I. Introduction/ Scope of Work

In order for the Transportation Security Administration (TSA) Technology Solution Division (TSD) to improve its understanding of market capabilities, identify qualified vendors, and better develop an acquisition strategy, the TSA is seeking input from industry regarding an upcoming requirement for continuous IT Operations and Maintenance (O&M) Services in order to:

- Ensure the security of transportation passengers;
- Provide and increase vetting services for various transportation operations;
- Ensure the security of systems;
- Support network and infrastructure activities;
- Ensure systems are maintained properly for Continuity of Operations (COOP) and Disaster Recover (DR); and
- Ensure continuous operations and support in a 24X7X365, geographically dispersed, systems environment.

The scope of work will include:

- Program Management
- On-Site Operations Support
- System and Infrastructure Monitoring
- Systems Security and Analysis
- Network Operations Support
- Infrastructure Support
- Help-Desk Support
- Physical Data Access Control
- Incident and Problem Management Escalation
- Configuration Management Database (CMDB)
- Change Management
- Release Deployment
- Quality Assurance

The TSA anticipates that the period of performance for this requirement will be a base period of (1) year, with (6) one-year option periods.

The anticipated award date is Q3, FY2020.

II. Background

The TSA TSD is responsible for O&M of four (4) highly-available Mission Essential Systems (MES) as follows: Secure Flight (SF), Transportation Vetting System (TVS), Consolidated Screening Gateway (CSG), and Technology Infrastructure Modernization (TIM) systems. Additionally, a General Support System (GSS) has been deployed and identified as the Security Threat Assessment Mission Platform (STAMP) that hosts the credentialing applications for the TVS, CSG, and TIM mission programs.

These systems operate in two (2) geographically separate data centers located in Annapolis Junction, MD and Colorado Springs, CO. In addition to the two (2) data center operations, there is an on-site 24 x 7 x 365 Operations Support Center that provides a host of services to include

system & infrastructure monitoring, physical data access control, end-user helpdesk support for mission applications, and incident & problem management escalation.

III. Questions

Please respond to the following questions.

A. Operations Management/Data Center Operations

1. What is your company's experience in supporting highly available, mission essential systems of national/homeland security in an operational environment, on-site, 24x7x365, across multiple locations?
2. Has your company successfully developed, supported, and/or instituted a Risk Management (RM) process? If so, provide examples.
3. What is your experience with implementing and/or supporting Software Licenses Management (SLM) tools and processes?
4. What is your experience in creating and maintaining a Configuration Management Database (CMDB)?
    i. What CMDB tool(s) do you have experience with implementing and supporting?
5. What is your experience with managing the tracking and maintenance information of all system components and software?
6. What is your experience with gathering data from multiple systems to provide detailed timelines of system events and issues?
7. What is your experience with supporting various development methodologies in a single organization of multiple systems?
8. What is your experience with supporting various governance practices, release schedules, etc., of multiple systems in a single environment?
9. What is your experience with the following?
    a. Providing on-site 24x7, 365 help desk personnel/support
    b. Organization and communication (electronic and oral) skills
    c. Interfacing with external entities and providing customer support services.
    d. Supporting dual on-site support
10. What is your experience in supporting Data Center operations?
11. What is your experience in monitoring and managing the mechanical and electrical services, HVAC, and issue reporting of a Data Center?
12. What is your experience with managing the reporting of critical system incidents, daily operational system status reporting, incident and problem tracking/metrics, incident review for root cause analysis, and developing a proposed solution?

B. Operations & Maintenance

1. What is your experience with Infrastructure as a Service (IaaS) environment? Platform as a Service (PaaS)? DevSecOps?
2. What is your depth of expertise with the products and tools identified in Attachment 1-System Application and Hardware?
    a. Please complete the table provided in Attachment 1-Systems Application and Hardware
    b. Please provide a list of clients where the products and tools were utilized and provide a very brief project summary. If possible, please focus your response on Federal Government clients.

C. **ITIL Framework**

The TSA TSD O&M program recognize IT infrastructure library (ITIL) as a standard & detailed practice for IT Service Management (ITSM), aligning its IT services with that of TSA's mission.

Provide your companies specific experience with supporting Federal agencies with establishing, supporting, and/or maintaining the following ITIL areas and sub-areas:

1. Service Design
2. Service Transition
3. Service Operations:
4. Continual Service Improvement

D. **Information Security**

1. What is your experience in supporting a Security Control Assessment (SCA), achieving an Authority to Operate (ATO), and maintaining that ATO through its duration?
    a. Provide Experience with the following:
        i. System Security Plan (SP)
        ii. Contingency Plan (CP)
        iii. Contingency Plant Test (CPT)
2. What is your experience in supporting systems with a security categorization of High (H) – High (H) – High (H) in regards to confidentiality, integrity, and availability?
3. What is your experience working with systems that collect, store and maintain Sensitive Personally Identifiable Information (SPII)?
4. What is your experience with Continuous Diagnostics and Mitigation (CDM)?
5. What is your experience in system security in an Infrastructure as a Service (IaaS) environment? Platform as a Service (PaaS)? DevSecOps?
6. What is your experience with successfully developing, supporting, and/or instituting a system security risk process?
7. What is your experience with Disaster Recovery (DR) planning and exercise of drills?

E. **Contracts**

1. Do you currently have any contract(s), or does your company have the capability to contract for O&M services in support of a highly available, mission essential systems of national/homeland security within a twenty-five (25) mile radius of Colorado Springs, CO and Annapolis Junction, MD?
    a. Vendors should indicate any DHS Strategic Sourcing Contract and or General Services Administration (GSA) Federal Supply Schedule (FSS) contract number (i.e. DHS Strategic Sourcing vehicle, GSA Alliant 2 contract number) if applicable.
    b. Vendors should indicate their SB size standard
2. Does your company currently have strategic partnerships/subcontracts in place with staffing organizations that performing the type of work/services detailed in this RFI?
3. What Key Personnel would you recommend for this requirement?
4. What labor categories and skill sets your company typically proposes for similar services?

5. Provide input and suggestion to any specific Performance Metrics or Service Level Agreements (SLAs) that are in-line with industry practices for this type of requirement.
6. The TSA would like to ensure that rapid and thorough knowledge transfer takes place in order to enable the team to continue delivering valuable software to stakeholders throughout the contract transition period. What has been your experience in transferring knowledge from a contractor in place? What obstacles did you encounter and how did you respond to overcome them?

IV. Response Instructions

All interested and qualified parties are encouraged to respond to this notice in accordance with the instructions addressed herein.

The information requested in support of RFI must be prepared in electronic format in either Microsoft Word or PDF format. Responses shall be prepared using Times New Roman, 12-point font, 1 inch margins, and 8.5" by 11" paper. Fonts and sizes for graphics, charts, displays and tables submitted in either Times New Roman or Arial will be accepted with a minimum font size of 10pt.

Responses to the questions in Section III shall not exceed 10 pages in length including all images, data displays, charts, graphs, and tables (excluding cover page). The submission of standard marketing material is acceptable but will be considered in the page length.

Responses shall also include a completed table as part of Attachment 01-Systems Applications and Hardware.

Questions: All questions regarding this RFI must be submitted via electronic mail to HSTS02.Contracting@tsa.dhs.gov by 1700hrs local time Washington, D.C. on Tuesday, January 22, 2019.

RFI Closing Date: All responses to this RFI must be submitted via electronic mail to HSTS02.Contracting@tsa.dhs.gov by 1700hrs local time Washington, D.C. on Wednesday, Feburary 6th, 2019.

Responses not received by the closing date and time may not be considered or reviewed by the TSA.

V. Disclaimer

This RFI is issued solely for market research, planning, and information purposes in order to assist TSA TSD in assessing industry interest O&M for TSA TSD Mission Essential Systems. The Government will review vendor responses for market research purposes only. The Government does not intend to provide a response to white papers submitted for this RFI; however, based on vendor submissions, the Government may arrange a technical information exchange to further future requirements definition.
This RFI does not commit the U.S. Government to any course of action in the future. The Government will protect the information shared in the RFI response from disclosure to other parties. Each respondent, by submitting a response to the RFI agrees that any costs incurred in responding to the request or in support of activities associated with this RFI shall be the sole responsibility of the respondent/vendor. The Government shall incur no obligations or liabilities whatsoever, to anyone, for costs or expenses incurred by the respondent/vendor in responding to this RFI.