

NOTE: This must be included for ALL services contracts, to include task and call orders issued against existing IDIQs or GSA schedules

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

1. Contract or Task Order Title:

2. Purpose:

This Quality Assurance Surveillance Plan (QASP) provides a systematic method to evaluate performance for the stated contract. This QASP explains the following:

- What will be monitored?
- How monitoring will take place.
- Who will conduct the monitoring?
- How monitoring efforts and results will be documented.

This QASP does not detail how the contractor accomplishes the work. Rather, the QASP is created with the premise that the contractor is responsible for management and quality control actions to meet the terms of the contract. It is the Government's responsibility to be objective, fair, and consistent in evaluating performance. In addition, the QASP should recognize that unforeseen and uncontrollable situations may occur.

This QASP is a "living document" and the Government may review and revise it on a regular basis. Updates shall ensure that the QASP remains a valid, useful, and enforceable document. Copies of the original QASP and revisions shall be provided to the contractor and Government officials implementing surveillance activities.

3. Roles and Responsibilities:

The following personnel shall oversee and coordinate surveillance activities.

Program/Project Manager (PM) – The PM provides program oversight and supports the COR's performance assessment activities.

Contracting Officer (CO) – The CO shall ensure performance of all necessary actions for effective contracting, ensure compliance with the contract terms, and shall safeguard the interests of the United States in the contractual relationship. The CO shall also ensure that the contractor receives impartial, fair, and equitable treatment under this contract. Determine the final assessment of the contractor's performance.

Contracting Officer's Representative (COR) – The COR is responsible for providing continuous technical oversight of the contractor's performance. The COR uses the QASP to conduct the oversight/surveillance process. The COR shall keep a Quality Assurance file that accurately documents the contractor's actual performance. The purpose is to ensure that the contractor meets the performance standards contained in the contract. The COR is responsible for reporting early identification of performance problems to the CO. The COR is required to provide an annual performance assessment to the CO which will be used in documenting past performance. The QASP is the primary tool for documenting contractor performance. The COR is not empowered to make any contractual commitments or to authorize any contractual change on the Government's behalf.

Other Key Government Personnel:

COR-

DDS Product Manager-

DDS Portfolio Leader-

DDS Technical Lead-

NOTE: This must be included for ALL services contracts, to include task and call orders issued against existing IDIQs or GSA schedules

4. Primary Method of Surveillance:

The government will conduct **100% inspection** on all work presented by the contractor. For the purpose of this contract, this means that all vulnerabilities discovered by the contractor that are determined to be eligible for a bug bounty.

- ✓ **100 Percent Inspection.** This is usually only the most appropriate method for infrequent tasks or tasks with stringent performance requirements, e.g., where safety or health is a concern. With this method, performance is inspected/evaluated at each occurrence. One hundred percent inspection is too expensive to be used in most cases.

5. Performance Standards:

TECHNICAL EXHIBIT 1

Performance Requirements Summary

The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Requirements	Performance Standards	Acceptable Quality Level	Method of Surveillance
Provide support personnel to meet PWS requirements	All contractor personnel possess the skills needed to perform the required tasks as specified in the PWS.	All contractor personnel possess the needed skills within 2 weeks of processing. The Contractor's work products are suitable to support the full range of analysis as specified in the PWS. The Contractor's personnel are qualified and adept at presenting clear, concise, factual reports free from personal conclusions or any judgment of individual Editorial and typographical errors should be few	The COR accepts after edit, review, and feedback from Government technical personnel.
Hours of Work/ Workload Management	The Contractor ensures that sufficient staff is available via telework locations always during core business hours to	The Contractor ensures that sufficient staff is	The COR accepts after review and feedback from

NOTE: This must be included for ALL services contracts, to include task and call orders issued against existing IDIQs or GSA schedules

	support assigned requirements. The Contractor shall ensure its personnel accomplish the assigned tasks within agreed upon schedules, and at an acceptable level of quality	available during core business hours to proactively interact with clients and complete the requirements specified in the PWS. The Contractor ensures the COR is informed of developments with assigned actions.	Government technical personnel.
Services and Deliverables	The Contractor provides the full range of services required to support the requirements addressed in Part 5 of the PWS	The Contractor provides competent expertise and analysis that is consistent with the quality levels specified in the PWS. Deliverables are factual, well-written, 99% free of grammatical errors or misspellings, and free from personal conclusions drawn by the analysts or any judgment of individual . Writing meets college Baccalaureate degree standards for English grammar, spelling, and composition. Deliverables are accomplished by the due date/time specified in Part 5 of the PWS.	Random review of work products by the COR and feedback from a Government expert no less than once a week. Feedback from appropriate Government sources.
Services and Deliverables	The contractor will respond to request and triage issues in a reasonable amount of time as referenced in Part 5 of the PWS.	The Contractor should be able to respond to requests within 48 hours and triage issues within a reasonable timeframe	This metric will be continuously monitored by the COR
Services and Deliverables	The Contractor will deliver a final report that rolls up all data from end of each phase status reports, including activity metrics and coverage analytics, researcher vulnerability discovery and remediation metrics, vulnerability	The out brief is successful in informing the Government on the results of the bug bounty in a timely	The COR will conduct a review of work products before presenting to stakeholders. The government expects

NOTE: This must be included for ALL services contracts, to include task and call orders issued against existing IDIQs or GSA schedules

	submission volume, triage speed, signal-to-noise ratio, and patch effectiveness and lessons learned from the challenge. This should be done within a reasonable time at the end of the event.	manner.	that an outbrief of bounty results will be delivered in a timely manner.
Services and Deliverables	The contractor coordinates with researchers and the government to ensure manages the compensation, both financial and non-financial, to the researchers.	Bounty distribution should match the metric set forth by the Government. Bounties should be given out in a manner that maximizes the finding of critical and relevant vulnerabilities.	The COR will review the pace of bounties being distributed on a continuous basis.
Provide support personnel to meet PWS requirements	The contractor is expected to recruit researchers with extensive experience against these types of assets (e.g. static and dynamic testing and industrial control systems).	As referenced in the PWS, the Contractor should be able to recruit the necessary number of quality researchers in order to accomplish the bounty.	The COR will check on recruitment numbers before the challenge phase begins.
Services and Deliverables	Ability to efficiently, effectively, and diplomatically resolve disputes between researchers and asset owners such that the researcher-DoD relationship is preserved.	The Contractor will aid in resolving disputes in a way that preserves the relationship between the government and the researcher community.	This metric will be continuously monitored by the COR

6. **Documenting Performance:**

Acceptable Performance.

The Government shall document positive performance. A Performance Assessment Report (PAR) template is attached (Appendix 2). Any report may become part of the supporting documentation for fixed price payments, award/incentive fee payments, CPARS entries, or other actions. Government acceptance of services permits the contractor to invoice for the service fee.

NOTE: This must be included for ALL services contracts, to include task and call orders issued against existing IDIQs or GSA schedules

Unacceptable performance.

Unacceptable contractor performance can be identified by customer complaints (Appendix 2) or upon schedule surveillance evaluations. When unacceptable performance occurs, the COR shall inform the contractor. This will normally be in writing unless circumstances necessitate verbal communication. The COR shall document the discussion and place it in the COR file and provide a copy to the CO.

When the COR determines formal written communication is required, the COR shall prepare a Corrective Action Report (CAR). The CAR is forwarded to the CO for dissemination to the contractor. A CAR template is attached to this QASP (Appendix 3).

The contractor shall acknowledge receipt of the CAR in writing. The CAR will specify if the contractor is required to prepare a corrective action plan to document how the contractor shall correct the unacceptable performance and avoid a recurrence. The CAR will also state how long after receipt the contractor has to present this corrective action plan to the CO and COR. The Government may withhold payment for services until corrective action is taken. The Government shall review the contractor's corrective action plan to determine acceptability. Upon Government acceptance of the corrected services the contractor will be permitted to invoice for the service fee.

Any CAR may become a part of the supporting documentation for contract payment deductions, fixed fee deductions, award fee nonpayment, CPARS or other actions deemed necessary by the CO.

7. Mandatory or regulatory compliance items:

DDS: The contractor will provide initial proof of compliance with regulatory and compliance items contained in the contract. The Contracting Officer's Representative (COR) and the Contracting Officer (CO) will evaluate the initial submission and will conduct ad hoc reviews of the contractor's compliance throughout the remainder of the contract. The contractor will monitor compliance as required by FAR 52.222-50, Combating Trafficking in Persons, and report any issues to the CO.

8. Acceptable Quality Level (AOL):

DDS: The AQL for this project is 100% due to the critical support provided by bug bounty monitoring tools

9. Evaluation Method:

DDS: The COR will document the time of verbal notification to the contractor. The COR will document the official time and date of notification on the Maintenance Call Record. The COR will review self-diagnostic systems logs, conduct a comparison with actual maintenance performance and otherwise verify and validate contractor performance. The contractor shall enter in the record the official time the system is restored to full operational status. The COR will confirm the date and time of problem resolution in the record.

10. Performance Rating

In evaluating the quality of contractor's performance, the following performance ratings may be used (same as CPAR ratings).

Performance Rating	Criteria
Exceptional	Performance meets contractual requirements and exceeds many to the government's benefits. The contractual performance of the element or sub-element

NOTE: This must be included for ALL services contracts, to include task and call orders issued against existing IDIQs or GSA schedules

	being assessed was accomplished with no problems and contractor actions were highly effective.
Very Good	Performance meets contractual requirements and exceeds some to the government benefits. The contractual performance was accomplished with few minor problems for which corrective actions taken by the contractor were effective.
Satisfactory	Performance meets contractual requirements. The contractual performance contains some minor problems for which corrective actions taken by the contractor were satisfactory.
Marginal	Performance does not meet some contractual requirements. The contractual performance reflects a serious problem for which the contractor has not yet identified corrective actions. The contractor's proposed actions appear marginally effective or were not fully implemented.
Unsatisfactory	Performance does not meet most contractual requirements and recovery is not likely in a timely manner. The contractual performance contains serious problem(s) for which the contractor's corrective actions appear or were ineffective.

Appendix 1 – Performance Assessment Report

PERFORMANCE ASSESSMENT REPORT (PAR) <i>(If more space is needed, use reverse and identify by number)</i>							
1. CONTRACT/TASK ORDER NUMBER		2. CONTRACTOR		3. TYPE OF SERVICES			
4. QUALITY ASSURANCE PERSONNEL (COR) SIGNATURE AND DATE				5. COR PHONE		6. SUSPENSE DATE	
I. PERFORMANCE							
7. <input type="checkbox"/> DEFICIENCY (CHECK ALL BOXES THAT APPLY) <input type="checkbox"/> NEW <input type="checkbox"/> REPEAT <input type="checkbox"/> NO DEFICIENCY NOTED				8. SERVICES SUMMARY or PWS PARAGRAPH ITEM REVIEWED			

NOTE: This must be included for ALL services contracts, to include task and call orders issued against existing IDIQs or GSA schedules

9. BRIEF DESCRIPTION OF DEFICIENCY (IF DEFICIENCY BOX WAS CHECKED)	10. DETAILED PERFORMANCE ASSESSMENT
II. CONTRACTOR VALIDATION	
11. CONTRACTOR REPRESENTATIVE <input type="checkbox"/> CONCUR <input type="checkbox"/> NON-CONCUR	12. CORRECTIVE ACTION ESTIMATED COMPLETION DATE
13. CONTRACTOR REPRESENTATIVE CORRECTIVE ACTION AND PREVENTION OF RECURRENCE <u>OR</u> REASON FOR NON-CONCURRENCE OF COR CITED DEFICIENCY	
III. ACTION CORRECTED	
14. <input type="checkbox"/> CONCUR <input type="checkbox"/> NON-CONCUR COR SIGNATURE AND DATE	
15. COR REMARKS (REQUIRED)	
6. CONTRACTOR REPRESENTATIVE REMARKS	

Appendix 3 – Customer Complaint Record

CUSTOMER COMPLAINT RECORD			DATE/TIME OF COMPLAINT
SOURCE OF COMPLAINT			
ORGANIZATION	BUILDING NUMBER	INDIVIDUAL	PHONE NUMBER

NOTE: This must be included for ALL services contracts, to include task and call orders issued against existing IDIQs or GSA schedules

NATURE OF COMPLAINT

CONTRACT REFERENCE

VALIDATION

DATE/TIME CONTRACTOR INFORMED OF COMPLAINT

ACTION TAKEN BY CONTRACTOR

CORRECTIVE ACTION REPORT (CAR)

(If more space is needed, use reverse and identify by number)

1. CONTRACTOR

2. CONTRACT NUMBER

3. TYPE OF SERVICES

4. FUNCTIONAL AREA

5. SUSPENSE DATE

6. CONTROL NUMBER

NOTE: This must be included for ALL services contracts, to include task and call orders issued against existing IDIQs or GSA schedules

7. DEFICIENCY ☐ MAJOR ☐ MINOR

FINDING:

FINDING IMPACT:

Please respond with a written corrective action plan that details the corrective action of the cited deficiency, the cause of the deficiency, and actions taken to prevent recurrence by Suspense Date in Block 5. If date was not entered in Block 5, the contractor is not required to provide a response.

8. QUALITY ASSURANCE PERSONNEL (COR)

TYPED NAME AND GRADE

SIGNATURE AND DATE

9. ISSUING AUTHORITY

TYPED NAME AND GRADE

SIGNATURE AND DATE

10. COR RESPONSE TO CONTRACTOR CORRECTIVE ACTION AND ACTION TAKEN TO PREVENT RECURRENCE

11. COR DETERMINATION

☐ ACCEPTED ☐ REJECTED

12. CLOSE DATE

RECEIVED/VALIDATED BY

NOTE: This must be included for ALL services contracts, to include task and call orders issued against existing IDIQs or GSA schedules

Appendix 4 – Corrective Action Report