS, WebLogic, SQL, Oracle, SOAP, Java, Visual Basic, JavaScript, etc)?
(i) Briefly outline the physical components that support the application (number of Web servers, app. servers, DB servers, etc.)
(j) Are there any special concerns (recent hacker activity, sensitive production environment, specific tests to perform) or anything that is unique to your application?
(k) Are there any timing (off-hours) or location (on-site) requirements? (Can the testing be performed remotely over the Internet?)

See RFP Section II-1, G, Approach. Additional information will be provided to the awarded proposer.

43) Does PTC have a classified / sensitive data policy or system in place?

No.

44) Are unstructured data repositories included within the scope or only relational database management systems (eg, Oracle, DB2, MySQL, etc.)? If yes for unstructured, how many unstructured repositories are expected to be reviewed?

No, unstructured data repositories are not included.

45) Has PTC built out a Vendor Management/Business Partner program? How many third parties exchange sensitive data with PTC applications?

No.

46) Does an incidence response team or Computer Emergency Response Team (CERT) exist? If so, how are incidents managed and what tools are used for incident response and incident/case management?

The Commission has an incident response process in place. Details will be provided to the awarded proposer.

47) Please describe the current Identity & Access Management program.

All authentication is done through Active Directory.

48) Has PTC implemented an enterprise-wide security awareness training program and is the program required for employees and contractors?

Yes.

49) SIEM Environment - Please describe the technology used, the number of log sources, how PTC administers, manages and reviews reports and logs. How does PTC continue to tune and incorporate new rules and policies into the SIEM environment?

The Commission's SIEM tool is QRadar. Additional details will be provided to the awarded proposer.

50) DLP – Please describe the implemented technology? Is it focused on DLP at the network, email, endpoint and data discovery areas?

See the answer to question 12.

51) (Section I-9. P. 2) On what date will answers to the questions be posted to the website?

RFP Addendum 2 will be the Q&A.

52) (Section II.1.F, p. 23) Can the relevant expertise and experience and the list of references include that for the prime and any subcontractors?

Yes.

53) (Section II-1.G, p. 23) For purposes of developing the project plan and timeline, what start date should be used by the offerors?

PTC would like to begin as soon as possible after award.

54) (Section II-1.H, p. 24) Would the PTC consider extending the diversity clause and evaluation criteria to also include those organizations that meet the Commonwealth of Pennsylvania's acceptance criteria of disadvantaged business such as those certified as U.S. Small Business Administration 8(a), Women's Business Enterprise National Council (WBENC) certified and/or U.S. Department of Veteran Affairs Service Disabled Veteran Owned at time of proposal submission?

No, as stated in Section II-1, H firms must be certified by the PAUCP.

55) (Section II-2, p. 25) Because of the skill sets required to conduct this type of evaluation, resources may have to travel to the PA Turnpike offices from outside the local commuting area. Will PA Turnpike consider creating a separate reimbursable not to exceed cost line to cover all travel costs rather than including them in the hourly rate? Adding travel costs into a Firm Fixed Price contract creates a risk for the government that estimated travel costs built into the proposal could exceed actual cost incurred.

No.

56) (Section III-3.4, p. 27) Although the criteria for selection has been provided in order of importance, can the Commission provide any more detail in the scoring criteria for selection listed, in terms of percentages? For example, what would be the total weight possible for including Disadvantaged, Minority and Women Business Enterprise? Can we assume that the approximate percentages for scoring a Commonwealth of PA proposal would be in play?

No. Weighting will not be used in the criteria for selection for this RFP.

57) (Section IV-3.B.1, p. 30) Does the scope of the Commission's boundary defenses also include any boundaries provided by 3rd party vendors, ISPs and/or contractors in addition to your 30-40 Business Partners? If so, will they be amenable to assessment and under the same contract terms as the Commission?

PTC anticipates a general approach for most business partners with specific assessments for at most four business partners. We anticipate full cooperation.

58) RFP Section I-11 indicates that proposals must be delivered to the Turnpike Commission's Contracts Administration Department ATTN: Wanda Metzger, whereas Section I-12 on the next page indicates ATTN: Donald Klingensmith. Please clarify the appropriate recipient.

See Revision Number 1 above.

59) Are all the SAP systems mentioned in appendix A in scope or only SAP ERP ECC

All systems mentioned in Appendix A are in scope.

60) Do you have the blueprint for all the phases implemented for the PA Turnpike.

Yes.

61) Do you have all the functional & technical scripts for the implemented SAP software.

Yes, to our knowledge.

62) Are all the SAP enhancements documented and if so to what detail are the functional and technical specifications documented

Yes. They are documented to the level that we deemed necessary for implementation and ongoing support.

63) Were any standard SAP functionality changed or enhanced without user exits or SAP approved methods?

No.

64) Do you have a system landscape document depicted the current system landscape, usage connections and system transport management?

No. We have each element appropriately documented but not currently in one system landscape document.

65) Do you use Solution Manager to manage projects and configuration of all the SAP systems?

No.

66) Are all SAP and Non SAP systems managed using SAP solution Manager – if not – what other system manage tools are in use.

No. None.

67) Did PA Turnpike implement Central User Administration – if so – are they integrated with the company LDAP.

No.

68) Does PA have a SAP strategy in place.

We are doing this assessment to inform revisions to the current strategy.

69) Doe the company experience current problems with the SAP install – if so please provide examples.

No.

70) When the system went live – did PA do a SAP go-live check using SAP earlywatch services – if so – do you have the results available.

Yes. Yes, they will be provided to the successful proposer.

71) How many earlywatch reports are available for the current systems

We have numerous reports but the most recent one was run in December of 2011.

72) Does the SAP systems run dual stacks or single stacks – please mention which systems are dual stacks vs. single stacks.

SRM, BI, XI and Solution Manager are dual stack systems. Core ECC and Portal (Java) are single stack systems.

73) Does PA have a centralized MDM policy in place for all SAP and non-SAP systems?

No.

74) Were any Six Sigma methodologies used in the current implementations?

No.

75) Will tools i.e. help desk logs, and resources, managers and product support leadership, used for tracking and managing defects, change requests, issues logs and items of the like be available for review, discussion and analysis?

Yes.

76) Were metrics or ROI calculations performed at any time, before the project, during the project or in post-production to establish a baseline or targets for efficiency, effectiveness and/or economy?

No.

77) From: Section IV-2, B (Page 28) - "The Commission is soliciting proposals from qualified I.T. consulting firms for the purpose of conducting an overall assessment of the Commission's Information Security **Program.**" (Emphasis mine.)

And, this is reinforced in the first paragraph of Section IV-3, B (Top of Page 30, but not reproduced here.) This all implies we are doing an assessment of how the Commission does things.

However...

From: Section IV-3, B (Page 30)
It seems to imply we are doing actual infrastructure assessments. Specific examples:

"1a. Internal/external network penetration testing. Scans must be coordinated with the Commission's staff and must not impact production capabilities of systems and networks. (This implies we are doing penetrations testing. jpm)"

"1c. Firewall rule set review. (This implies we are actually doing ruleset reviews. jpm)"

Are we to review your methodologies, or are we doing actual assessments?

Yes.

78) Which vendors for:

Firewalls
Routers
Switches

The RFP states "primarily" Cisco. Are there others in scope?

All are Cisco – no others are in scope.

79) What government or contractual regulations apply (PCI, etc.)

See the answer to question 13

80) How much of the infrastructure is managed by PTC and how much by 3rd party?

All infrastructure located at the Central Office and TIP buildings are managed by PTC.

81) Is analysis of Disaster Recovery (processes, procedures, infrastructure) considered in scope?

No.

82) What is the allotted timeframe and duration for offerors to conduct this engagement for each of two lots?

See II-1 G. Approach.

83) How many sites would this assessment entail?

See the answer to question 41.

84) How many stakeholders would we anticipate to interview in order to understand the PTC environment landscape as it relates to people, processes, technology for each of two lots?

See the answer to question 3.

85) PTC may have a list of many dozens of Business Partners. For the boundary defenses, does PTC expect an assessment against specific business partners or general approach?

PTC anticipates a general approach for most business partners with specific assessments for at most four business partners

86) Provided that ISO 27001 is the reference model for the assessment, where 11 domains are defined, are there particular security domains that would be deemed as out of scope?

See II-1 G. Approach.

87) Would PTC wish as a result of the engagement to understand their maturity level /rating against the selected industry guideline?

See II-1 G. Approach.

88) Would PTC wish as a result of the engagement to understand their capability level against other organizations through a comparative analysis?

See II-1 G. Approach.

89) While PTC has approximately 9100 IP addresses in use, approximately how many would be in-scope for the external network penetration testing?

See the answer to question 27.

90) Would the network penetration testing be limited to automated scans? Would the testing permit manual validation testing procedures?

See II-1 G. Approach.

91) Does PTC wish to have configuration assessments performed (ie. sampled selection of routers, switches, desktop/laptop computers, databases)? What would be in-scope / out-of-scope?

See II-1 G. Approach.

92) Would the data loss prevention portion of the engagement include an assessment of a tool currently being used?

See answer to question 12

93) Would the SIEM assessment include an evaluation of current use cases for security monitoring? Would the assessment entail an evaluation of the logs (suggesting where to further fine tune, etc)?

See II-1 G. Approach.

94) Would the Incident Response (SIRT) assessment include a test simulation of the processes and procedures real-time?

See II-1 G. Approach.

95) Are authentication and authorization controls centralized to a single device (e.g. PKI, TACACS, AD and LDAP)?

See answer to question 47.

96) Noting that PTC has various public facing applications, approximately how many web applications would be in-scope for the web application security testing?

See answer to question 9.

97) Would the web application security testing allow for both authenticated (valid user credentials) and unauthenticated (anonymous) testing?

See II-1 G. Approach.

98) Would PTC wish to have configuration assessments performed for the underlying web servers of the web apps identified in-scope for testing?

See II-1 G. Approach.

99) Would PTC want the Offeror to propose which standard/framework (i.e. NIST SP800 or ISO27000) to use in the assessment or discuss our ability to use one, the other, or both?

See II-1 G. Approach.

100) Does PTC have a desire to certify their ISMS processes and program, or does PTC want an assessment as, essentially, a gap analysis and performance improvement effort?

See the answer to question 26. Additionally, the Commission is not looking for an ISMS certification.

101) What scope of vulnerability assessments does PTC foresee: for example, will the assessments be port-scans? Wireless access points survey? Operating system and database updates?

See II-1 G. Approach.

102) Does PTC expect that the vulnerability assessment and other ISM assessment areas will be assessed at all or some remote sites, e.g., turnpike service stations or ticket stations?

Remote sites are considered to be out of scope for this assessment.

103) Will PTC be willing to share additional financial data for effective financial analysis?

Yes, this information will be provided to the successful proposer.

104) Would PTC dedicate resources for this assessment i.e., engagement director and/or coordinators, analysts, specialists, etc.

Yes.

105) Appendix A was not attached to the RFP document, nor does it seem to be available on the procurement page for the opportunity. May we please have a copy of Appendix A—SAP System Summary?

Appendix A was attached.

106) To ensure that our potential response is as complete and comprehensive as possible, will the commission provide Earlywatch reports for each of the SAP landscapes?

These will be provided to the successful proposer.

107) How many servers are in the Commission's computing environment?

145 physical servers and 234 virtual servers.

108) How many firewalls are in the Commission's computing environment?

See the answer to question 29.

109) How many physical locations does the Turnpike Commission have that could be part of scope?

Two locations are within scope (Central Administration Building, Highspire, PA and Turnpike Industrial Park Building, Middletown, PA).

110) Is wireless part of the Information Security assessment?

See the answer to question 31.

All other terms, conditions and requirements of the original RFP dated January 7, 2013 and Addendum 1 remains unchanged unless modified by this Addendum.