STATEMENT OF WORK

Software Vulnerabilities Testing Services

**Warning:**

The Statement of Work (SOW) paragraphs, Contract Data Requirements List (CDRL) items, and Data Item Descriptions (DIDs) identified for your type of acquisition are recommendations only. You are expected to modify or add SOW paragraphs, CDRLs, or DIDs to address the specific requirements of your program.

**Table of Contents**

[1.0 Scope 1](#_Toc393445300)

[2.0 General Tasks 1](#_Toc393445301)

[3.0 Specific Tasks 1](#_Toc393445302)

[4.0 References 2](#_Toc393445303)

[5.0 Deliverables 3](#_Toc393445304)

[6.0 Other Considerations 4](#_Toc393445305)

[7.0 Government Furnished Information, Facilities, and Equipment 4](#_Toc393445306)

[8.0 Other Special Requirements 5](#_Toc393445307)

# Scope

The primary mission of the Federal Aviation Administration (FAA) is to provide the safest, most efficient aerospace system in the world. Major FAA functions include regulating civil aviation; developing new aviation technology; developing and operating common air traffic control system for civilian and military aircraft; and research and development centered on the National Airspace System. The FAA must also regulate and certify the people and aircraft that use the airspace. Daily, the FAA manages more than thirty thousand commercial flights that move over two million passengers safely each day. The FAA mission depends on secure information sharing and information systems to ensure safety of both civilian and military aircraft.

The mission of the (Office Name) is to (identify office mission) e.g. information technology (IT), IT investment analysis, process engineering, enterprise architecture, program and portfolio services, information management, and information security.

# General Tasks

The objective of this SOW is to obtain enterprise wide license for vulnerability analysis services in order to discover flaws in agency-owned, agency-controlled, and third party software code. The vulnerability analysis must include the entire application, including components, any open source software and third party reference libraries without requiring the Government to provide source code. The service provider must also provide an on-line query and report capability that allows the Government to review the finding and recommendations; as well as conduct trend analysis across the enterprise.

# Specific Tasks

The Contractor is required to perform the following tasks:

1. Applications Testing Services for Government-owned applications.
2. The Contractor must assess application binaries statically and/or web applications dynamically for FAA-owned or controlled applications to find security-related flaws in Government applications/systems. The Contractor will conduct a vulnerability assessment on the entire application, including components, without requiring the Government to provide the source code.
3. At a minimum, the vulnerability assessment will be based upon list of common vulnerabilities and exposures (CVE) developed and maintained by the MITRE Corporation.
4. The Contractor provided service must utilize approved software and tools on the National Institute of Standards and Technology’s (NIST) binary scanning tool list.
5. The Contractor will provide the FAA with an on-line query/report capability that contains the findings and information on flaw type, severity, and recommendations.
6. The Contractor must also provide limited access to FAA business partners and contractors to the on-line query/report tool, as requested by FAA COTR.
7. Applications Testing Services for Commercial, Off-the-Self (COTS) software.

1. The Contractor must assess application binaries statically and/or web applications dynamically for third party (COTS) applications made available to the Contractor by FAA or Third Party Vendor to find security-related flaws in the application, including components and reference libraries.
2. At a minimum, the vulnerability assessment will be based upon CVE list developed and maintained by MITRE Corporation.
3. The service provided must use software and tools approved and added to the NIST’s binary scanning tool list.

1. The Contractor will provide the Government with an on-line query/report capability that contains the findings and information on flaw type, severity, and recommendations. The Contractor must also provide limited access to FAA business partners and contractors to the on-line query/report tool, as requested by FAA COTR. Training and Technical Support.
2. The Contractor will provide e-mail and telephone support during normal business hours, Monday through Friday, except Federal holidays. All messages left will be answered within one (1) business day.
3. The Contractor will assign a FAA Technical Account Manager. The person will serve as the FAA’s point of technical contact outside of the telephone and e-mail and may be contacted by the FAA COTR or other FAA representative, as necessary.
4. The Contractor will establish and maintain a self-service reference library that provided documentation to assist FAA employees and contractors on how to compile software code, upload guidance, access application’s test report electronically; and other information needed to use the service provided by the contract.

# References

All applicable documents referenced in this SOW are listed below.

1. Department of Transportation (DOT) Information Technology and Information Assurance Policy Number 2006-22 (revision 1): Implementation of DOT’s Protection of Sensitive Personally Identifiable Information (SPII), October 11, 2006.
2. FAA Order 1370.79A, Internet Use Policy, October 12, 1999.
3. FAA Order 1370.82A, FAA Information Systems Security Program, September 11, 2006.
4. FAA Order 1370.100, Media Sanitization and Destruction Policy, October 1, 2008.
5. FAA Order 1370.103, Encryption Policy, November 12, 2008.
6. FAA Order 1600.1D, Personnel Security Program, February 28, 2001.

1. FAA Order 1600.2E, Safeguarding Classified National Security Information, March 13, 2006.
2. FAA order 1600.38, Employee and Other Internal Security Investigations.
3. FAA Order 1600.72, Contract and Industrial Security Program, April 4, 2001.
4. FAA Order 1600.75, Protecting Sensitive Unclassified Information, February 1, 2005.
5. Any other applicable handbooks, policies, and guidelines.

# Deliverables

During the course of this contract, the Contractor must submit the following List of Deliverables and reports.

1. Progress Reports: The Governance requires the Contractor to submit the following reporting requirements electronically. The Format for the progress reports will be provided by the Contracting Officer’s Technical Representative (COTR) within ten (10) days after the contract award.
2. Annual Project Timeline.
3. Monthly Status Report: This report provides details on the work performed during the prior month and status on meeting timelines. This is due no later than the tenth (10th) working day of each month. Monthly Budget Report must provide expenditures from prior month broken down by task. The report will provide data related to subscription usage patterns, inventory of applications reviewed, list of top flaws, and results of on-line survey data, if applicable.
4. Quarterly Program Review and Report: The Contractor must maintain a single project schedule in Microsoft Project for Windows for internal use from which various project reports must be produced.
5. Software Development Lifecycle (SDLC) Review and Test Report.
6. The Contractor will provide the results electronically to the Government within five (5) business days after the compiled software code is made electronically available to the Contractor.
7. The SDLC Review and Test Report will contain the following information for each application tested, at minimum.
	1. Executive Summary;
	2. Summary of Flaws by Severity;
	3. Application Assurance Level;
	4. Overall Rating;
	5. Flaw Types of Severity and Category based upon MITRE CVE; and
	6. Explanation of Report Methodology, as needed (such as rating definition)

# Other Considerations

1. Travel: The Contractor must perform travel as required in the performance of the task order specified in the task areas. Travel must consist of domestic travel in support of the task order requirements as identified in the Task areas. Travel requirements will be coordinated with and approved by COTR in accordance with FAA and Department of Transportation policies, procedures and guidance as well as other appropriate guidance as listed elsewhere in this task order, but in no case in excess of travel amounts identified on the face of the contract Travel Ceiling. Reimbursement for travel will be in accordance with the Federal Travel Regulation (FTR). Receipts for hotel, airfare and car rentals must accompany invoice for payment.
2. Transmittal, Delivery, and Accessibility. The Contractor must provide two hard copies of each deliverable and one electronic version, an e-mail attachment, or a special Lotus Notes Database designated by the COTR.

# Government Furnished Information, Facilities, and Equipment

1. Government Furnished Information: The FAA may make available application/system information it has in its possession that would facilitate Contractor analyses, assessments, and reports required by this contract. This inventory of application/system and compiled software code will be specified upon award of each task order. The Contractor must be responsible for identifying in a timely manner via e-mail or telephone to the Government COTR, the specific data or information required for timely response to a task order.
2. Property and Equipment: The Contractor must provide appropriate office space and equipment for the performance of all task orders awarded under this contract. The Government will provide no property or equipment to the Contractor unless approved in writing by the FAA Contracting Officer.
3. Facilities: All work under this contract must be performed primarily at the Contractor’s facility.

# Other Special Requirements

1. Personnel Security: The Contractor must comply with FAA Order 1600.1D, Personnel Security Information.
2. Protection of Information: The Contractor must comply with FAA Order 1600.72, Contractor and Industrial Security Program. The Contractor must be responsible for properly protecting all information used, gathered, or developed as a result of work under all task orders issued under this contract.
3. Sensitive Security Information Storage:
4. Storage, handling and control of Sensitive Security Information (SSI) must be in accordance with FAA Order 1600.2E, Safeguarding Classified National Security Information and FAA Order 1600.75, Protecting Sensitive Unclassified Information. This applies to all task orders issued under this contract.
5. SSI and/or Government-Furnished Property or Equipment will be identified at the award of each task order. The Contractor must ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of government furnished information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to FAA control; destroyed; or held until otherwise directed. Items returned to the Government must be hand carried or mailed in a secure form to FAA COTR, or to the address indicated in the delivery/task order and/or DD Form 254. Destruction of national security information must be accomplished in accordance with FAA Order 1600.2D, Safeguarding Controls and Procedures for Classified National Security Information. Sanitization and destruction of all Sensitive Unclassified Information must be accomplished in accordance with FAA Order 1370.100, Media Sanitation and Destruction.